Nuclear Safety
NEA/CSNI/R(2012)2
July 2012
www.oecd-nea.org

Workshop on PSA for New and Advanced Reactors

OECD Conference Centre
Paris, France
June 20–24, 2011

Organised by the Working Group on Risk Assessment (WGRISK)

NUCLEAR ENERGY AGENCY

Unclassified **NEA/CSNI/R(2012)2**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **19-Jul-2012**

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

Workshop on PSA for New and Advanced Reactors

OECD Conference Centre, Paris, France, 20-24 June, 2011
Organized by the Working Group on Risk Assessment (WGRISK)

JT03324848

Complete document available on OLIS in its original format

NEA/CSNI/R(2012)2
Unclassified

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 34 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 30 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, the Republic of Korea, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include the safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information.

The NEA Data Bank provides nuclear data and computer program services for participating countries. In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

THE COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

"The Committee on the Safety of Nuclear Installations (CSNI) shall be responsible for the activities of the Agency that support maintaining and advancing the scientific and technical knowledge base of the safety of nuclear installations, with the aim of implementing the NEA Strategic Plan for 2011-2016 and the Joint CSNI/CNRA Strategic Plan and Mandates for 2011-2016 in its field of competence.

The Committee shall constitute a forum for the exchange of technical information and for collaboration between organisations, which can contribute, from their respective backgrounds in research, development and engineering, to its activities. It shall have regard to the exchange of information between member countries and safety R&D programmes of various sizes in order to keep all member countries involved in and abreast of developments in technical safety matters.

The Committee shall review the state of knowledge on important topics of nuclear safety science and techniques and of safety assessments, and ensure that operating experience is appropriately accounted for in its activities. It shall initiate and conduct programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach consensus on technical issues of common interest. It shall promote the co-ordination of work in different member countries that serve to maintain and enhance competence in nuclear safety matters, including the establishment of joint undertakings, and shall assist in the feedback of the results to participating organisations. The Committee shall ensure that valuable end-products of the technical reviews and analyses are produced and available to members in a timely manner.

The Committee shall focus primarily on the safety aspects of existing power reactors, other nuclear installations and the construction of new power reactors; it shall also consider the safety implications of scientific and technical developments of future reactor designs.

The Committee shall organise its own activities. Furthermore, it shall examine any other matters referred to it by the Steering Committee. It may sponsor specialist meetings and technical working groups to further its objectives. In implementing its programme the Committee shall establish co-operative mechanisms with the Committee on Nuclear Regulatory Activities in order to work with that Committee on matters of common interest, avoiding unnecessary duplications.

The Committee shall also co-operate with the Committee on Radiation Protection and Public Health, the Radioactive Waste Management Committee, the Committee for Technical and Economic Studies on Nuclear Energy Development and the Fuel Cycle and the Nuclear Science Committee on matters of common interest."

FOREWORD

As stated in the mandate of the OECD/NEA Committee for the Safety of Nuclear Installations' (CSNI) Working Group on Risk Assessment (WGRISK), the working group supports improved uses of Probabilistic Safety Assessment (PSA) in risk informed regulation and safety management through the analysis of results and the development of perspectives regarding potentially important risk contributors and associated risk-reduction strategies. WGRISK's activities address the PSA methods, tools, and data needed to provide this information.

Probabilistic Safety Assessment/Probabilistic Risk Assessment (PSA/PRA) for new and advanced reactors is recognized as an important approach to achieve improved safety for the future nuclear power plants. For the purpose of this work, new reactors are defined as having a stable general design which is typically within five to ten years of commencing power operations. Advanced reactors are reactors which are generally in the earlier conceptual or preliminary design stage.
The application of PSA to these reactors encounters concurrent challenges, which are slightly different for new and advanced reactors due to their development phases. The ability of current PSA technology to support design decisions for such reactors, and the potential value of advanced methods have not been internationally assessed in recent times. In order to address the above issues, WGRISK conducted two coordinated tasks: "PSA for Advanced Reactors" and "PSA in the Frame of Design and Commissioning of New NPPs". The objectives of the two tasks are:

- PSA for Advanced Reactors:
  - Characterize the ability of current PSA technology to address key questions regarding the development, acceptance, and licensing of advanced reactor designs;
  - Characterize the potential value of advanced PSA methods and tools for application to advanced reactors;
  - Develop recommendations to CSNI for any needed developments regarding PSA for advanced reactors.
- PSA in the frame of Design and Commissioning of New NPPs:
  - Identify and characterize current practices regarding the role of PSA in the frame of design, construction and commissioning of new nuclear power plants in the member states;
  - Identify key technical issues regarding the PSA for new reactors, current approaches for dealing with these issues and associated lessons learned, as well as issues requiring further work;
  - Develop recommendations regarding the use of PSA by different actors in the frame of new nuclear power plant projects: appropriate PSA scope and level of details, pertinent PSA applications and decision-making process;
  - Identify future international cooperative work on the identified issues.

In order to support the objectives of these two tasks, two task-specific questionnaires were developed by the task core groups and answered by the participating countries and organisations. Additionally, a joint workshop entitled "OECD/NEA Workshop on PSA for new and advanced reactors" was held at the OECD Conference Centre during June 20-24, 2011. The present report documents the proceedings and the outcome of this workshop.

Workshop on PSA for New and Advanced Reactors
OECD Conference Centre, Paris, June 20-24, 2011
Organized by the Working Group on Risk Assessment (WGRISK)

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

1.1 Background

Probabilistic Safety Assessment/Probabilistic Risk Assessment (PSA/PRA) for new and advanced reactors is recognized as an important approach to achieve improved safety and performances of new nuclear power plant (NPP), comparing to the existing plants. However, the application of PSA to these reactors encounters concurrent challenges, which are slightly different for new or advanced reactors due to their development phases. The technical challenges of the PSA for new reactors, which are in the last phases of design and commissioning stage, typically within five to ten years of commencing power operations, include a lack of design detail, a lack of empirical data, and the possibility of failure scenarios that differ in character from those treated in PSAs for current reactors. These challenges can affect a variety of decisions (e.g. plant safety level assessment, defense in depth assessment and risk balanced concept etc.) The technical challenges of the PSA for more advanced reactors, which are in research stage or in the early phases of conceptual design, in addition to the above-mentioned aspects, also include the potential need to address very different systems and phenomenology. The ability of current PSA technology to support design decisions for such reactors, and the potential value of advanced methods have not been internationally assessed in recent times.

In order to address the above issues, the WGRISK is currently conducting two coordinated tasks: “PSA for Advanced Reactors” and “PSA in the frame of Design and Commissioning of New NPPs". In order to support the objectives of these two tasks, the WGRISK organized a joint workshop entitled “OECD/NEA Workshop on PSA for new and advanced reactors,” which was held at the OCED Conference Center during June 20-24, 2011. The present report summarises the result of this workshop.

1.2 Objective of the workshop

The key objective of the workshop was to support the fulfillment of the two coordinated WGRISK Tasks on “PSA for Advanced Reactors” and on “PSA in the frame of Design and Commissioning of New NPPs." The objectives of the two tasks are:

(1) PSA for Advanced Reactors

- Characterize the ability of current PSA technology to address key questions regarding the development, acceptance, and licensing of advanced reactor designs;
- Characterize the potential value of advanced PSA methods and tools for application to advanced reactors;
- Develop recommendations to CSNI for any needed developments regarding the PSA for advanced reactors.

(2) PSA in the frame of Design and Commissioning of New NPPs

- Identify and characterize current practices regarding the role of PSA in frame of design, construction and commissioning of new nuclear power plants in the member states;
- Identify key technical issues regarding the PSA for new reactors, current approaches for dealing with these issues and associated lessons learned, as well as issues requiring further work;
- Develop recommendations regarding the use of PSA by different actors in the frame of new nuclear power plant projects: appropriate PSA scope and level of details, pertinent PSA applications and decision-making process;
- Identify future international cooperative work on the identified issues.

1.3 Organization of the workshop

The main topics of interest, discussed during the workshop, included the followings: regulatory aspects, risk-informed methods, technical aspects of the PSA for new and advanced reactors, hazards of PSA (internal and external), severe accident/source term/Level 2 PSA, and consequence analysis/Level 3 PSA.

The workshop program is provided in Appendix 1.

The paper presentations and discussions were performed during the first 3 days of the workshop (20-22 June 2011). Two additional days (23-24 June 2011) were dedicated to the preparation of the draft proceeding and conclusions by the Workshop Technical Committee members and Workshop session chairpersons.

Fifty experts from 13 countries and one international organization (IAEA) participated in the present workshop, and 35 technical papers and 2 CAPS task activities were presented as shown in the following:

National contributions (35 papers from 12 countries & IAEA)

	France	USA	Korea	China	Japan	Germany	Others	Total
Papers	8	9	4	3	2	2	7	35

(*) Others (1 paper per country) : Belgium, Finland, Italy, Russia, UK, India, IAEA

Category	France	USA	Korea	China	Japan	Germany	Others	Total
New	3	4		3			3	13
Advanced	4	3	3		2	1	1	14
Common	1	2	1			1	3	8

(*) **New:** Gen-III/III+ (EPR/AP1000/ABWR...); **Advanced:** Gen-IV (HTGR/VHTR/FBR/SMR...)

Category	France	USA	Korea	China	Japan	Germany	Others	Total
Level 1	7	1	2	2	1	1	2	16
Level 2	1	1			1	1	1	5
Common		7	2	1			4	14

1.4 Results

The joint workshop provided an interesting and useful forum for the participants to share and discuss their respective practices regarding PSA applications for new and advanced reactors.
The workshop discussions indicated that there is currently a wide spectrum of views and practices, key technical and regulatory issues requiring further work, as well as potential areas for future international collaboration. Since the workshop was not designed to achieve consensus, this report does not provide any group recommendation regarding the underlying issues. However, the workshop results are an essential input to these two WGRisk tasks on "PSA for Advanced Reactors" and on "PSA in the frame of Design and Commissioning of New NPPs" and the final report for these tasks will provide recommendations.

Globally, the technical issues discussed during the workshop, like passive systems reliability, reliability data, digital I&C (Instrumentation and Control), HRA (Human Reliability Assessment), and external events (however widely discussed after Fukushima events) etc., are not newly added emerging issues, the workshop was regarded as a good opportunity to discuss the day status and to exchange lessons learned among the participants.

The followings summarize key points of the presentations and discussions made during the workshop.

(1) PSA in the frame of Design and Commissioning of New NPPs:

Current practices:

- For all new reactor projects, the role of PSA is more important and more formalized as compared with the operating plants;

- For new reactors, PSA is used by the industry at all stages of the design for a wide variety of applications, including demonstration of safety level, balancing between accident prevention and mitigation features of the design, identification of design vulnerabilities and improvements, comparison with the risk of existing plants, and establishment of requirements for systems/sub-systems;
- Regulatory agencies are using PSAs to identify risk-significant areas for safety reviews and some of them developed requirements for PSAs and applications;
- Regulatory and industry organizations in some countries are supporting the development of standards for PSA development and applications;
- Regulatory PSA models are developed in some countries and are used for a confirmatory check of an applicant's model;
- The participants expressed the need for better advice, based mainly on the lessons learned, on how to use PSA during the different design phases;
- It is more difficult to ensure PSA quality for the newer designs because of a lack of peers, limited scope PSA (mainly at the beginning of design), challenges in ensuring strong interaction between design and PSA teams as the design evolves;
- Despite data, modeling and code limitations, Level 3 PSA was identified as a necessary support for some new reactor applications (e.g. definition of the emergency zones);
- Applicability of PSA for addressing the safety-security interface is an interesting topic.

Key technical issues for further work:

- Better guidance and lessons learned exchange on PSA development and use in the different design phase;
- Data and modeling improvements and clarifications, especially in the modeling of: new components, new severe accident features, passive systems, digital I&C, intersystem CCF (Common Cause Failures), and human actions etc;
- Improve completeness in the modeling of external events, including treating of potential combinations of hazards and their impacts on multi-unit sites.

Potential areas for international collaboration:

- External events modeling;
- Passive systems modeling;
- International reviews of new/advanced reactors PSA and PSA applications.

(2) PSA for advanced reactors:

Current practices:

- PSAs are being used at the conceptual or preliminary design stages, most analyses use currently available PSA methods including the conventional ET (Events Tree) / FT (Fault Tree) and RMPS (Reliability Method for Passive Systems) approaches;
- The regulatory agencies have expressed explicitly their expectations or requirements to encourage the activities to integrate the use of risk insights more fully into the design and safety review;
- Many efforts are focused on identifying and resolving well-recognized issues in an advanced reactors-specific context, which are major concerns of designers and regulators;
- Nevertheless, there is no consensus and guidance on how to take into account the foregoing issues (including the level of depth of the analyses) and on how to incorporate them into the PSA framework;
- The use of the non-ET/FT methods/tools is being explored as a mean to more explicitly tie phenomenological modeling into the PSA (e.g., RMPS, Dynamic PSA, and DDETs (Discrete Dynamic Event Trees));
- Gen IV RSWG (Risk and Safety Working Group) is developing TNF (Technology Neutral Framework) and ISAM (Integrated Safety Assessment Method) for safety assessment of advanced reactors, which synthesizes the different approaches to safety;
- The USA is developing ASME/ANS standards for advanced non-LWR ((Light Water Reactor) PRA.

Key technical issues for further work:

- Scope of the PSA for advanced reactors, compared to that of the current and new reactors;
- Modeling approaches and tools to assess potential severe accidents at the pre-conceptual design phase, especially non-LWR types of reactor;
- Increasing competence in identifying potential hazards and accident scenarios (what can go wrong), helpful for designers;
- Some guidance to answer the question as to whether the PSA state of the art is adequate to support a specific application;
- Risk metrics and safety goals for advanced reactors;
- Handling the safety-security interface;
- Peer review guidance for the PSA.

Potential areas for international collaboration:

- Guidance to determine technical acceptability of PSA for advanced reactors (including the ASME/ANS non-LWR standard) and provide its implementation process;
- Modeling approaches and tools to support advanced reactor-specific phenomena analysis;
- Assessment of potential severe accidents at the pre-conceptual design phase of advanced reactors;

- Passive safety systems reliability and ISAM under advanced design features;
- Collaboration with ongoing international activities (e.g., GIF-RSWG and IAEA CRP on passive system reliability).

2. SUMMARY OF THE WORKSHOP SESSIONS

The workshop was composed of 9 technical sessions and 3 break-out sessions. The break-out sessions were intended to provide a framework to present summaries of the day presentations and to discuss the day open issues and conclusions. The summaries of the task questionnaire answers were presented during the first two break-up sessions (advance reactors on Monday 20 June and new reactors on Thursday 21 June. The last break-up session on Wednesday 22 June was also dedicated to preparatory discussion for the proceedings development. The following is a summary of these sessions prepared by the corresponding session chairs.

2.1 Day 1 (20 June)

(1) Summary of Technical Session 1 (by Nathan Siu)

This session involved presentations on the performance of PSAs for four advanced reactor designs. (All four designs employ passive decay heat removal systems.) All of the analyses were performed by the authoring organization(s) to support the design process some of the analyses have been discussed informally with regulatory authorities but none have been formally reviewed.

The first presentation ("Level-1 PSA to Support the Design of the KALIMER-600 Sodium-cooled Fast Reactor," S. J. Han, KAERI-Korea) introduced the application of a Level 1, internal events, at-power PSA to support the design of KALIMER-600, a 600 MWe, metallic-fueled, sodium-cooled fast reactor being designed by KAERI. The paper outlined the technical approach used, presented a number of results for CDF (Core Damage Frequency), including the results of sensitivity analyses, and identified important sources of uncertainty.

The second presentation ("Study on Preliminary Level-1 PSA for Japan Sodium-cooled Fast Reactor," K. Kurisaka, JAEA-Japan) introduced the application of a Level 1, internal events, at-power PSA to support the conceptual design of the JSFR (Japanese SFR), a 1500 MWe, mixed-oxide fueled, sodium-cooled fast reactor being designed by JAEA. The paper also described a seismic margins analysis performed to show conformance with stricter seismic standards imposed after the 2007 Niigata-ken Chuetsu-oki earthquake. Further, the paper develops reactor-specific CDF and CFF (Containment Failure Frequency) goals based on: a) the point that existing CDF and CFF goals (1E-5/yr and 1E-6/yr, respectively) apply to the site as a whole, and b) a fractionation of these goals to account for the number of reactors on site.

The third presentation ("Level 1 Probabilistic Safety Assessment to Support the Design of the CEA 2400MWth Gas-cooled Fast Reactor," F. Bertrand, CEA-France) introduced the general use of deterministic and probabilistic methods in the design of the GFR 2400, a 1120 MWe ceramic-plate fueled, helium-cooled fast reactor being designed by CEA. Similar to the previous papers, the PSA addresses Level 1 internal events occurring during power operation. The analysis does not include human reliability considerations – these are planned to be addressed later. Some specific technical aspects of the PSA are dealt with in companion papers presented later in the workshop.

The fourth presentation ("Overview of VHTR's PSA Approach in Korea," S. J. Han, KAERI-Korea) introduced the application of an internal events, at-power PSA to support the conceptual design of a KAERI-designed, TRISO-fueled, helium-cooled VHTR (Very High-Temperature Reactor). Due to the non-threshold release characteristics of the reactor's TRISO (TRi-ISOtropic-coated fuel particles) fuel, the paper addressed plant damage states with varying degrees of release as well as a consolidated core heat-up frequency. Due to the stage of the project, the results presented in the paper are tentative.

Discussion: All of the reported analyses employed currently available PSA event tree/fault tree analysis technology. Specific analysis features reported included the use of: Master Logic Diagrams and methods considering heat balance and reactivity balance to support initiating event identification; worldwide experience to estimate the leak frequency-magnitude relationship; documented assumptions regarding PSA model parameters (including initiating event frequencies); explicit models for passive system actuation; multi-state event sequence modeling to address the continuous performance of passive systems; Monte Carlo methods to propagate uncertainties and sensitivity studies to address the potential importance of key uncertainties. The PSA technical issues raised by the papers and subsequent group discussion included: reliability parameter estimation for new SSCs (Structure, Systems and Components) (including CCF) and phenomena (e.g., sodium solidification frequency), passive safety system reliability estimation, digital I&C system reliability, human reliability, and severe accident modeling and source terms.

The PSA uses identified in the papers and subsequent discussion included: the identification of design improvements (e.g., addition of non-safety, electrically-powered blowers; addition of redundant, diverse actuation; rejection of a proposed additional cooling loop to simplify the plant's design); and the demonstration of achievement of design targets (including "balanced design" as well as specific risk-related targets). One of the papers raised the potential need for a common regulatory framework for advanced non-LWRs, and the group also discussed the potential need for different design targets to reflect the specifics of plant damage states.

(2) Summary of Technical Session 2 (by Attila Bareith)

Four presentations were given in Session 2. The focus was on using PSA for advanced reactor designs, although two papers from the four also addressed currently operating as well as new reactors. The first two papers covered safety assessment methodologies, while the last two presentations described examples of specific safety analyses either as full-scope PSAs or as system analyses performed in support of a risk-informed approach to plant design.

The first presentation ("Generation IV Integrated Safety Assessment Methodology," T. Leahy, INL-USA) described the activities of the Gen. IV RSWG that supports the efforts on developing Generation IV systems by promoting a consistent approach to safety, risk and regulatory issues. RSWG develops a technology neutral methodology for safety assessment of advanced reactors. The most important requirements and desired characteristics for the methodology were described. An ISAM is being developed in response to these needs, which synthesizes the different approaches to safety assessment with PSA having a key, central role in the process from pre-conceptual design up to licensing and operation. Some elements of the proposed methodology have been applied to a limited extent to French and Japanese SFR concepts. The methodology document will be finalized in 2011. Its detailed applications are to come afterwards with pilot studies on selected Generation IV systems.

The second presentation ("ASAMPSA2 Project: Appliance of LWR PSA2 Methodology to GEN IV Reactors," H. Bonneville, IRSN-France) included an overview of the European ASAMPSA2 (Advanced Safety Assessment Methods on PSA Level 2) project in the first place. In particular, the harmonized methodology guide on Level 2 PSA was highlighted as the most important result of the project. A draft version is available, improvements are foreseen in 2011. A limited effort was made to examine the relevance and applicability of the guide to actual Generation IV concepts. Four selected concepts were used for the assessment: SFR (Sodium-cooled Fast Reactor), GFR (Gas-cooled Fast Reactor), LFR (Lead-cooled Fast Reactor) and VHTR. The conclusions of the study suggest that Level 2 PSA can be performed at an early stage in the design of advanced reactors to yield risk insights and help prioritize R&D activities. However, compliance/applicability of the guide to Generation IV reactors cannot be assessed yet in detail due to the current status of design, lack of PSA models and other information, like EOP (Emergency Operating Procedure) and SAMG (Severe Accident Management Guideline) necessary for performing Level 2 PSA.

As follow-on to the description of risk-informed support to the design of the CEA's 2400 MWth gas-cooled fast reactor, the third presentation ("Reliability Analysis of 2400 MWth Gas-cooled Fast Reactor Natural Circulation Decay Heat Removal System," M. Marques, CEA-France) discussed the reliability analysis of the decay heat removal system with natural circulation as a specific example of this approach. System reliability was evaluated for two representative scenarios, a LOFA (Loss Of Flow Accident) and a LOCA (Loss Of Coolant Accident) sequence, respectively) based on a complex set of failure criteria following the RMPS methodology. Uncertainties were propagated through thermal-hydraulics model during simulations performed by the CATHARE-2 code. The system failure probability was found very low in the LOFA scenario, while improvements in design parameters and associated uncertainties were seen necessary in case of LOCA. The study yielded insights into making these improvements.

The last presentation ("Level-1 PSA for Internal Events for TAPS3&4 - A Challenge," R. Guptan, NPCIL-India) covered PSA for Indian PHWRs (Pressurized Heavy Water Reactors) including the existing 540MWe reactor, and, to a lesser extent, the new reactor of 700MWe as well as their advanced heavy water reactor. Extended level 1 PSA for internal events was performed to find dominant risk contributors and identify weak links / imbalance using mostly IAEA guidelines and applying a strict quality assurance program. Over and above risk quantification, recommendations were developed to maintain and further improve plant safety by focusing better on important risk contributors (e.g. ensuring risk awareness through training) and also by making modifications (e.g. introduction of staggered testing

for ECCS (Emergency Core Cooling System). Risk reduction was also found feasible for the 700 MWe PHWR. Finally, PSA resulted in very low frequency of core damage and core degradation attributable to some salient passive safety design features of the plant. From the point of view of methodology the intention to apply the ATHEANA (A Technique for Human Error Analysis) framework to human reliability analysis was emphasized.

Discussion: The most important aspects from the follow-on discussions that have relevance to the objectives of the WGRISK task for advanced reactors and, to a certain degree, to new reactors can be summarized as follows:

As it is envisaged, ISAM promises to be a methodology that helps ensure the use of appropriate considerations to safety/risk aspects throughout the life cycle of advanced reactors. By putting the use of risk assessment and risk information into the center of the proposed methodology an important aim is to promote risk-informed decisions in the various life cycle phases.

In response to a question it was mentioned that ISAM does not propose particular quantitative safety objectives to be met. It was also discussed that the six System Steering Committees for the Generation IV reactors support ISAM largely. However, there is some concern as far as the level of effort and expertise needed to perform the proposed assessment. These concerns might have important implications for the way forward including the requirements for ensuring PSA quality.

It was clearly spelled out that for Level 2 PSA the core degradation mechanisms specific to the different reactor concepts have to be considered. Although there are noticeable differences in the level of knowledge for the different concepts, in general there is a lack of understanding needed to better model severe accidents due to the lack of experimental data and to the limitations of existing analysis tools. Developments of EOPs and severe accident management guidelines is also seen as an important condition to be able to better assess the capabilities and limitation of current level 2 PSA methodology for advanced reactors.

There were some interfacing discussions with the last workshop session in relation to the modeling of passive systems. In that last session the needs for improving analysis methods, tools and data were discussed at length. On the other hand, the example of the reliability analysis for the decay heat removal system in the 2400MWth GFR reactor witnesses an application and use of currently available techniques and tools (RMPS methodology) up to the level of quantification needed for PSA. Similarly, failure of natural circulation was modeled in the PSA of the advanced Indian PWHR too. Thus some analysts argue that the methodology is mature enough for useful and credible applications. Although a consensus was not aimed at and could not be reached at the workshop, there appears to be an agreement that meaningful analysis of passive systems is possible in the framework of PSA with considerations to the limitations of current methodologies, tools and data. In parallel, the analysis areas in need for further developments have also to be emphasized.

(3) Summary of Technical Session 3 (by J.J. Tong)

In this session, there are four presentations given by different organizations/countries.

The first presentation ("Applying Risk Insights in USNRC Reviews of Integral Pressurized Water Reactor Designs," M. Caruso, NRC-USA) gives the background of the framework which USNRC will use to more fully integrate the use of risk insights for the review of the SMR (Small Modular Reactor), and take the identification of risk-significant SSCs and other aspects of the design that contribute most to safety as the illustration. It concludes that the framework is a graded approach. The four-step process for determining risk significance of SSCs includes: Assembly of Design/Plant-Specific Information; Identification of Plant Systems and system features; Risk Significance Determination for System Functions; and Update Risk Significance Determinations as Necessary. NRC doesn't have any iPWR (integral Pressurized Water Reactor) licensing applications yet. Since there's no pool of experience peer reviewers, self-assessments are expecting. Challenges about the handling of new improvements, e.g., submerged valves, helical SGs (Steam Generators) are foreseen. The objective is to use PSA to help NRC doing its job more efficiently and effectively.

The second presentation ("Development of PSA Audit Guideline and Regulatory Model for SMART," N. Cho, KINS-Korea) summarizes the design features of the SMART (System-Integrated Modular Advanced Reactor, 330MWt) which is under development by KAERI for dual purposes of power generation and seawater desalination, and also the purpose to develop a regulatory PSA model in order to assure the technical adequacy of SMART PSA. Key technical issues identified during the development of SMART PSA include the modeling of PRHRS (Passive Residual Heat Removal System), and the insights from the preliminary quantification results. General standard modeling approach is used for PRHRS, but does have the phenomena related failures in the fault tree.

The third presentation ("Use of PSA in the Development of SMRs," A. Maioli, Westinghouse-USA) shares the Westinghouse experience of using PSA both in the design of AP1000 and IRIS (International Reactor Innovative and Secure, an Integral PWR under development, 200MWe with straight-tube steam generator). It indicates that a risk-informed framework within which PSA and the resulting risk insights can be used in the decision making process at various stages of the design needs to be developed. Challenges of using risk insights in the design include the coordination and interaction among PSA team, design team and the T-H team, epistemic uncertainty treatment, unique modeling problems due to the design (e.g., HRA, code abilities to model other than classic LWR scenarios, external events...), risk metrics and new applications such as risk-informed Emergency Planning Zone. CDF/LRF (Large Release Frequency) may be not of interest in the initial steps of the risk-informed design process other than system reliability.

The last presentation ("Achievement of the Level 1 PSA in Support to the CEA 2400MWth Gas-cooled Fast Reactor," M. Balmain, EDF-France) intended to define what could be the contribution of a level 1 PSA to support the design and safety demonstration by the application for the GFR, and also to exhibit the methodological trends for an efficient PSA model through the project life cycle. It presents with the example of using the relative results and a limited perimeter to support the design, and also another example of using the absolute results and enlarged perimeter. It reports that the design team may put their focuses on the key-points from the feasibility or technical points of view, e.g. the core or some components, so that the preliminary design of GFR presented a heterogeneous level of design for various components and support systems. The nature of the PSA model provides a good frame to link different

kinds of knowledge together and balance them. And PSA also led to the consideration of long mission time. It is foreseen that the use of PSA will be continued in the design of a new SFR based on the successful experience.

In general, three of the presentations in this session, including No.1, No.3 and No.4, are focused on the overall roles and applications which PSA played during the design and review of the advanced reactors. General common conclusions which can be drawn from these practices as well as the discussions followed are:

- The regulatory agencies have expressed explicitly their expectations or requirements to encourage the activities to integrate the use of risk insights more fully into the design and safety review;
- PSA has been used and are also highly recommended to be used from the very early stage of the design phase. The nature of PSA can provide a frame for the synthesis of the different kinds of available knowledge (T-H, neutronics, and mechanics, etc.) at the design stage;
- The continuous iteration and interaction among PSA team and design teams are recognized to be of very important necessity to the success of risk-informed processes;
- Epistemic uncertainties due to lack of design information, unknown phenomena, plant-specific hazards, data, etc., may be larger than that from existing reactors, and will impose a significant challenge to the decision making.

One presentation raised another issue about establishing a regulatory PSA model for confirmatory check of the technical adequacy during the design certification phase. Since technical adequacy of a design phase PSA is an essential part of risk-informed decision making, the regulatory PSA model which is independent from the applicant's model may be one of the possible choices that some countries may endorse.

(4) Summary of Breakout Session 1 (by K.I. Ahn)

This session includes both a summary review of the questionnaire responses and key discussion points of the day's technical paper sessions.

(4-1) Summary of Questionnaire Answers Survey on PSA for Advanced Reactors by K.I. Ahn

The questionnaire answers on PSA of advanced reactors collected from the twelve countries (16 organizations) spanned wide spectrum of reactor types and associated programs, including new/evolutionary reactors (e.g., EPR, AP1000, ABWR, APWR, ESBWR, APR1400, etc.) as well as advanced reactors in the conceptual or preliminary design stage (e.g., SFR, LFR, GFR, HTGR, iPWR, SMR, SMART, etc.). In order to draw out common-interest PSA issues required specially for advanced reactors, first of all, it seems necessary to more clearly discriminate the underlying difference between new/evolutionary and advanced reactors among member countries. Based on the questionnaire answers, major preliminary observations and findings were presented to the workshop participants and are summarized as follows:

Regarding the use of PSA in the design and licensing stages of advanced reactors.

- While a few countries are limitedly using for the conceptual or preliminary design stages of advanced reactors, more efforts are currently being focused on indentifying and resolving PSA issues for the designer and regulatory bodies;
- While a few questionnaire answers are addressing the potential use of regulatory approaches where risk plays a greater role, these activities have not yet led to actual changes in regulation and many other countries that answered are not developing new approaches for advanced reactors and relevant PSA technologies yet;
- While the questionnaire answers express many technical and regulatory issues which should be resolved for advanced reactor designs, many of them do not seem to think that advanced reactors pose fundamentally different types of challenges and that methodological work for some specific areas (e.g., digital systems, passive systems, and HRA, etc.) is expected to be generally applicable for a wide variety of designs.

Regarding the ability of current PSA to address PSA for advanced reactors,

- Many questionnaire answers take into account a direct extension of the existing PSA methods to advanced reactor systems (e.g., reliability databases, development and application of appropriate PSA models for advanced reactors);
- The questionnaire answers seem to express different viewpoints on scope of hazards, quality, and framework of the PSA to be treated in advanced reactors, more specifically (a) while some respondents express the applicability of Level 1/2/3 for some reactor types, (b) others have no issue; while some respondents expect treatment of all modes and all hazards, others are more limited; and (c) while some respondents think current ET/FT technology is fine, some are doing research, some are using different methods for certain problems. So far, those items remain possible to discuss (in the conclusions for this workshop) the extent to which workshop discussion helped.

Regarding the potential use of advanced PSA methods and tools for advanced reactors,

- While some questionnaire answers address development of new methods-related work for challenging topics (e.g., DI&C (Digital I&C), HRA, and Level 2 under advanced design features), they do not seem to be aimed at specific reactor types;
- A few questionnaire answers express the use of the non-ET/FT methods/tools as a mean to more explicitly tie phenomenological modeling into the PSA (e.g., RMPS, Dynamic PSA, DDETs). While those methods have a potential value for their application to advanced reactors, there is no clear guidance on how to incorporate into the PSA framework for advanced reactors yet;
- A few questionnaire answers also address the need of advanced reactor-specific SA analysis models, definition of source terms risk, and their countermeasures which could be critical in determining the risk of advanced reactors. While they could be involved in the realm of PSA, however, there seems not currently exist any consensus on how to take into account those issues for some advanced reactors and on the level of depth to take into account. So far, those items

remain possible to discuss (in the conclusions for this workshop) the extent to which workshop discussion helped.

Based on these results, the potential topics of interest for further discussions in the workshop may include

- Scheme to determine technical acceptability of PSA for advanced reactors (including the ASME/ANS non-LWR standard) and provide its implementation process;
- Establishment of surrogate risk metrics and target for advanced reactors;
- Compliance of the PSA with defense-in-depth principle in the regulation framework;
- Advanced reactors-specific accident phenomena and passive safety system reliability, reliability databases, human and digital system reliabilities, accident sequences and event classifications for PSA modeling and adequacy of current phenomenological models to support the analysis, and aggregation of the risk from different hazard types into the plant risk in an integrated or technology-neutral way;
- Assessment for the possibility of potential severe accidents in the pre-conceptual design phase of advanced reactors;
- More consolidated ways to collaborate with the other international programs (e.g., OECD/CNRA-WGRNR, GIF-RSWG, and IAEA CRP on passive safety systems reliability).

(4-2) Summary of the Day's Presentations and Key Discussion Points

Summaries and highlights of the Day 1 Sessions (especially dedicated to PSA for advanced reactors) were introduced by each session chair (Session 1 by N. Siu, Session2 by A. Bareith, and Session 3 by J.J. Tong), and key points made in the discussion of those sessions are as follow:

- PSA community needs to challenge itself in identifying scenarios on what can go wrong for new designers;
- The targets of risk for advanced reactors should be determined as soon as possible;
- Quantitative PSA results may not be very useful at the conceptual design stage of advanced reactors but PSA is still reasonable in providing a systematic approach;
- Security issues should be considered for advanced reactors;
- Some groups are wrestling with the question as to whether the PSA state of the art is adequate to support a specific application. Guidance would be helpful;
- Some surprise that there was not much discussion on issues and phenomena where tools used did not do very well. This would indicate where more work would be helpful.

2.2 Day 2 (21 June)

(1) Summary of Technical Session 4 (by J.M. Lanore)

In this session three papers were presented: two papers relating to I&C modeling in PSA, and a more general paper relating to the application of Design-Reliability Assurance Program.

The first presentation ("Application of Fault Tree Methodology to Modeling of the AP1000 Plant Digital Reactor Protection System," David Teolis, Westinghouse-USA) introduced a real example, the characteristics for modeling of I&C by fault tree methodology, taking into account hardware and software failures, and CCF corresponding to these different failure modes. The paper mentions the difficulties for finding data. However the model is being developed and is intended to be integrated in the PRA model.

The second presentation ("I&C Modeling in the IRSN EPR Level 1 PSA" J. Delache and G. Georgescu, IRSN-France) introduced a real example of I&C modeling by fault tree methodology, taking into account hardware, software, CCF, support systems (electrical and ventilation). The model was reviewed by I&C specialists; this model is rather simple but still has hundreds of fault trees. CCF contribution is dominant. The objective of this work is to analyze the PSA proposed by EDF for Flamanville3 EPR design. A particular objective is to assess the importance of a backup system.

The discussions following these two papers were very similar: the main issues are firstly the ability of the models to identify dependences due to I&C, in particular dependencies between an initiating event (due to a spurious signal) and failures of safety functions (in principle the fault tree modeling is a potential solution for this question). The second issue is the problem of data, which are still very difficult to find, especially for software and CCF failures.

A general comment is that although there is no real methodology consensus for I&C modeling and quantification, some tentative approaches are developed and integrated in PSAs. Another general comment is that digital I&C is not really specific to new plants, but due to the improved general safety level the role of I&C is increasing and becomes a potentially dominant issue.

The third presentation ("Analysis of Design-Reliability Assurance Program in ACP600 Application," Huang Zhichao, CNPE-China) introduced D-RAP (Design-Reliability Assurance Program), which is a formal management system of plant performance and safety information, applied to ACP600 (a new GEN III advanced reactor). The conclusion is that D-RAP is a useful tool for new reactor development, combining deterministic and probabilistic analyses advantages.

Moreover an answer to a question indicates that this tool contributed to the definition of several safety improvements. The discussion was also related to the treatment of passive systems, and this point was discussed more widely during other sessions.

(2) Summary of Technical Session 5 (by K. Ahn and G. Georgescu)

Four papers were presented in this session: two papers addressing new and improved modeling employed in a severe accident analysis code, MAAP5, and two papers related to the Level 2 PSA (one for Japanese SFR and the other for PHWR employing some partly uncommon features).

The first presentation ("In-Vessel Retention Modeling Capabilities – IVR - in MAAP5," Quan Zhou, FAI-USA) introduced new models and improvements made in MAAP5.01 specifically to address complex phenomena important for IVR (In-Vessel corium Retention). The key parameters affecting the IVR success are the metal layer emissivity and thickness of the top metal layer, which depends on the amount of steel in the oxidic pool and in the heavy metal layer. These models important to the IVR evaluation were implemented in MAAP5.01 and were successfully tested for the AP1000® passive plant. He said that the AP1000® plant results demonstrate how MAAP5.01 can be used to evaluate IVR and to gain insight into responses of the lower head during a severe accident. Finally, he emphasized that this was one of the first integrated, transient calculations for evaluation of IVR and the MAAP5.01 will be used as a platform of severe accident simulator for the AP1000®.

The second presentation by Quan Zhou ("MAAP5 Modeling Capabilities for Initial Plant Transients and Shutdown States, and Application to Shutdown PSA and Full Scope SAMG Covering All Plant States for Operating and New Plants") introduced major improvements made in the latest MAAP5.0.1 code to simulate initial transients and shutdown conditions in nuclear power plants, status of development of the full scope SAMGs covering all plant operating states including Shutdown SAMG (SSAMG) integrated into at-power WOG (Westinghous Owners Group) SAMG to form a complete symptom-based SAMG package applicable to all POSs (Plant Operational States), and capabilities of the MAAP code simulating non-severe accident transients demonstrated with selected AP1000 transients. He also emphasized capabilities of MAAP5 as an appropriate tool for severe accidents and key steps of the Shutdown SAMG development, and to execute long term non-severe accident transients and PRA Level 1 success criteria calculations. Nevertheless, a few challenges and uncertainties still remain for the followings:

- There are specific challenges to thermal-hydraulic codes for low power and Shutdown plant states; verification of codes, model modifications and improvements;
- Regarding the severe accident phenomenology, the remaining uncertainties, and also the diversity of accident scenarios considered, the development of Shutdown SAMG is still a very complex activity;
- For SSAMG validation, operator and TSC (Technical Support Center) training exercises and upgrades to Full Scope Simulators are required to support high fidelity simulation of shutdown states, including low reactor inventory states, open reactor and open containment states, refuelling operations, and spent fuel pool accidents.

The third presentation ("Development of level 2 PSA Methodology for Sodium-Cooled Fast Reactors," T. Suzuki, JAEA-Japan) introduced the current status of evaluation-technology development of Level 2 PSA for SFRs made by JAEA to systematically assess the phases/sequences to be evaluated in Level 2 PSA: development and verification of computational tools for the material-relocation phase and the ex-vessel

accident sequence, and consolidation of the technical basis for constructing phenomenological event trees, in which the information on the related analyses/experiments were compiled so as to determine the event progression and branch probabilities within the event trees. The conclusions of the paper are summarized as follows:

- JAEA newly developed MUTRAN and SIMMER-LT codes in order to evaluate the long term behaviors of the material-relocation in the degraded core. These tools enabled systematic simulations of the material-relocation phase;
- JAEA also improved CONTAIN/LMR code taking into account the feature of SFRs and verified the analytical models in CONTAIN/LMR by utilizing the new experiments such as sodium-concrete reaction test. As a result, the CONTAIN/LMR code with the improved models enabled appropriate simulations of the ex-vessel accident sequence taking into account the feature of SFRs;
- The general information needed for the Level 2 PSA of SFRs (including the construction of event trees) was compiled as a technical data basis, in which the dominant factors having significant effects on the event progression were corresponded to the related analytical/experimental results.

The last presentation ("PSA Level 2 as Element of an Integral Safety Assessment before Plant Commissioning," H. Löffler, GRS-Germany) introduced the experience with CNA II (PHWR reactor under near completion in Argentina) with respect to PSA Level 2 for new and advanced reactors. He emphasized that although CAN II is not a recent design, it has some partly uncommon features, so that there is a certain resemblance to performing a PSA for a new design. Additional focus was on the definition of the two interfaces to PSA Level 1 and Level 3, and key issues taken into account in defining release categories. For the Level 2 PSA, both MELCOR code and EVNTRE methodology were used for deterministic accident simulation and Probabilistic accident progression analysis, respectively. Experience gained from the PSA Level 2 for CNA II was highlighted as follows,

- Existing deterministic (MELCOR) and probabilistic (EVNTRE) methods and PSA guidelines in general are flexible enough to analyze new or especially uncommon reactor designs;
- Plant specific design details may require specific analyses or estimates beyond present code capabilities, and they can largely determine the PSA results;
- If PSA level 3 is required, significant uncertainty exists regarding the definition of source terms and the selection of representative or most "challenging" cases;
- In particular the behaviour of Iodine is still not covered satisfactorily by state-of-the-art models in MELCOR. Additional effort was needed in the event tree to represent gaseous iodine;
- A precise definition of interfaces between the PSA levels supports understanding among different PSA teams and enables parallel work on the different levels. A direct transfer of MELCOR results to the PSA Level 3 team is a simple and useful approach.

(3) Summary of Technical Session 6 (by Reino Virolainen)

The first presentation ("Regulatory Assessment of the PSAs for the UK-EPR and AP1000 Reactors in the UK," A. Gomez Cobo, NII-UK) gave a detailed procedure to conduct a reactor type specific regulatory

assessment, "Generic Design Assessment (GDA)" which includes also a PRA review. The GDA is running through four steps, from general to detail.

PRA is mainly reviewed during GDA step 3 focused on methods, techniques and scope. This corresponds to a generic review step in a typical PRA review procedure. The main review is performed during GDA step 4 but the review is not focused on each event tree, fault tree and data in detail but a representative sample is selected. This corresponds partly to a detailed review step in a typical PRA review procedure. However the assessment does not pursue an in- depth review level but the Risk Gap Analysis plays an important role.

Because of the Fukushima aftermath the GDA is exposed to changes. The presentation posed also interim results and conclusions of AP 1000 and UK EPR assessments. Because of the Fukushima accident the results of the GDAs are exposed to changes. Potential needs for changes in the GDA are foreseen.

The GDA resembles a kind of reactor type specific pre-licensing. However before start of nuclear safety related construction, the licensee shall ensure that the existing PRA is representative and sufficient insights into the vulnerabilities and strengths of the unit are presented.

Before delivery of the mechanical, electrical and I&C systems, structures and components to the site, the licensee shall provide updated PRA including all technical assessment findings.

- Before fuel into the site: Updated PRA including as-built and as operated information;
- Before power rise: Full scope risk monitor. The paper also noted that UK-ONR (Office for Nuclear Regulation) has developed a technical Assessment Guide on PRA that has proven valuable on their reviews. This Guide was developed using available ASME standards and IAEA TECDOC 1511.

The second presentation (“Lessons Learned from IRSN Review of Flamanville 3 Level 1 PSA,” G. Georgescu, IRSN-France) raised several important findings:

- The design phase PRA was based on partial design information;
- Updated design information documentation is necessary for better traceability;
- CCF: the assumptions of full diversification of redundant components should be better justified;
- Loss of ultimate heat sink: independence between main heat sink and secondary heat sink should be better justified;
- I&C modeling: Better justification of FMEA (Failure Mode and Effect Analysis) for different sub-systems and components;
- HRA: Correct identification and justification of dependencies;
- Sump clogging: Should be modeled in PRA;
- Spent fuel pool: the assumptions used in quantification of recovery actions should be traceable and better documented;

- For the decision making: Impact of incomplete information should be assessed and iterative approach should be applied.

STUK had similar conclusions in its regulatory review of OL3 PRA and this was noted in the discussion.

The third presentation ("Role of PRA in New NPP Projects in Finland," Ari Julin, STUK-Finland) gave a generic survey of the risk informed licensing process and insights into the plant changes performed in the OL3 EPR design based on risk information. As set forth in the legislation, a mandatory pre-requisite for a Construction license is acceptable with full-scope Design Phase PRA and few risk-informed applications and for an Operating Licensee Application an acceptable full-scope PRA and several risk-informed applications. The presentation highlighted some key point in the PRA reviews:

- Staff instead of contractors perform the PRA reviews;
- Importance of checking the PRA results as design evolves;
- Aim to have balanced design;
- The quantitative design objective includes also spent fuel pool.

The last presentation ("Introduction of PSA Team Works in CNPE," Zhao Bo, CNPE-China) gave a general survey of NPP projects, documents and standards used and PRA techniques. PRA team was introduced too.

- In China, there are 28 new build projects in progress;
- IAEA , ASME, and NUREG documents, reports and standards are used to support PRA projects;
- In modeling small event trees and large fault tree are applied;
- PRA data is generic;
- Post-Fukushima conclusion is that more attention has to be paid to external events. So far PRAs include only internal initiators.

CDFs of analyzed NPPs are in range of 5.0×10^{-6}/y ~ 2.0×10^{-5}/y including power and shut down operations.

(4) Summary of Breakout Session 2 (by G. Georgescu)

This session involved a summary presentation of the answers on the survey on "PSA in the frame of Design and Commissioning of New NPPs, the presentation of the summary of the technical presentations of the day and general discussions.

The questionnaire was answered by 16 organizations, referring to the EPR, AP1000, ABWR, APWR, ESBWR new designs as well as to advanced small modular reactors (iPWR, HTGRs).

The topics of most interest for the workshop mentioned by the respondents were:

- Reliability analysis of digital I&C and software reliability;

- Assessment of internal and external hazards;
- Risk-Informed application for new plants and use of PSA throughout the reactor design cycle;
- Role of PSA in licensing new NPPs;
- Reliability analysis of passive systems.

Regarding the regulatory role of PSA the answers show that in general, the Level 1 and Level 2 PSA are considered essential or mandatory for construction and operation of new reactors.

In general, the design stage PSA is a full scope level 1 and level 2 (internal events, internal and external events hazards) for power and shutdown states. The spent fuel pool is not always included. The design PSA is not always site specific. The computerized PSA model is not always available to the regulatory or TSO (Technical Safety Organizations). Some regulatory organizations develop own PSA models.

The main roles of the PSA during the development of the plant design identified by the respondents are:

- Safety demonstration;
- Supporting the choice of design options;
- Well-balanced safety concept;
- Defense in depth assessment /multiple failures conditions;
- Appreciation of the improved safety level compared to existing plants.

The main fields were risk-informed applications are performed are:

- Technical specifications;
- Safety classification of SSCs;
- In-service testing;
- Online preventive maintenance;
- Emergency operation procedures;
- In-service inspection;
- Operator training program / simulator training.

In general, the risk-informed applications are not required by safety authority. Only 4 countries have legislation in this respect.

The respondents recognized that in general the design PSA has important uncertainties. The data uncertainties are analyzed quantitatively using uncertainties propagation methods. For the others non-quantifiable uncertainties, sensitivity analyses are generally performed. Always the limitations of the PSA and main assumption are indicated and discussed. Conservative safety margins are in general considered in the design PSA. The design PSA is developed in general by using international guidelines are used

IAEA, NUREG, ASME, etc. In some cases, country specific guidelines are also used. No specific guidelines for new reactors were mentioned in the answers.

The international groups dealing with that PSA for new reactors mentioned by the respondents are: MDEP (Multinational Design Evaluation Program) (EPR, AP1000), EPR Family Group, WGRISK, WANO, and CANDU Senior Regulator Groups.

The summary of the answers to the questions on PSA Level 1 technical aspect are the followings:

- Initiating events list. The initiating events list is mostly developed based on similar reactors PSA and on generic lists. Some design specific analyses are also performed (system analyses/FMEAs and Master Logic Diagram). In general, few new initiating events specific for the new design were identified;
- PSA supporting studies. In general, specific support studies are performed. Also the Safety Report analysis / design basis reports are used as well as studies of similar reactor PSAs;
- Reliability data. Various sources of data (NUREG/CR-6928, T-Book, EIReDA, NUREG/CR-5497, IAEA-TECDOC-478, IEEE-500, ZEDB, etc.) were mentioned. For evolutionary / limited experience components, ancient components data, supplier's information, supporting reliability evaluations or expert judgment are used;
- New / evolutionary design features modeling. In general these features are reflected by safety improvement. Some new initiating events (like spuriously I&C) were also identified;
- Availability of Tech-Specs and preventive maintenance procedures. In general Tech. Spec. and preventative maintenance procedures are not available, the PSA being based on simplified information;
- HRA. In general, generation 1 methods are used for HRA (THERP (Technique for Human Error Prediction), ASEP (Accident Sequence Evaluation Program)). In some cases, the using of generation 2 methods is foreseen in the future. The accident procedures are not available for the actual design PSA development the respondents identified the need of detailed accident procedures for the next stage PSA. Simulators are not available; in the future the using of simulators is in general expected;
- External hazards. In general, screening analyses were performed. The answers show that the lists of hazards to analyze are different for different projects. The future possible hazards evolution, generally, is not taken into account. Only few external hazards PSA are available, the hazards being generally treated with other methods (bounding analyses, simple quantification). In general, seismic margins assessments are available at the design stage. Full seismic PSA is expected later (requested by some countries);
- Internal hazards. Internal fire and internal flooding are generally modeled in the design PSA. NUREG/CR-6850 is used generally for fire PSA. Heavy load drops were assessed by one project.

The summary of the answers to the questions on PSA Level 2 technical aspect are the followings:

- Generally a Level 2 PSA is available. The Level 2 is integrated with Level 1 PSA, but generally does not include the spent fuel pool. Some internal hazards are included in the Level 2 PSA;
- Severe accident progression support studies. In general, specific support severe accident progression studies are performed (MAAP, Crystal Ball, MELCOR, ASTEC, GOTHIC, TEXAS-V, LS-DYNA, and FLOW-3D). Very limited experiments were performed;
- New severe accident reactor features modeling. In general, the new severe accident reactor features are considered in the Level 2 PSA.

The summary of the answers to the questions on Consequences analysis /PSA Level 3 technical aspect are the followings:

- Several Level 3 PSA were performed for reactor at the design stage;
- Sites specific aspects: In general bounding assumption are used;
- Emergency actions. In general bounding assumption is used, i.e. the emergency actions are not typically considered in the design stage PSA.

The discussions pointed-out the following important aspects:

- The need for phenomenological code developments to address design specific issues (e.g., potential thermal radiation to the containment);
- Challenges of using long running code models in the PSA;
- GDA represents practices used in UK and USA but not necessarily in other countries;
- Some regulators and TSO may not have a direct access to the PSA models; this is a challenge;
- UK ONR highlighted the value of the using of a generic Level 3 PSA in early stages of the design cycle;
- IAEA sees Finland's use of PSA in construction process is very efficient and effective;
- One participant asked if the Level 3 goals should be used to demonstrate the safety of new reactors. The group has widely varying viewpoints.

2.3 Day 3 (22 June)

(1) Summary of Technical Session 7 (by G. Georgescu)

The first presentation ("Probabilistic Modeling of Passive Design Features," F. Sassen, Westinghouse-Germany): The current PSA-guidelines in Germany can in some aspects only be applied to LWRs with active safety systems. The application of the relevant PSA-rules on modern future reactor types (e.g. high temperature reactors) demands an interpretation of these rules. The PSA for advanced light water reactors with passive safety features has increased demands on data for the event tree and fault tree modeling. The PSA-model for a "passive" safety system not only needs to model the few active powered components of the system, but all passive components must be consider in fault tree, if they contribute to the same extent

to unavailability of the system. The new challenge for the modeling of passive systems thus is that the failure rates for both the active components and passive components must be defined. For the passive systems for example the failure of pipes and tanks at the start of the system function should be considered as well as the wrong standby system alignment and the damage mechanisms that cause moving parts, which must keep their original position, change. As an example, the model of the AP 1000 Core Makeup Tank system was presented. The paper addresses potential failure of hardware components but does not addresses potential contributions due to uncertainty in phenomena arguing that the design has large safety margins.

The second part of the presentation referred to the requirements for PSA modeling of other reactor types than light water reactors. Valid PSA guidelines apply to a large extent to plants which are analyzed "as-built-as-operated". Since for non-LWR plants usually even during the conception phase a PSA is required, a corresponded data base is missing. This leads to demanded scopes for uncertainty and sensitivity analysis which may not be fulfilled with a reasonable effort. Because of the utilization of new materials and due to incomplete knowledge on phenomena partially success criteria can only be established with some uncertainty, as is known from Level 2 PSAs. Besides the question whether such systems are fit for licensing from the deterministic point of view, this causes increased demands for the PSA.

The second presentation (“Uncertainty Analysis Methods for Estimation of Reliability of Passive System of VHTR,” S. J. HAN, KAERI-Korea): An estimation of reliability of passive system for the VHTR PSA is under development in Korea. The essential approach of this estimation is to measure the uncertainty of the system performance under a specific accident condition. The uncertainty propagation approach according to the simulation of phenomenological models (computer codes) is adopted as a typical method to estimate the uncertainty for this purpose. The paper introduced the uncertainty propagation and discussed the related issues focusing on the propagation object and its surrogates. To achieve a sufficient level of depth of uncertainty analyses results, the applicability of the propagation should be carefully reviewed. For an example study, Latin-hypercube sampling (LHS) method as a direct propagation was tested for a specific accident sequence of VHTR. The presentation discussed the obtained insights (benefit and weakness) to apply an estimation of reliability of passive system.

The third presentation (“Problems Facing the Use of Passive Safety Systems,” L. Burgazzi, ENEA-Italy) referred to the current state of the art in the reliability of passive systems and identify the critical issues which need further consideration.

The paper stress that, due to the specificities of passive systems that utilize natural circulation (small driving force, large uncertainties in their performance, lack of data, etc.), there is a strong need for the development and demonstration of consistent methodologies and approaches for evaluating their reliability. Recently, the development of procedures suitable for establishing the performance of a passive system has been proposed. In order to get confidence in the achieved results, it is necessary to reduce the level of uncertainty pertaining to the passive system behavior, and in particular the phenomenological uncertainty. The determination of the dependencies among the relevant parameters adopted to analyze the system reliability is also essential. The study of the dynamical aspects of the system performance, because the inherent dynamic behavior of the system should to be characterized, is another important aspect. It is

also necessary to compare the passive systems against the active systems, in order to evaluate the economical competitiveness, while assuring the same level of safety.

Summary of discussions: Many new reactor designs use passive safety systems. On the other hand, in the available design PSA the passive systems models considers only the failure of the systems components (pipe break, spuriously actuation of valves, etc.), the "failure" of the phenomena (natural circulation for example) not being generally taken into account. Some group members expressed the opinion that the scenario dependent situations which can lead to a combination of conditions for which the passive system function cannot be performed should be identified and modeled explicitly in the PSA. Some other group members expressed the opinion that parametric models can be used. The modeling of passive systems in the PSA raised also the question of the impact on other PSA aspects. For example, the functioning of the passive systems for long term accident scenarios should carefully be analyzed. Another important issue is the treatment of the physical and thermal hydraulic data uncertainties as well as of the uncertainties in the behaviour of the passive systems. The group highlighted also the fact that the existing thermal hydraulic codes may not be completely applicable for the analysis of the passive systems behaviour in the context of developing design PSA support studies. The international activities performed up to now on the passive systems reliability didn't treat explicitly the modeling of the passive systems in the PSA. For the group, recognizing that have been no analyses indicating the relative importance of dealing with this issue as opposed to other sources of uncertainties (e.g. digital I&C reliability) the passive systems reliability and modeling in the PSA is an open issue which needs more efforts.

(2) Summary of Technical Session 8 (by T. Leahy)

This session consisted of four presentations focused on relevant activities by national and international organizations, and on the topic of PSA technical adequacy for advanced light water reactors. Because the presentations were quite diverse in their scope and focus, broad, cross-cutting conclusions were not apparent. Nonetheless, presenters made a number of important points, and several notable results and conclusions arose from the presentations and subsequent discussion during the session.

The first presentation ("NRC Activities Concerning PSA for New and Advanced Reactors," N. Siu, NRC-USA) outlined the status of new and advanced reactor design reviews, relevant guidance regarding the use of PSA in these reviews, and certain related NRC research activities that are in progress. It was noted that the licensing process explicitly calls for the use of risk insights, and for comparison of risk with established safety goals and with existing plants. In this regard, it was specifically noted that the NRC has determined that existing safety goals and risk guidance are sufficient for new plants. In the longer term, NRC will be developing a new "risk informed framework" for advanced reactors. Significant NRC research programs are being conducted in the areas of High Temperature Gas Reactor issues, Digital Systems, and Human Factors Analysis for new and advanced Reactors.

The second presentation ("ASME/ANS Standards for ALWR and Advanced Non-LWR PRA: Status and Challenges," N. Siu, NRC-USA) provided an overview of the status of developing guidance and standards for advanced reactor PSAs. It was noted that key aspects of useful standards cover the risk assessment application process, PSA technical requirements, configuration control, and peer review to assure technical quality. Echoing a major theme of the entire workshop, early use of risk insights in

design, construction, and "pre-operation" is desirable. Several approaches to develop the ALWR standard are under consideration, but no consensus has yet emerged. The non-LWR standard is further developed, and a draft standard has been developed. Review and comment is in progress. Both technical and non-technical challenges were discussed.

IAEA activities were discussed in the third presentation ("Insights from Recent Activities on PSA Being Pursued by the IAEA," I. Kuzmina, IAEA). This presentation provided updates on several recent or ongoing IAEA activities including further work in the definition and application of the principle of "defense in depth." The use of PSA in assessing defense in depth was briefly described, and the importance of PSA quality and independent peer review was emphasized. The availability of IAEA peer review services was also noted. This presentation also reported on the IAEA's April 2011 Technical Meeting on Safety Goals in Application to Nuclear Installations. Results, conclusions, and agreements established during that meeting will be outlined in a meeting report that is currently under preparation. Finally, it was noted that the IAEA is developing guidance on the use of Integrated Risk Informed Decision Making (IRIDM).

The final presentation of the session ("Assuring PSA Technical Adequacy for New Advanced Light Water Reactor Designs," A. Maioli, Westinghouse-USA) described some of the challenges of using PSA to design and license new technologies, and emphasized the importance of PSA technical adequacy in light of those challenges. It was recommended that in the design stage, PSA is best used to identify vulnerabilities and to help identify opportunities for possible design improvements. In the construction stage, PSA is used for equipment procurement, development of technical specifications, and training of plant personnel. In pre-operational and early operational stages, it was recommended that the PSA be used to develop regulatory oversight programs and to validate design assumptions. When used for these important purposes, PSA quality and technical adequacy are essential. Practical difficulties of finding knowledgeable experts to conduct peer review for novel technologies were noted.

Perhaps the main unifying thread of Session 6 was the idea that PSA quality and technical adequacy are critically important when the PSA is to be used in reactor design and licensing. Because new and advanced reactors are likely to use innovative technologies, with which we have relatively little experience, this need is greatly magnified relative to PSA applications for current plants. Collectively, presenters in this Session made the point that appropriately focused research in selected areas, careful thinking about both qualitative and quantitative safety goals, well conceived PSA standards, and independent peer are important allow PSA to fulfill its potential in supporting design and licensing.

(3) Summary of Technical Session 9 (by L. Burgazzi)

This session included 4 papers which addressed different areas:

- Lessons learnt from New and Advanced Reactors in Russia, presented by V. Morosov (Atomenergoproekt, Russia),
- Risk-informed, Performance based Safety-Security Interface, presented Farouk El-Tawila (FANR, UAE),

- Automatic fault tree generation in the EPR PSA project, presented by Natalie Villatte (EDF, France),
- Investigations of inter-system common cause failures, presented by Philippe Nonclercq (EDF, France).

The first paper focused on new evolutionary VVERs which feature new systems, basically passive systems such as hydro-accumulators, passive residual heat removal system and fast injection boron system to achieve redundancy and diversity of main active systems. Preliminary analysis revealed a decrease in both CDF and LERF (Large Early Release Frequency) values as compared with current operating VVERs.

Some of the open issues highlighted in the presentation concern (i) adequacy of regulatory approach, (ii) probabilistic safety targets definition, (iii) PSA scope, (vi) uncertainties induced by new designs, (v) consistency and need of interaction between design and PSA teams leading to an iterative PSA process, (vi) longer mission time, (vii) human reliability during longer time, (viii) safe end states, (ix) homogeneity and consistency of data coming from different sources as there are no specific data for new designs. The paper mentioned also some considerations following the Fukushima accident to be taken into account in PSA such as combined external events, multi-units scenarios and extension of SAMG.

During the discussion, contribution of passive systems to the risk reduction was confirmed. Also the importance of communication between PSA and design teams was noted.

The second paper addressed the safety-security interface which refers to the actual or potential interactions that may adversely affect security due to design or operation activities (e.g., maintenance) or vice versa. This interaction is recommended to be included in a PSA framework at the early stage during site selection and design in order to optimize it in compliance with safety and security requirements. Means to enhance synergy of safety, security and emergency preparedness are recommended in order to assure protection of the workers, public and environment. A risk-informed security analysis framework was proposed aiming at broadening security-related event scenarios, increasing the number of mitigation alternatives, adding greater realism to the construction of the sequences of events and considering similar elements as those addressed in the safety assessment.

During the discussion of this paper concern was raised on whether PSA should be a confidential security tool not open to every analyst and hence limiting the safety culture. One proposal to overcome this difficulty is to foresee two versions, a restricted one including the safety-security interface and the other one limited to safety.

The third paper presented a tool (KB3) developed by EDF for automatic fault tree generation to be incorporated within the main tool (RiskSpectrum). This tool which is used in conjunction with a knowledge basis (electrical, thermal-hydraulics and I&C) is particularly suitable to overcome some difficulties such as complexity of the systems, different level of experience of PSA practitioners and dispersion of PSA teams in different places. The tool was stated to be flexible, effective and beneficial to the safety analysts as it provides diagrams, homogeneity between the fault trees, and allows better

traceability and control of modeling. However, some improvements are needed in terms of fault tree readability, export to RiskSpectrum and handling of the tools.

During the discussion, concern was raised regarding the loss of learning and knowledge which might be induced by the use of automatic tools as the act at model construction is important in helping analysts understand how a system works and how it can fail.

The fourth paper presented investigations of inter-system CCF through three studies on EDF 900 MWe pumps and motor operated valves, and EPR 10 kV breakers. These investigations used a methodology based on NUREG/CR-5485 and the related French PSA fundamental safety rule. The methodology includes 4 steps: (i) analysis of similarities in design, operation, environment and cause of failure, (ii) search for CCF in the operating experience feedback, (iii) qualitative and quantitative analysis of the possible impact of multiple failures with Risk Achievement Worth Cumulative Factor (RAWC), (iv) modeling of new CCF groups in the model. The results for EDF 900 MWe pumps and motor operated valves, and EPR 10 kV breakers showed a small risk impact of inter-system CCF.

(4) Summary of Breakout Session 3 (by A. Amri)

During this session, the participants were invited to ask questions or to provide any comment related to the papers presented during the day. The main questions, comments and insights are highlighted below:

- The reliability of passive systems may be impaired by external hazards (e.g., external high temperature); hence, one participant recommended to include the effect of external hazards on passive systems;
- As for the failure of passive systems by physical phenomena change or degradation, one participant expressed whether we may be able to include such a failure in a fault tree. Some of these failures may be addressed by design; for others, there is a need for Thermal-hydraulic community and PSA community to work together in order to get better understanding and to develop an appropriate method to address them;
- Another participant wondered whether we need a specific PSA and specific tools to address long time scenarios including later recovery actions;
- One participant underscored that there is no consensus to address the reliability of passive systems which may fail through physical phenomena degradation (category B); he expressed his personal opinion on how to address and for which important uncertainties remain by considering a fault tree and by assuming the failure of the system/ sub-system impacted by this degradation (e.g., effect of non-condensable gases = assume failure of venting, degradation of heat transfer coefficient = assume heat exchanger plugging). Others did not agree to say in the report that the issue is difficult and there is no consensus, so we cannot do anything as we can at least try to have some order of magnitude. They see in the method of uncertainty propagation method a promising one which should be further explored, e.g., through an international effort to address major issues in this method (robustness of system codes, uncertainty methods, etc.);

- A participant raised the concern whether too much standardization, harmonization, consensus model might prevent us to learn more as being outside the standard mode pushes us to investigate more and to learn more;
- Several comments were provided regarding data, e.g., use generic vs. specific data and influence on CDF; use of data from different sources and the induced uncertainties;
- In general, the participants found the workshop very interesting and useful as it had shown that studies and data exist, and that they may use its outcomes in their guidelines.

3. CONCLUSIONS

A wide spectrum of presentations and discussions on the PSA for new and advanced reactors were made during the three days workshop of June 20-22 2011, including current practices among member countries (e.g., analysis methods, tools and relevant data), efforts to improve technical problems, and potential challenges to the use of the risk-informed decision makings in design improvements of new and advanced reactors and related potential regulation processes, and technical practices according to the basis of these challenges.

The workshop participants also paid particular attentions to the necessity of more guidance to ensure the quality of the PSA for new and advanced reactors (like ASME/ANS LWRs and non-LWR standard) and peer-review process. The capability of the current PSA methods and applications in the frame of new and advanced reactors PSAs, as well as the potential areas for future improvements were also addressed by the participants, whose major concerns included passive safety system reliability, human reliability, and digital system reliability, new and advanced reactors-specific risk assessment methodology and relevant computational tool, and safety-security interface, etc).

The workshop played a great role in sharing the current state-of-the art on the PSA of new and advanced reactors, and points of interest among member countries. Main findings obtained from the workshop are as follows:

- For new reactors, the role of PSA is more important and more formalized comparing with exiting reactors. The PSAs are being used in the design of new reactors for purposes such as balance between accident prevention and mitigation features of the design, demonstration of safety, identification of design vulnerabilities and improvements, and comparison with the risk of existing plants, etc.
- For advanced reactors, the role of PSA is also being regarded as an essential tool for safety improvement and comparison of reactor designs at the conceptual or preliminary stages, but their practical use is at the early stage to gain the insights of risk into these reactors. This is due that the use of PSA for advanced reactors is mainly focused on indentifying the PSA issues for designer and regulatory bodies, and developing the relevant methodologies and tools. Differently from the PSA for the existing and new reactors, moreover, there seems to not currently reach any general consensus on how to take into account several technical issues discussed in the workshop and on what scope and level of depth to take into account them in implementing the PSA for advanced reactors.

General conclusions of this workshop are as follows:

- Periodic survey on further activities among member countries will be helpful in finding and clarifying further issues related to the PSA of new and advanced reactors;
- Better guidance and peer review process on the PSA of new and advanced reactors was identified by both industry and regulatory as an important aspect;
- Regarding high-priority technical issues related to the PSA of new and advanced reactors, pilot study and international collaboration will provide more insights into the underlying issues. Such kind of technical issues and common areas of interest among member countries were raised and discussed in the workshop.

All the findings and insights obtained in the workshop will be fed back into the respective task report on "PSA for new reactors and PSA for advanced reactors."

Appendix 1: Daily Program of the Workshop

20 June	21 June	22 June
9:00 – 10:40 (N.SIU)	**9:00 – 10:40 (JM. LANORE)**	**9:00 – 10:40 (G. GEORGESCU)**
Introductory remarks	Modeling of the AP1000® Digital Instrumentation and Control Systems, David S. Teolis, Westinghouse, USA	Probabilistic modeling of passive features, F. Sassen, Westinghouse, Germany
Level-1 PSA to support the design of the KALIMER-600 Sodium Cooled Fast Reactor, Sang Hoon HAN, KAERI, Korea		
Study on preliminary level-1 PSA for Japan sodium-cooled fast reactor, K. Kurisaka, JAEA, Japan	I&C modelling in the IRSN EPR level 1 PSA, J. Delache, IRSN, France	Comparison of two uncertainty analysis methods for the estimation of reliability of passive system of VHTR, Seok Jung HAN, KAERI, Korea
Level 1 probabilistic safety assessment to support the design of the CEA 2400MWth gas-cooled fast reactor, F. Bertrand, CEA, France	Fire PSA Development in CGNPC, X. Jun, CGNPC, China	Problems Facing the Use of Passive Safety Systems, L. Burgazzi, ENEA, Italy
Overview of VHTR's PSA approach in Korea, Seok Jung HAN, KAERI, Korea	Analysis of Design-Reliability Assurance Program in ACP600 Application, Huang Zhichao, CNPE, China	
11:00 – 12:40 (A. BAREITH)	**11:00 – 12:40 (R.J. LUTZ)**	**11:00 – 12:40 (T. LEAHY)**
Generation IV Integrated Safety Assessment Methodology, Timothy Leahy, INL, USA	In-Vessel Retention Modeling Capabilities in MAAP5, C.Y. Paik, Westinghouse, USA	NRC Activities Concerning PSA for New and Advanced Reactors, N. Siu, NRC, USA
ASAMPSA2 project : appliance of LWR PSA2 methodology to GEN IV reactors, H. Bonneville, IRSN, France	Development of level 2 PSA Methodology for Sodium-Cooled Fast Reactors, T. Suzuki, JAEA, Japan	ASME/ANS Standards for ALWR and Advanced Non-LWR PRA: Status and Some Challenges, N. Siu, NRC, USA
Reliability analysis of 2400 MWth gas-cooled fast reactor natural circulation decay heat removal system, M. Marques, CEA, France	PSA Level 2 as Element of an Integral Safety Assessment before Plant Commissioning, H. Löffler, GRS, Germany	Insights from Recent Activities on PSA Being Pursued by the IAEA, Irina Kuzmina, IAEA
Level-1 PSA for internal events for TAPS3&4 - A Challenge, Rajee Guptan, Nuclear Power Corporation of India Ltd, India	MAAP5 Modeling Capabilities for Initial Plant Transients and Shutdown States, and Application to Shutdown PSA and Full Scope SAMG Covering All Plant States for Operating and New Plants, Chan Y. Paik, Fauske and Associates, Westinghouse, Belgium	Assuring PSA Technical Adequacy for New Advanced Light Water Reactor Designs, R.J. Lutz, Westinghouse, USA
14:00 – 15:40 (J.J. TONG)	**11:00 – 12:40 (R. VIROLAINEN)**	**11:00 – 12:40 (L. BURGAZZI)**
Applying Risk Insights in USNRC Reviews of Integral Pressurized Water Reactor Designs, M. Caruso, NRC, USA	Regulatory Assessment of the PSAs for the UK EPR and AP1000 Reactors in the UK, A.G. Cobo, NII, UK	Lessons Learnt from PSAs for New and Advanced Reactors in Russia, V. Morozov, Atomenergoproekt, Russia
Development of PSA Audit Guideline and Regulatory Model for SMART, Namchul Cho, KINS, Korea	Lessons learned form IRSN review of Flamanville 3 Level 1 PSA, G. Georgescu, France	Safety-Security Interface, Bruce Mrowca, Information System Laboratories, USA
Use of PSA in the Development of SMRs, Andrea Maioli, Westinghouse, USA	The Role of PRA in New NPP Projects in Finland, Ari Julin, STUK, Finland	Automatic fault tree generation in the EPR PSA project, P. Nonclercq, EDF, France
Achievement of the level 1 PSA in support to the CEA 2400 MWth Gas-cooled Fast Reactor, M. Balmain, EDF, France	Introduction of PSA team works in CNPE, Zhao Bo, CNPE, China	Existence and impact on safety of inter-system common cause failures : a method, P. Nonclercq, EDF, France

16:00 – 17:40 (K. AHN)	16:00 – 17:40 (G.GEORGESCU)	16:00 – 17:40 (A. AMRI)
Breakout session (*) PSA for advanced reactors - Session summary by each session chair - CAPS on PSA for advanced reactors: summary of questionnaires and answers, K. Ahn, KAERI, Korea	Breakout session (*) PSA for new designs - Session summary by each session chair - CAPS on PSA for new reactors: summary of questionnaires and answers, G. Georgescu, IRSN, France	Breakout session (*) Common discussion - Session summary by each session chair - **Closing remarks**.

(*) The breakout sessions are intended to provide a framework to present summaries of the day presentations and to discuss the day open issues and conclusions. A presentation of the summaries of the task questionnaire answer is foreseen during the first two breakout sessions (advance reactors on Monday and new reactors on Thursday. The last breakout session is also dedicated to preparatory discussion for the proceedings development

Level-1 PSA to support the design of the KALIMER-600 Sodium Cooled Fast Reactor

Sang Hoon HAN, Tae-Woon KIM, Hae-Yong JEONG, Seok Joong HAN, Kwang-Il AHN and Joon-Eon YANG

Integrated Safety Assessment Division, Korea Atomic Energy Research Institute, 1045 Daedeokdaero, Yuseonggu, Daejeon, 305-353, Korea, hanseok@kaeri.re.kr

Abstract

A sodium-cooled fast reactor, KALIMER-600, is under development. Its fuel is the metal fuel of U-TRU-Zr and it uses sodium as a coolant. KALIMER-600 has passive safety features such as passive shutdown functions, passive pump coast-down features, and passive decay heat removal systems. It has inherent reactivity feedback effects.

The probabilistic safety assessment (PSA) will be one of the initiating subjects for designing KALIMER-600 from the aspects of risk informed design. A preliminary level-1 internal full power PSA has been performed to evaluate the safety level and its applicability for the KALIMER-600 conceptual design.

Various design alternatives are evaluated from the viewpoint of PSA in order to support the design of the KALIMER-600. Sensitivity studies are also performed to evaluate the assumptions made for the PSA. The applicability and weakness of the KALIMER-600 PSA are discussed. The technical issues to be solved in performing the PSA will be discussed.

Keywords: Sodium Cooled Fast Reactor, Probabilistic Safety Assessment, Risk Informed Design, Uncertainty Issues

1. Introduction

A sodium-cooled fast reactor (SFR), KALIMER-600, is under development at Korea Atomic Energy Research Institute (KAERI) (Hahn 2007). Its fuel is the metal fuel of U-TRU-Zr and it uses sodium as a coolant. Its advantages are excellent uranium resource utilization, inherent safety features, and non-proliferation.

The probabilistic safety assessment (PSA) will be one of the initiating subjects for designing KALIMER-600 from the aspects of a risk informed design. For core damage prevention, the core damage frequency (CDF) for KALIMER-600 should be lower than that of currently operating LWRs, thus KALIMER-600 will be designed so that its CDF is lower than 10^{-6}/yr, and a large radioactivity release is also excluded by limiting a large dose release rate lower than 10^{-7}/yr.

Using the conventional event tree and fault tree method which are used in LWR PSA, Level-1 PSA for the internal events during power operation is performed to evaluate the safety level and design alternatives for the KALIMER-600. The methodology and procedure of a PSA of an SFR has do not have a large difference compared to the current light water reactors. Among the Level 1, 2, and 3 PSAs (core damage frequency, containment capability, and public health effects analysis), only the Level 1 PSA (core damage accident scenario analysis) is now considered. Internally initiated events such as loss of flow events, reactivity insertion events, and loss of heat sink events are considered. Externally initiated events such as fire or earthquake events are not considered yet.

The safety features of KALIMER-600 are briefly presented in Section 2. The software used for the PSA is described in Section 3. The preliminary PSA is described in Section 4. The sensitivity analysis and conclusions are given in Section 5 and 6, respectively.

2. Safety Features of KALIMER-600

KALIMER-600 is a sodium cooled fast reactor with an electricity output of 600MWe and reactor core thermal power of 1523.4 MWt. It uses U-TRU-10%Zr metal fuel for a breakeven core. An overview of the KALIMER-600 plant is illustrated in Figure 1.

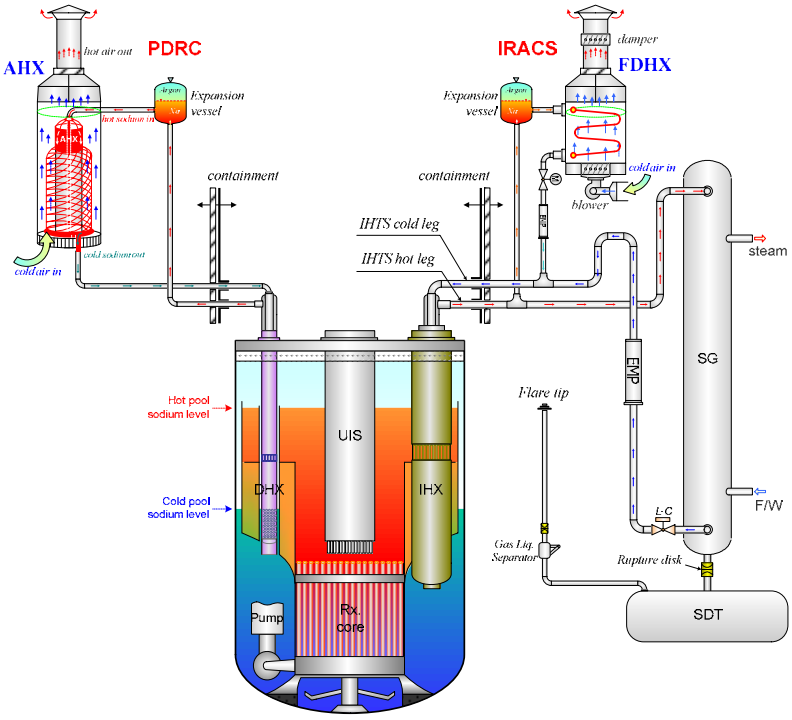


Figure 1. Schematic of KALIMER-600

KALIMER-600 has safety systems with passive as well as active safety features. It has passive safety features such as passive shutdown functions, passive pump coast-down features, and passive decay heat removal systems. The passive decay heat removal system is called PDRC (Passive Decay Heat removal Circuit), which is installed in the reactor vessel. The active decay heat removal system is called IRACS (Intermediate Reactor Auxiliary Cooling System), which is installed in the intermediate loop. The KALIMER-600 has also inherent reactivity feedback effects such as Doppler, sodium void, core axial expansion, control rod axial expansion, core radial expansion, and etc. For the reactor trip functions, independent and diverse features are assumed among the primary reactor trip systems (RPS), the secondary RPS and SASS (Self-Actuated Shutdown System).

The safety functions of KALIMER-600 are summarized as follows.

- Reactivity Control Function (1st Reactor Trip System, 2nd Reactor Trip System, Inherent Reactivity Feedback Features)
- Decay Heat Removal Functions (PDRC, IRACS, Secondary Heat Removal System)
- Inventory Control Functions (External Vessel)
- Supporting System such as Electrical Power

The safety functions between conventional PWR Plants and KALIMER-600 are compared and summarized in Table 1.

Table 1. Comparison of Safety Functions between PWR and KALIMER-600

Safety Features	KALIMER-600	OPR1000
Reactivity Control	RPS (1st trip system, 2nd trip system, SASS)	RPS (main trip system, diverse trip system)
Inventory Control	External Vessel	Safety Injection (High Pressure, SIT, Low Pressure)
Decay Heat Removal	PDRC (Passive), IRACS	AFWS (2 MDP + 2 TDP), Safety Injection + Bleed (SDS Valves)
	Normal Feedwater	Normal Feedwater, Startup Feedwater Pump
Pressure Control	Not Required	Pressurizer, PRV
Supporting System	Electrical Power System	Electrical Power System, Component Cooling Water System, HVAC, etc.

3. PSA Software

The AIMS-PSA (HAN 2010) and FTREX (JUNG 2004) are used for the PSA of the KALIMER-600, which were developed by KAERI. The AIMS-PSA provides a tool to construct fault trees and event trees, to generate minimal cut sets for each sequence in connection with FTREX, and to perform the importance and uncertainty analyses. The FTREX is the most powerful cut set generator and has been successfully used for many PSAs or risk monitors in Korea and USA. The accident sequence quantification for KALIMER-600 PSA can be done in a couple of seconds using the FTREX. The AIMS-PSA was developed to simplify and automate PSA tasks. If a PSA model is provided, the AIMS-PSA integrates the PSA model to build one fault tree model for the evaluation of whole core damage frequency, and it also generates minimal cut sets for the core damage frequency. Only a few button clicks are required to perform the quantification of a PSA. It helps a PSA analyst to perform PSA tasks easily and quickly. The following figure illustrates the user interface of the AIMS-PSA.

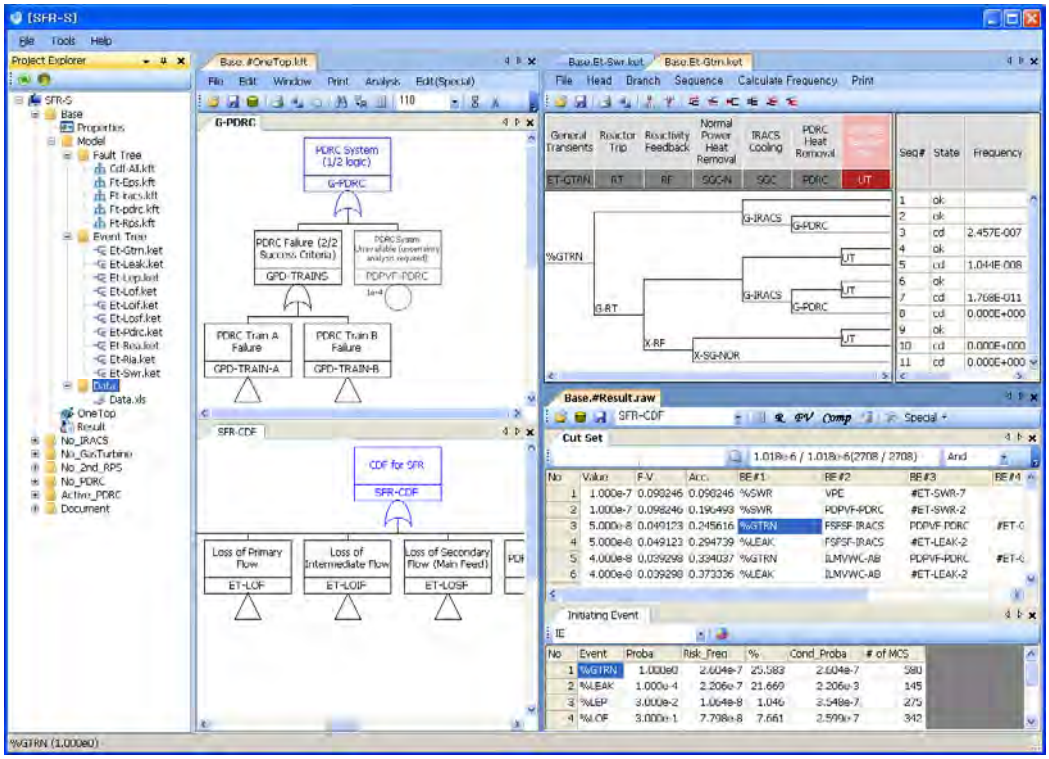


Figure 2. Example Work Screen of AIMS-PSA

4. Development of preliminary level-1 PSA model

4.1 Selection of Initiating Event

Initiating events are selected by reviewing the design of KALIMER-600, the PSA report for PRISM (General Electric 1987) and the PSA report for OPR1000 nuclear power plants (KAERI 1997). Initiating events related to the failure of supporting systems are not considered because the KALIMER-600 is currently in the conceptual design stage. The list of initiating events is shown in Table 2.

Table 2. Estimation of Initiating Event Frequency

Group	KALIMER-600	Frequency	Remark
Transients	General Transients	1	Commercial NPP's experience shows less than 1/yr in Korea
	Loss of Primary Flow	0.3	The same value assumed as the loss of main feedwater
	Loss of Intermediate Flow	0.3	The same value assumed as the loss of main feedwater
	Loss of Normal Electrical Power	3e-2	A little bigger value assumed than 2e-2/yr of OPR1000 PSA
	Loss of Secondary Flow (Main Feed)	0.3	0.3 is the sum of the loss of main feedwater and condenser vacuum for OPR1000 PSA
LOCA	Vessel Leak	1e-4	Conservative value assumed
Reactivity	Reactivity Insertion Accident	1e-3	The same value for 0.1$~0.2$ reactivity insertion for PRISM PSA
Special	Sodium Water Reaction in SG	1e-3	Similar value as 1.1e-3/yr of PRISM PSA
	PDRC Unavailable	3e-3	No experience in the world. It is assumed that it would occur once per 100 yr ~ 1000 yr.

4.2 Definition of Core Damage

The core damage of a metallic fuel SFR can be defined as follows in the PRISM PSA Report (General Electric 1987). The core damage is assumed to occur when one of the following temperature limits is challenged.

- peak fuel centerline temperature is greater than 955℃ (melting temperature)
- peak clad temperature is greater than 700℃ (eutectic temperature)
- peak coolant temperature is greater than 760℃ (structural damage temperature, ASME service level D limit)

In the metallic fuel SFR, the cladding damage temperature is much lower than the MOX (mixed oxide) fuel SFR due to the eutectic formation between the metallic fuel and metallic cladding. In the metallic fuel SFR, however, the heat transfer from the fuel to sodium coolant through the cladding is much better and much faster than in the case of the MOX fuel SFR.

4.3 Development of Event Trees

An event tree analysis is used to determine the accident scenarios for a given initiating event. It postulates accident scenarios for a given initiating event and facilitates the identification of failure or success of mitigating systems associated with various consequences of such accidents. Event trees are developed for the selected 9 initiating events.

If an initiating event occurs, the safety features required are the reactor trip and decay heat removal. The KALIMER-600 design does not require safety systems for the inventory and pressure controls, which are essential in light water reactors.

The reactor would be shut down by the reactor protection system. Even if the reactor protection system fails, the inherent reactivity feedback feature in the KALIMER-600 design would shutdown the reactor, and the reactor power could be maintained at the decay heat level. There is enough time for the operation crew to shutdown the reactor. The operation crew can shutdown the reactor manually if the RPS fails due to a trip signal or trip breaker, not because of stuck rod. The decay heat removal is accomplished by the IRACS, PDRC, or main feedwater system.

An example event tree is shown in the following figure.

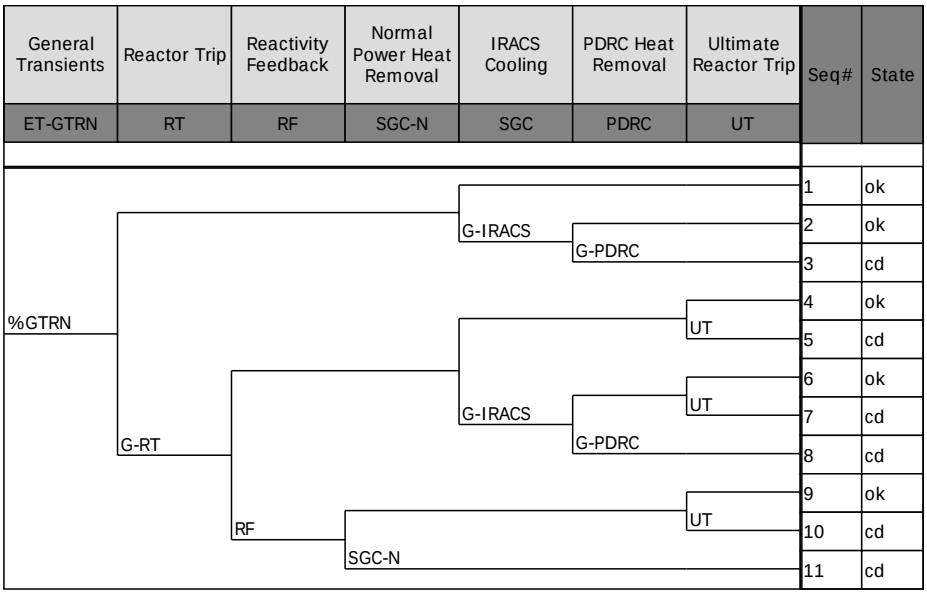


Figure 3. Event Tree for General Transients (GTRN)

4.4 Development of System Fault Trees

A system failure that appears in an event tree is modelled by a fault tree. There are two types of systems. One is front-line systems such as RPS, PDRC and IRACS, that appear in the event tree. The other is supporting systems such as an electric power system that supports the function of front-line systems.

Simple fault tree models for the PSA are developed instead of a detailed model at this conceptual design stage. We tried to consider major dominant failure modes instead of a detailed model and to consider the dependencies between systems.

In this article, the fault tree model of the PDRC is discussed because the PDRC is a passive system for which the modelling characteristic is different with that of light water reactors. For other systems, the modelling characteristic is almost the same as that for light water reactors.

The PDRC is used to remove the decay heat in case the IRACS cannot remove the decay heat after a reactor trip. The PDRC has 2 trains, and each train has 50% capacity. Thus, all trains should function to remove the decay heat successfully. The PDRC is a fully passive system that consists of pipes, heat exchangers (DHX), and a cooling tower (AHX). It has no valves in the main loop. It does not require any active components. The temperature sensor and heat tracing are installed, which are used to ensure that the temperature is above the solidification of sodium in the pipes.

During normal power operation, the DHX is separated with the sodium inventory of the reactor. However a small amount of heat is transferred to the PDRC thru the DHX. It maintains the temperature of sodium at a liquid state in the PDRC pipes. If the sodium temperature becomes lower than a set point, the heat tracing will start to operate so as to prevent sodium solidification.

If the decay heat is not removed after the reactor trip for any reason, the sodium level increases inside the reactor as the temperature rises, and contact is made between the DHX and sodium inventory of the reactor. Then, the PDRC starts to remove the decay heat. The AHX is used to release the heat transferred to the PDRC into the atmosphere.

Electric power is supplied to the temperature sensors and the heat tracing to prevent sodium solidification during normal power operation. Electric power is not required for the decay heat removal function of the PDRC.

The PDRC is a passive safety system that does not require any active components. The failure mode considered for the PDRC is different with those of an active system. The following failure modes are considered for the PDRC in this study.

- Passive system reliability due the phenomenological uncertainty
- Pipe leak
- Sodium solidification
- The failure of temperature sensors and heat tracing in the case of sodium solidification

The following figure illustrates the fault tree for the PDRC.

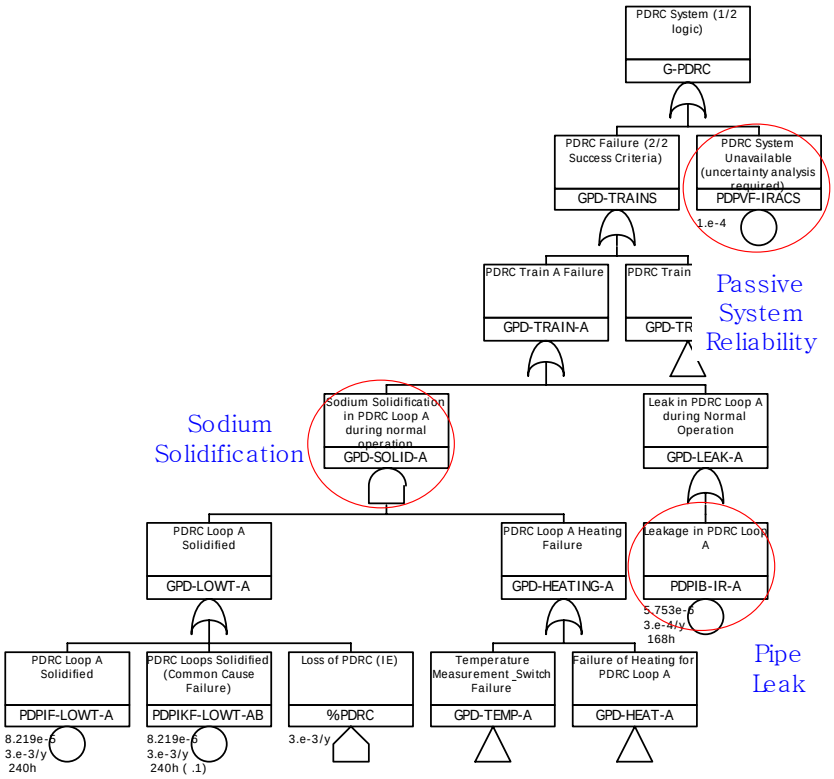


Figure 4. Top Logic of the Fault Tree for PDRC

The reliability data for the pipe leak, electric components and I&C components are quoted from those for commercially operating light water reactors. The assumptions are made for the development of a fault tree for PDRC:

- The PDRC is a passive system. Even though the PDRC will be designed to function for all situations, it is assumed that there is a possibility that the PDRC cannot remove decay heat sufficiently in some cases that we have not expected. This is called passive system reliability due to the phenomenological uncertainty in this analysis, which is assumed to be 1e-4 for the PDRC. This value is a kind of target reliability for the PDRC to be met in the design stage. The passive system reliability due to the phenomenological uncertainty is addressed as reliability of the thermal hydraulic passive system if the phenomenon is for the movement of working fluids (Burgazzi 2007). The passive system reliability should be analyzed in future.

- It is assumed that sodium solidification may occur once in 100 to 1000 years. A logarithmic mean of 3e-3/yr is used.

- It is assumed that the mission time (the time that the PDRC should operate after an accident) for the PDRC is 1 week.

4.5 Reliability Data

The reliability data is necessary for events used in the event trees and fault trees. The reliability data can be categorized as follows:

- Initiating event frequency
- Component hardware failure data
- Common cause failure data
- Human reliability data
- Reliability data for special events

It is impossible to obtain reliability data from operating experiences because the KALIMER-600 is currently in the design stage. The reliability data for the pump, valve, I&C, and electric components are quoted from EPRI URD (EPRI 1995), NUREG reports (USNRC 2007, USNRC 2001), and OPR1000 PSA (KAERI 1997). The data for some components specific to the SFR are assumed based on engineering judgment.

Common cause failure (CCF) events are modelled using the beta factor method. The value 0.1 of the beta factor (USNRC 1987) is used for all component types. This results in a very conservative output because the beta factor method produces conservative results in most cases. The value 0.1 of the beta factor is also conservative compared to the recent CCF data. The alpha factor method and recent CCF data will be applied in the final analysis.

At this moment, two human actions are modelled in the KALIMER-600 PSA. One is the operator recovery action when the isolation valve of the IRACS is spuriously closed during normal operation where a 0.01 failure probability is assumed. The other is operator action to shutdown the reactor when the reactor trip fails due to the failure of a trip signal or trip breaker, where a 0.1 failure probability is assumed. The failure probabilities are assumed based on expert opinion in a human reliability analysis. A more detailed human reliability analysis will be done in the next phase of the KALIMER-600.

There are several special events considered in this PSA, whose data are not obtained from the typical PSAs for commercial nuclear power plants. The following table shows examples of special events.

Table 3. Reliability Data for Special Events

Special event	Reliability Data	Remark
The pipe leak for IRACS and PDRC	3.0e-4/y	2.5e-10 / (h ft) (USNRC 2007), 140 ft assumed
Sodium solidification of PDRC and IRACS	3e-3/y	An occurrence frequency of once per 100 to 1000 year is assumed.
Phenomenological uncertainty for PDRC where the system can not remove the decay heat as designed	1.0e-4	We assign the reliability target that the PDRC should have. The value of 1e-4 is similar to the failure probability for the check valve to open. The phenomenological uncertainty will be analyzed in future work.
Phenomenological uncertainty for the reactivity feedback following the RPS fails	1.0e-6	The designer confirms there is no possibility that the reactivity feedback fails. However, the value of 1e-6 is assigned to be analyzed in more detail in the future. The phenomenological uncertainty will be analyzed in future work.
The failure of safety systems affected by the sodium water reaction in a steam generator	1.0e-4	The safety systems such as the reactor vessel, RPS and PDRC are designed not to be damaged against the sodium water reaction in a steam generator. The value of 1e-4 is assumed and should be confirmed in the final design.

4.6 Accident Sequence Quantification

Accident sequence quantification is used to evaluate the CDF for each sequence. The event tree and fault tree linking approach are used as a basic method of the accident sequence quantification. The AIMS-PSA generates the minimal cut sets using the FTREX and calculates the CDF for each sequence.

The CDF from the internal events of the KALIMER-600 is estimated to meet the design target even if the PSA is performed with conservative reliability data. There is a lot of uncertainty in the CDF results at this moment.

5. Sensitivity studies on the design alternatives and PSA assumption

The KALIMER-600 is in the design stage, and various configurations are now under consideration. A lot of assumptions are made in performing this PSA. Therefore, we try to evaluate the impact of configuration change and assumptions on the core damage frequency. The sensitivity study results are summarized in Table 4.

There are one passive and one active system for the decay heat removal function. The sensitivity studies are performed for the cases of various design alternatives when only a passive or active system is installed (Cases 1, 2 and 6). The CDF is increased beyond the acceptable level in every case. The results show that both passive and active features are essential. The option to increase the capacity of PDRC from 2x50% to 2x100% is not considered to be effective (Case 5).

The base case assumes that there are two independent groups of the RPS, and there are two gas turbine generators to support a safety grade electric power system. The CDF also increases beyond the unacceptable level if any feature is removed from the base case (Cases 7 and 8).

Several sensitivity analyses were performed for assumptions made such as the solidification frequency (Case 3), phenomenological uncertainty of PDRC (Case 4) and reactivity feedback probability (Case 9). These sensitivity analyses show that the phenomenological uncertainty of PDRC has a big impact on the CDF, and should be studied in detail in the future.

The current design features of the safety systems are identified to be the most acceptable in terms of risk as well as cost, out of various alternative designs.

Table 4. Summary of Sensitivity Studies on the Design Alternatives and PSA Assumptions

System	Assumption used in Base Case	Assumption used in Sensitivity Study (Case number)	CDF Ratio*
PDRC	PDRC	(1) No PDRC	5,176
	2 trains x 50% decay heat removal, Passive System	(2) 2 trains x 100% decay heat removal, Active System	10.2
	Solidification frequency (0.003/yr)	(3) Solidification frequency, 10 times increased (0.03/yr)	1.76
	Unavailability of PDRC due to Phenomenological Uncertainty (1e-4)	(4) Unavailability of PDRC due to Phenomenological Uncertainty, 10 times increased (1e-3)	5.66
	2 x 50% Passive	(5) 2 x 100% Passive	0.86
IRACS	2 x 100%, Safety Class Electrical Powers (2 Gas Turbine backup)	(6) No IRACS	364
EPS	2 Gas Turbine backup	(7) No Gas turbine	11.4
RPS	2 diverse system (1st, 2nd)	(8) No 2nd RPS	23.4
	Reactivity feedback failure probability (1e-6)	(9) Reactivity feedback failure probability increased to 0.1	1.03

*CDF Ratio = CDF in sensitivity study / CDF in Base Case

6. Conclusions

The KALIMER-600 is under design with defense-in-depth concept with active, passive, and inherent safety features. The PSA is performed for several purposes. One is to confirm that the typical PSA methodology can be applied to the SFR and to find further research items. The other is to evaluate the safety level from the viewpoint of PSA and to evaluate the design options for the KALIMER-600.

The PSA methodology has been used in conventional nuclear power plants, which mainly have active safety systems. Even though there are still some limitations in developing PSA models for plants such as the KALIMER-600 with its inherent and passive systems, core damage scenarios are identified and developed using event tree and fault tree models.

The reliability data is mainly quoted from the database of conventional nuclear power plants with some assumptions and expert judgments. The core damage scenarios and frequency of the KALIMER-600 are identified. Sensitivity studies on the design alternatives of safety systems and PSA assumptions are also performed.

Because of the assumptions made, the following areas are identified for future studies to improve the quality of the PSA;

- Develop a methodology to estimate the reliability of a newly introduced system or component for the SFR.

- Develop a methodology to estimate the frequency of phenomenology such as sodium solidification in the PDRC.

- Develop a methodology to estimate the passive system reliability. The method can be applied to estimate the phenomenological uncertainty for the PDRC and reactivity feedback.

- Establish a methodology for evaluating the reliability of a Digital I&C system.

- Establish a methodology for estimating the common cause failure data of a newly introduced component.

- Develop a methodology for a severe accident analysis for non-light water reactors to evaluate the source term.

7. References

Hahn, D. et al, (2007), KALIMER-600 Conceptual Design Report, KAERI/TR-3381/2007, Korea Atomic Energy Research and Institute.

HAN, Sang Hoon, et al, (2010), Improved Features in a PSA Software AIMS-PSA, Transactions of the Korean Nuclear Society Spring Meeting, Pyeongchang, Korea, May 27-28.

JUNG, Woo Sik, et al, (2004), "A Fast BDD Algorithm for Large Coherent Fault Trees Analysis", Reliability Engineering and System Safety, Vol. 83, pp. 369-374.

General Electric, (1987) PRISM Preliminary Safety Information Document, Vol. IV, Chapters 15 to 17 and Appendix A, Preliminary Probabilistic Safety Assessment, GEFR-00793, UC-87Ta.

KAERI, (1997), Final Level 1 Probabilistic Safety Assessment for Ulchin Nuclear Units 3 and 4 (Internal Event Analysis) Rev.1.

Burgazzi Luciano, (2007), State of the Art in Reliability of Thermal-Hydraulic Passive Systems, Reliability Engineering and Systems Safety, Vol. 92, pp 671-675.

EPRI, (1995), Advanced Light Water Reactor Utility Requirements Document, Volume II ALWR Evolutionary Plant, Chapter 1, Appendix A, PRA Key Assumptions and Groundrules, Rev. 7.

USNRC, (2007), Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, NUREG/CR-6928.

USNRC, (2001), Reliability Study: Combustion Engineering Reactor Protection System, 1984–1998, NUREG/CR-5500, Vol. 10.

USNRC, (1987), Procedures for Treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR-4780.

WGRisk Workshop on PSA for New & Advanced Reactors, Paris, June 20 – 22, 2011

Level-1 PSA to support the design of the KALIMER-600 Sodium Cooled Fast Reactor

Sang Hoon HAN, Tae-Woon KIM, Hae-Yong JEONG,
Seok Joong HAN, Kwang-Il AHN and Joon-Eon YANG

KAERI Korea Atomic Energy Research Institute

Contents

- Introduction
- PSA Methodology & Software
- KALIMER-600 System
- KALIMER-600 Preliminary PSA
- Sensitivity Analysis
- Passive System Reliability
- Conclusion

1. Introduction

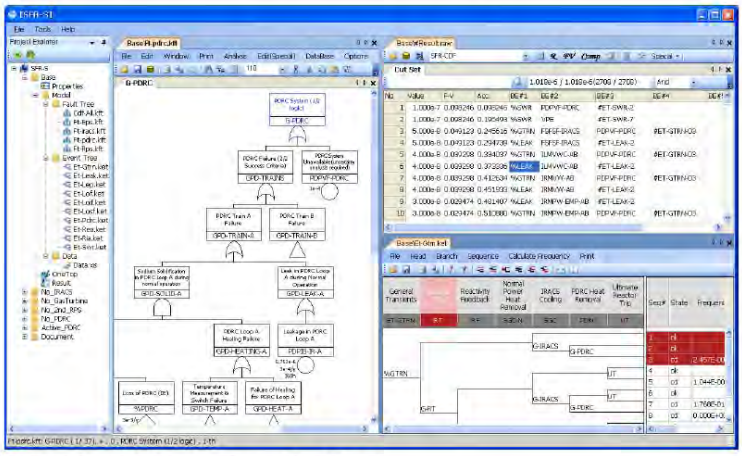
- Preliminary PSA for KALIMER-600
  - Internal Full Power Level-1 PSA
  - External PSA and Level-2 & 3 PSA will be done in future

- Purpose
  - Evaluate the safety level of KALIMER-600
  - Support the design of KALIMER-600
  - Apply the typical PSA methodology to KALIMER-600
  - Find issues for future studies

3

PSA Software

- AIMS-PSA : Integrated PSA Software
- FTREX : PSA Quantification Engine

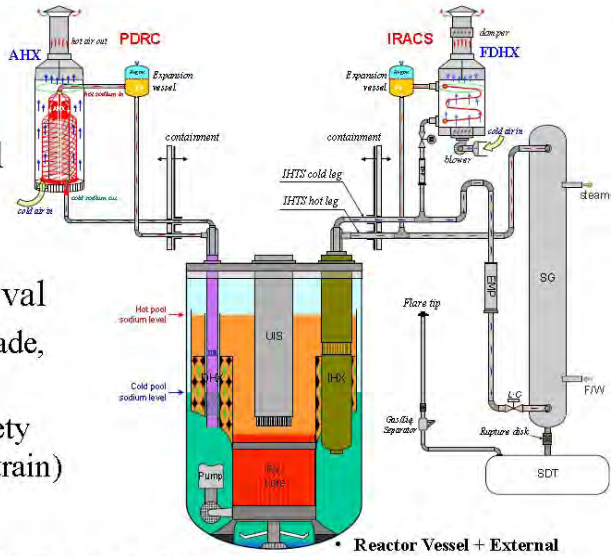


*) AIMS-PSA & FTREX : developed by KAERI

4

3. SFR Safety Systems

- Reactivity Control
  - RPS : 2 diverse systems
- Decay Heat Removal
  - PDRC (Safety grade, 50% x 2)
  - IRACS (Non-safety grade, 100% x 2 train)



❖ IRACS (Intermediate Reactor Auxiliary Cooling System)
❖ PDRC (Passive Decay Heat removal Circuit)

- Reactor Vessel + External vessel (Inventory control)
- No pressurized (Pressure control)

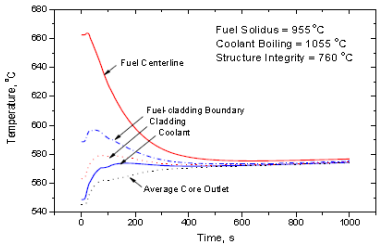
5

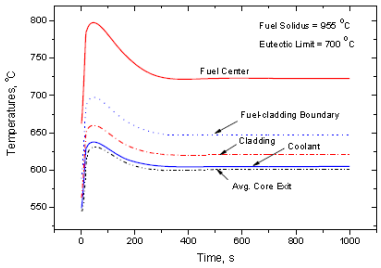
참고

- Definition of Core Damage
  - The core damage of the metallic fuel SFR can be defined as follows in the PRISM PSA Report. The core damage is assumed to occur when one of the following temperature limits are challenged.
    - peak fuel centerline temperature is greater than 955℃ (melting temperature)
    - peak clad temperature is greater than 700℃ (eutectic temperature)
    - peak coolant temperature is greater than 760℃ (structural damage temperature, ASME service level D limit)
  - In the metallic fuel SFR the cladding damage temperature is much lower than MOX (mixed oxide) fuel SFR due to the eutectic formation between the metallic fuel and metallic cladding. In the metallic fuel SFR, however, the heat transfer from the fuel to sodium coolant through the cladding is much better and much faster than in the case of MOX fuel SFR.

6

Safety Analysis



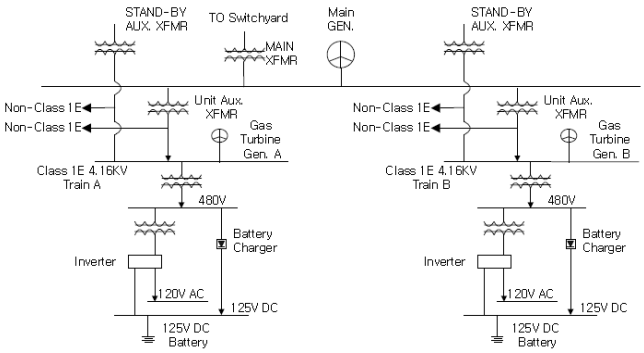


- Loss of Heat Sink (ULOHS)
  - the PDRC works to transfer heat through DHX at 70 seconds
  - no core damage has occurred even though some reactivity feedback functions are assumed to be degraded.
  - The fuel, clad, and coolant temperatures are saturated to 575℃.
- Reactivity Insertion Accident (Unprotected Transient Over-Power (UTOP))
  - Peak Cladding Temp = 660 °C at 26 sec

7

SFR Safety Systems

- Electric Power System
  - 2 train + 2 Gas turbine generator Assumed (OPR1000 design)



- Component Cooling Water System or HVAC
  - No information
  - Assumption
    - CCWS or HVAC is not necessary for the operation of critical safety systems

8

SFR-600 vs PWR (OPR 1000) Safety Functions

❑ Critical Safety Functions

CSF	KALIMER-600	OPR1000
Reactivity	RPS (2 group Diversity)	RPS
Inventory	External Vessel	Safety Injection (High Pressure, SIT, Low Pressure)
Decay Heat Removal	PDRC (Passive) IRACS Normal Feedwater	AFWS (2 MDP + 2 TDP) Safety Injection + Bleed (SDS Valves) Normal Feedwater Startup Feedwater Pump
Pressure	Not Required	Pressurizer, PRV

9

4. SFR-600 Preliminary PSA

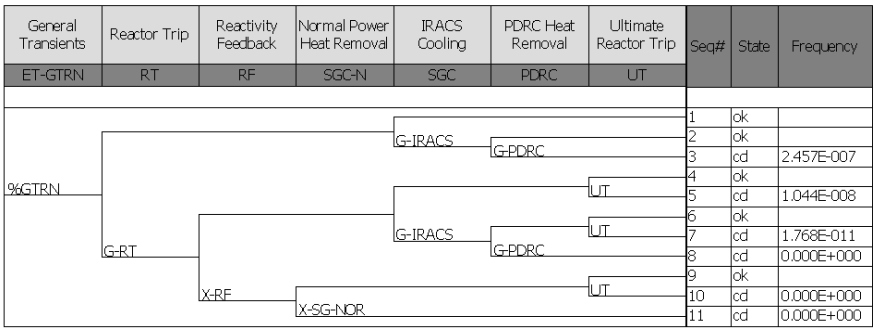
❑ Selection of Initiating Events

Group	KALIMER-600	Frequency	Remark
Transients	General Transients	1	Commercial NPP's experience shows less than 1/yr in Korea
	Loss of Primary Flow	0.3	The same value assumed as the loss of main feedwater
	Loss of Intermediate Flow	0.3	The same value assumed as the loss of main feedwater
	Loss of Normal Electrical Power	3e-2	A little bigger value assumed than 2e-2/yr of OPR1000 PSA
	Loss of Secondary Flow (Main Feed)	0.3	0.3 is the sum of the loss of main feedwater and condenser vacuum for OPR1000 PSA
LOCA	Vessel Leak	1e-4	Conservative value assumed
Reactivity	Reactivity Insertion Accident	1e-3	The same value for 0.1$~0.2$ reactivity insertion for PRISM PSA
Special	Sodium Water Reaction in SG	1e-3	Similar value as 1.1e-3/yr of PRISM PSA
	PDRC Unavailable	3e-3	No experience in the world. It is assumed that it would occur once per 100 yr ~ 1000 yr.

10

Event Tree for Accident Scenario

- Safety Functions Models
  - Reactivity Control
    - Reactor trip system, inherent reactivity feedback, Manual
  - Decay Heat Removal
    - PDRC, IRACS, Normal Feedwater
  - Inventory & Pressure Control not required



Seq#	State	Frequency
1	ok	
2	ok	
3	cd	2.457E-007
4	ok	
5	cd	1.044E-008
6	ok	
7	cd	1.768E-011
8	cd	0.000E+000
9	ok	
10	cd	0.000E+000
11	cd	0.000E+000

11

Fault Tree for System Models

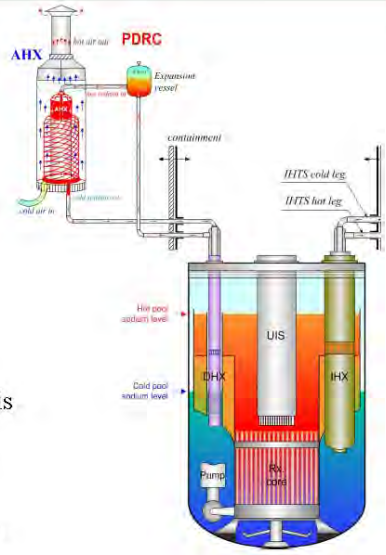
- PDRC

System	Major components	Modeling characteristics
PDRC	Passive system (heat exchanger, pipe, cooling tower)	Passive system reliability Pipe leak Sodium solidification
IRACS	Active system (EMP, blower, valve, heat exchanger, pipe, cooling tower)	Active components (EMP, valve, blower) Pipe leak Sodium solidification Actuation signal
RPS	Digital system (trip rod, trip circuit breaker, digital I&C)	Group1 & 2 (1st RPS, 2nd RPS) Digital I&C No detailed design information ➔ system reliability assumed
EPS	Electric system (grid, transformer, bus, breaker, gas turbine generator, battery, …)	Active components (grid, transformer, bus, breaker, gas turbine generator, battery, …)

12

PDRC System Fault Tree

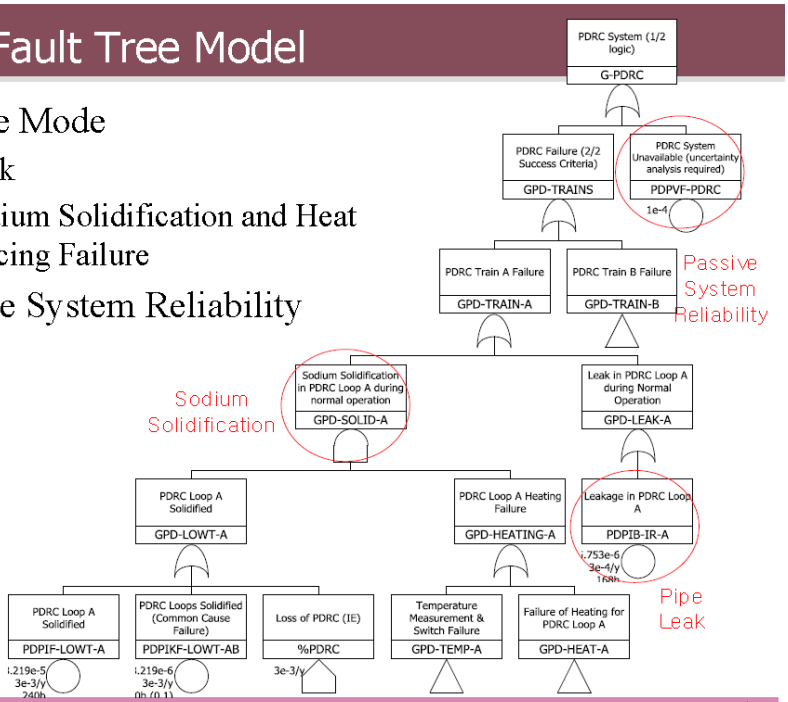
- Design Concept
  - Passive, 2 x 50% Loops
- Failure Mode
  - Pipe Leak
  - Passive system reliability due to Phenomenological uncertainty
    - 10^{-4} assumed : design target
    - Future study necessary
  - Sodium Solidification
    - If sodium temp. becomes low, heating is required via Heat tracing
    - The reason of sodium solidification ? The frequency ? CCF ?
    - Once per 100 ~ 1000 year (negotiation with designer)
  - Any other Failure Mode ?



13

PDRC Fault Tree Model

- Failure Mode
  - Leak
  - Sodium Solidification and Heat Tracing Failure
- Passive System Reliability



14

Reliability Data

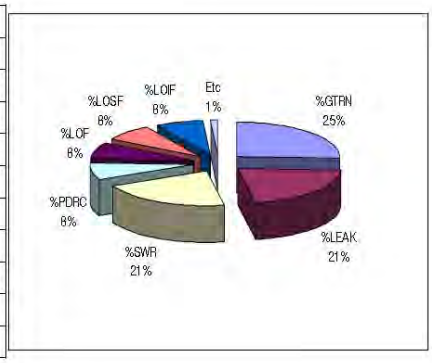
- Component Reliability Data (for components in PWR)
  - EPRI ALWR Utility Requirement Doc/PRA Key Assumptions
  - NUREG/CR-5500, PRISM PSA, IEEE Std 500, OPR1000 PSA
- Assumptions for special component/system
  - RPS reliability
    - Trip signal : $1^{st} = 10^{-4}$, $2^{nd} = 10^{-3}$ assumed
    - CEA, circuit breaker : 10^{-4} assumed (conservative than NUREG/CR-5500)
  - IRACS actuation signal reliability : 5×10^{-4} Assumed
  - Pipe Leak : 2.5e-10/h ft assumed ➔ PDRC : 3×10^{-4} /y
  - EMP Pump fails to start : 3×10^{-3} /demand assumed (typical motor driven pump)
- Common Cause Failure
  - CCF Factor : 0.1 assumed (conservative, 2 trains)
- Initiating Event Frequency
  - Assumed based on Korean Nuclear power plant experience & PRISM PSA
- Assumptions for phenomena
  - PDRC solidification : once every 100~1000 year assumed ➔ 3×10^{-3} /yr
  - PDRC passive system reliability = 10^{-4}
  - Containment/reactor/PDRC integrity against Sodium Water Reaction in SG = 10^{-4}

15

Core Damage Frequency (CDF) Quantification

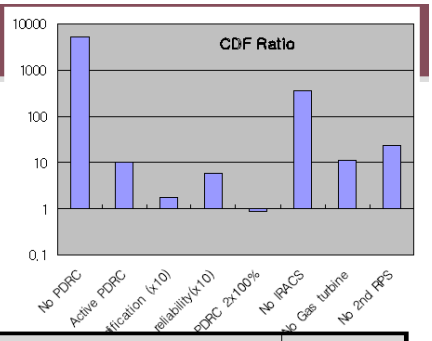
- Full Power Internal Events for KALIMER-600
  - CDF = 10^{-6}/yr

Initiating Event	IE Freq/yr	CDF/yr	%
General Transients	1.0	2.60e-7	25.58
Vessel Leak	1.00e-4	2.21e-7	21.67
Sodium Water Reaction in SG	1.00e-3	2.12e-7	20.84
PDRC Unavailable	3.00e-3	7.99e-8	7.85
Loss of Primary Flow	3.00e-1	7.80e-8	7.66
Loss of Secondary (Feedwater)	3.00e-1	7.80e-8	7.66
Loss of Intermediate Flow	3.00e-1	7.80e-8	7.66
Loss of Electric Power	3.00e-2	1.06e-8	1.05
Reactivity Insertion Accident	1.00e-3	2.41e-10	0.02
Total		1.02e-6	



16

5. Sensitivity Analysis



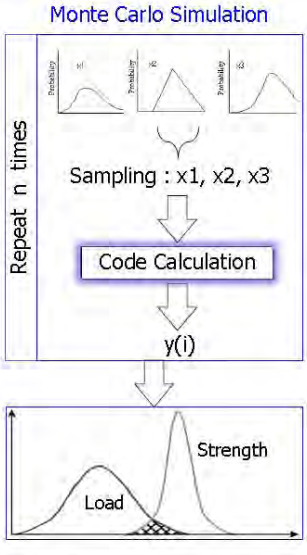
- Sensitivity study for
  - design alternatives
  - major assumptions

System	Base Case	Sensitivity Case	CDF Ratio
PDRC	PDRC	No PDRC	5176
	2 x 50% Passive	2 x 100% Active System	10.2
	Sodium solidification frequency (0.003/yr)	10 times of base case (0.03/yr)	1.76
	PDRC passive system reliability (10^{-4})	10 times of base case (10^{-3})	5.66
	2 x 50% Passive	2 x 100% Passive	0.86
IRACS	2 x 100%	No IRACS	364
EPS	2 Gas Turbine backup	No Gas turbine	11.4
RPS	2 diverse system (1st, 2nd)	No 2nd RPS	23.4

17

6. Passive System Reliability

- Uncertainty in Phenomena
  - Analyze the phenomena using the computerized simulation model
  - Sources of uncertainty
    - input variables of computer code, approximations in modeling, variety in real situation
- Need to estimate uncertainty
  - in results from the computer code simulation
- Monte Carlo approach
  - can be used when difficult to get analytic solution
  - Monte Carlo analysis or Response surface analysis



MOSAIQUE : Support the uncertainty analysis of computational simulation model

18

7. Conclusion

- SFR PSA
  - Typical LWR PSA approach can be used to evaluate the risk of SFR
  - Support decision making in design
- Issues to be resolved (Sources of uncertainty)
  - Reliability for newly introduced system or component
  - Reliability for unknown phenomena (such as sodium solidification frequency in the PDRC)
  - Passive system reliability (PDRC and reactivity feedback)
  - Digital I&C system reliability
  - Common cause failure data for newly introduced component
  - Severe accident analysis for non-light water reactors
  - Common regulatory framework for non-light water advanced reactors

19

Thank You for Your Attention

STUDY ON PRELIMINARY LEVEL-1 PSA FOR JAPAN SODIUM-COOLED FAST REACTOR

Kenichi Kurisaka [1]

[1] Japan Atomic Energy Agency, 4002 Narita-cho, O-arai, Ibaraki, 311-1393, Japan
kurisaka.kennichi@jaea.go.jp

Abstract

Japan Atomic Energy Agency (JAEA) has been preliminarily applied a level-1 PSA to the safety design concept of a loop-type large scale of the Japan sodium-cooled fast reactor (JSFR). As for internal initiators in power operation, typical core damage sequences (i.e., anticipated transients without scram (ATWS), loss of reactor sodium level (LORL), and protected loss of heat sink (PLOHS)) were evaluated to identify dominant failure combinations. The core damage frequency (CDF) was quantified to evaluate the adequacy of the safety design. This evaluation served to improve safety by modifying the decay heat removal system of JSFR. As part of development of reliability evaluation technology, we studied on the quantification of the sodium leak probability depending on the leak flow rate. This study serves to evaluate accident management effectiveness in the sodium-leak-related core damage sequences. As for external initiators, we conducted the seismic margin evaluation based on the seismic fragility evaluation for the principal structures and components, and confirmed that they have sufficient margin against the postulated seismic condition.

Keywords: Sodium-cooled Fast Reactors (SFRs), Internal Events, Level 1 PSA, Seismic Margin Evaluation

1. Introduction

JAEA has been developing the JSFR in the Fast reactor Cycle Technology development (FaCT) project from JFY2006. In this development process, it is needed to identify vulnerability in safety and to evaluate the achievement level of JSFR to the risk targets at the FaCT project phase-I: JFY2006 to JFY2010. For this purpose, JAEA has been applying the level-1 PSA to the conceptual system design of JSFR. This paper describes (1) the level-1 PSA for internal initiators in power operation, (2) current status of the related reliability evaluation technology, and (3) the seismic margin evaluation as part of external initiators evaluation.

JAEA established the development targets and design requirements in the FaCT project (Kotake 2008). The development target in safety is commonly applied to a fast reactor system and its relevant fuel cycle systems. This safety development target is defined as follows: the safety level shall be equal to future light water reactors and related fuel cycle system. In order to achieve this target, the three design requirements were settled. One of them is a requirement to reach risk targets: i.e., the CDF should not exceed 10^{-5}/site-year even considering multiple units in a site, and the frequency of loss of containment function in core damage conditions (i.e., containment failure frequency: CFF) should not exceed 10^{-6}/site-year. If we assume ten reactor units in a site and if both core damage and loss of containment function take place independently among their units, the requirements for a single reactor unit is described as follows: the CDF should not exceed 10^{-6}/reactor-year (/ry), and the CFF should not exceed 10^{-7}/ry (Kotake 2008).

JSFR is a loop-type sodium-cooled fast reactor: i.e., primary pumps and intermediate heat exchangers (IHX) constituting two loops of primary heat transport system (PHTS) are installed outside the reactor vessel as illustrated in **Fig. 1**. The thermal energy generated at the rated power of 3570MW heats up the primary coolant to 550 ºC at the reactor vessel outlet, then it is transferred to the secondary coolant with being heated to 520 ºC at the two IHXs. The main steam with temperature of 497 ºC and pressure of 19.2 MPa is generated at the two steam generators, and it rotates the turbine generator to produce the electric power output of 1500MW.

In the JSFR system, there are major innovative safety features to be evaluated as follows: (1) passive reactor shutdown system; i.e., Self-Actuated Shutdown System (SASS), (2) passive decay heat removal system; i.e., natural circulation of sodium coolant and natural air flow at the air cooler, (3) leak tight backup structures in the sodium cooling systems; i.e., guard vessels and guard pipes in the primary cooling system, enclosures in the secondary cooling systems which include both the decay heat removal system (DHRS) and the main heat transport system, (4) Double wall heat transfer tubes in the steam generators and the air coolers of the DHRS, and (5) In-vessel retention against typical core disruptive accidents by pursuing practical elimination of the severe re-criticality and the in-vessel core debris cooling; where the typical core disruptive accidents could be caused by unprotected loss of flow (ULOF) and/or unprotected transient over power.

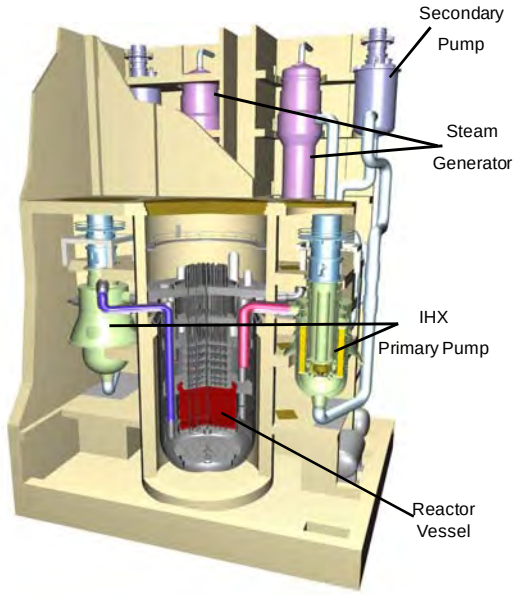


Fig. 1 Schematic view of JSFR nuclear steam supply system (Kotake 2008)

2. Preliminary level-1 PSA for internal events

2.1 Analytical Model and Data Sources

A Level-1 PSA has been implemented preliminarily to evaluate the CDF related to internal initiators in power operation. Our PSA is based on the standard probabilistic risk assessment method (USNRC, 1983), which is broadly used. In order systematically to identify core damage sequences, typical initiating events were selected. In this selection, we considered the similarity of event progression and functional dependency between the initiating events and safety systems. Event trees for each initiating event were developed in a simplified manner based on the plant design features and on some available transient analysis results. Fault trees were also developed to quantify branching probabilities in the event tree. We also took into account common-cause failure of active components that have the same design specifications so as to evaluate the effectiveness of the diversity incorporated into the system design.

Quantitative estimation of both the initiating event frequency and component failure rate in the sodium cooling system was based mainly on the data consisting of operating time and the number of failure instances, which are stored in the component reliability database system for sodium-cooled fast reactor systems, named CORDS (Kurisaka, 1997). Those data came from the Japanese fast reactors Joyo and Monju, and the U.S. fast reactors EBR-II and FFTF. Since there is too little operational experience for steam generators in Japanese fast reactor systems statistically to estimate their reliability, the failure rate of steam generator tubes was estimated on the basis of operational experience data for various foreign fast reactor systems. The failure rates of other components in the electrical system, water/steam system, etc. were estimated on the basis of the operational experience of Japanese light water reactors (Kirimoto, 2000).

2.2 Types of Core Damage Sequences in JSFR

In terms of difference of safety systems required for preventing core damage, typical event sequences leading to core damage are categorized into three types as follows: (1) Anticipated Transient Without Scram (ATWS), (2) Loss Of Reactor sodium Level (LORL), and (3) Protected Loss Of Heat Sink (PLOHS). ATWS is defined as a failure in rapid reactor shutdown under abnormal transient and accident condition (e.g., loss of off-site power). LORL is a failure in making up the reactor sodium level under primary cooling system leak condition. PLOHS is a failure in maintaining decay heat removal under the adequate reactor sodium level condition after reactor shutdown.

Among these types, ATWS events have high possibility of preventing dependent failure of the containment function because of in-vessel retention combined with post-accident heat removal. On the other hand, LORL and PLOHS events could lead to dependent failure of the containment function because the degraded core cannot be cooled, thus resulting in molten fuel leak through the reactor vessel and containment. Therefore, it is necessary to reduce the frequency of LORL and PLOHS events lower than the target value of CFF.

2.3 ATWS Events

Since the reactor shutdown system has not been designed in detail yet, we assumed that JSFR has a main reactor shutdown system and a backup one as shown in **Fig. 2**. The two reactor shutdown systems having no shared components are double-redundant (i.e., success criterion is at least one out of the two systems). In addition, they consist of different types of active components with inter-system diversity, and each shutdown system is actuated with at least one reactor trip signal against representative initiators from the standpoint of occurrence frequency and consequence. Each system also satisfies a single-rod-stuck condition and a single-failure criterion. In order to enhance the safe shutdown, the Self-Actuated Shutdown System (SASS) consisting of the Curie point electromagnet is installed as a part of the control rod releasing mechanisms in the backup reactor shutdown system.

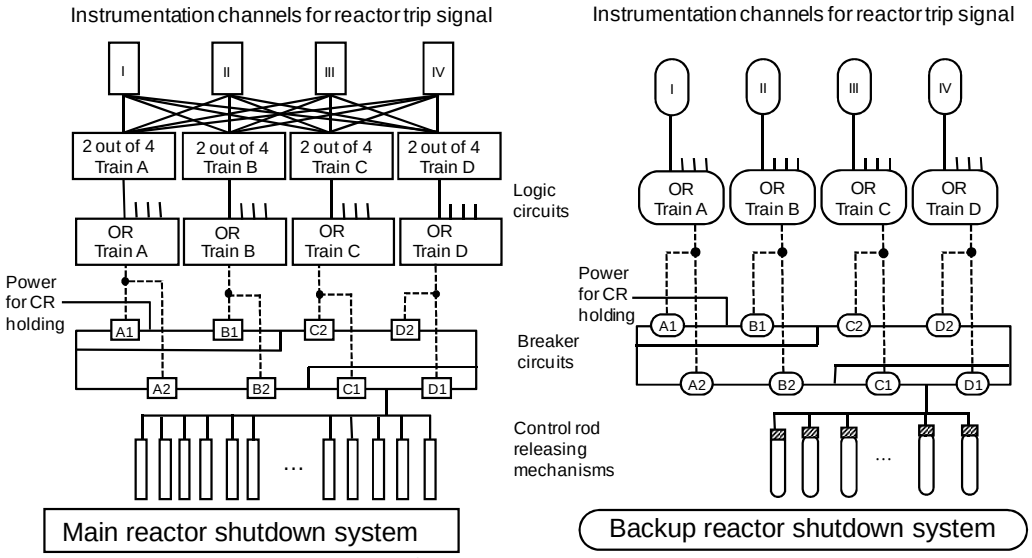


Fig. 2 Schematic diagram of reactor shutdown systems assumed in this study

Owing to high redundancy and to adequate diversity, the point estimation value of ATWS frequency stayed within the range from $1x10^{-8}$/ry to $3x10^{-8}$/ry, corresponding to an unreliability value for the SASS of 0.1 to 1, respectively. The unreliability of the SASS is defined as probability, with which the reactor shuts down by means of SASS actuation not before core damage. The timing of SASS actuation depends not only on actuation temperature but also on core performances (e.g., reactivity coefficient, average of core outlet temperature around the control rod equipped with the SASS) and cooling system characteristics (e.g., the halving time of the primary flow rate). The unreliability of the SASS arises from uncertainty of these

parameters. In this study, we assumed the SASS unreliability of 0.1 by referring the preliminary evaluation of an unprotected loss-of-flow event in the fast reactor with a large-scale core (Kurisaka, 2001).

The evaluation result of ATWS frequency indicates small sensitivity to the SASS reliability. There are two reasons. One reason is that the SASS can recover only loss of actuation signals for the backup reactor shutdown system. In other words, the SASS is not effective under the control-rod-stuck situation. The other reason is that we considered a conservative possibility of rod-stuck failure due to an unknown common cause with probability of $2x10^{-5}$/scram-demand per backup reactor shutdown system.

There is, however, a quite large uncertainty in estimation of the control-rod-stuck probability because of the lack of instances of failure in sodium-cooled fast reactor operating experience. It cannot be also expected for the control rod to be stuck even though reactor shutdown obviously requires the active motion of the control rod. This is because once the control rod is released from the control rod drive mechanism after the SASS actuates, the control rod drops into the core through the liquid sodium inside the guide tube with a large clearance. Therefore, it is important to understand the sensitivity of ATWS frequency to the rod-stuck failure probability of the backup reactor shutdown system. Assuming that the rod-stuck probability of the backup reactor shutdown system could be reduced by one-tenth, the point estimation value of ATWS frequency fell to the range from $3x10^{-9}$/ry to $3x10^{-8}$/ry, corresponding to an unreliability of the SASS from 0.1 to 1, respectively. This result indicates that the SASS can be effective under a severe accident condition, although the effect of its introduction depends on the reliability of the rod insertion.

2.4 LORL Events

In order to prevent the LORL event with high reliability, the systematic design measures described below are adopted in JSFR.

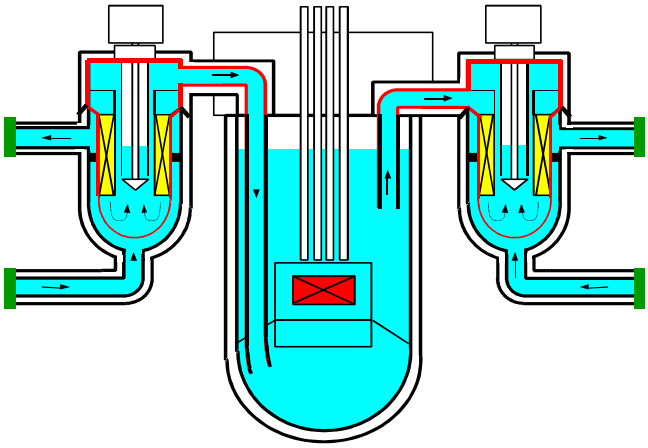


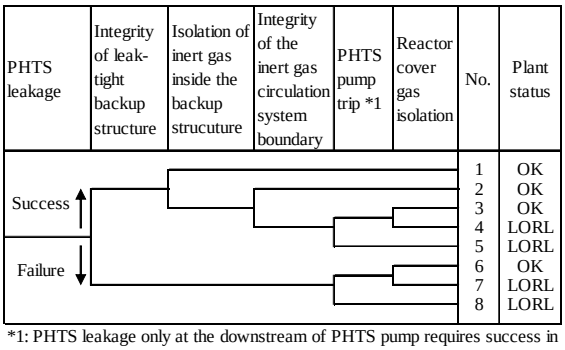
Fig. 3 Outline of the primary heat transport system in JSFR

(1) The primary coolant boundaries in the Primary Heat Transport System (PHTS) are located in the position above the liquid surface level in the reactor vessel in order to eliminate leaking by the siphon effect (see **Fig. 3**).
(2) The primary coolant boundaries are enclosed with a leak-tight backup structure (i.e., guard vessel and guard pipe) so as to restrict coolant leak against the boundary failure.
(3) Removing the leak driving force (i.e., PHTS pump trip, isolation of the reactor cover gas from its supply system) is automatically actuated so as to prevent the LORL combined with the above item (1) against double failures in the PHTS boundary and its backup structure.
(4) The reactor vessel and its guard vessel have no penetration at the lateral sides and bottom.
(5) The pressure of the Secondary Heat Transport System (SHTS) is kept slightly higher than that of the PHTS so as to prevent the leaking of primary coolant at the interface breach.

(6) The open space between the primary pipe and its guard pipe is partitioned to limit the volume of the leak, and this volume limitation prevents LORL combined with some operator's action (e.g., control of coolant temperature), even if two of the segments partitioned inside the guard vessels/pipes are fully filled with leaked sodium.

In addition, the inert gas is circulated between the leak-tight backup structure and the inert gas circulation system for the sodium leak monitoring; the inert gas inside the backup structure is automatically isolated from its circulation system under PHTS leak condition. Since the inert gas circulation system is not usually designed so as to maintain its integrity under high temperature condition, we assumed that unless the inert gas circulation system is isolated, its gas boundary becomes breached due to heat shock caused by ingress of the leaked sodium.

In order to identify LORL event sequences, the event tree shown in **Fig. 4** was developed on the basis of all the above information. The point estimation value of the LORL frequency became ~$4x10^{-9}$/ry. The dominant event sequences leading to LORL are sequences 4 and 5. In these sequences, hot sodium leaks into the piping line of the inert gas circulation system, the leaked sodium would give a heat shock to the pipe wall, and it could result in failure of the pipe wall in the inert gas circulation system and in leak of sodium into the cell. If the leak magnitude were restricted by smaller-diameter piping of the inert gas circulation system, there would be a longer time margin to the LORL condition. By then, it could be expected that the operators would have taken some recovery action to prevent the LORL event. It may be better to enhance the integrity of the inert gas system boundary at a high temperature so as to reduce possibility of sodium leak into the cell as well as possibility of LORL event.



*1: PHTS leakage only at the downstream of PHTS pump requires success in PHTS pump trip.

Fig. 4 Event tree diagram to identify loss-of-reactor sodium level sequences under primary cooling system leak condition.

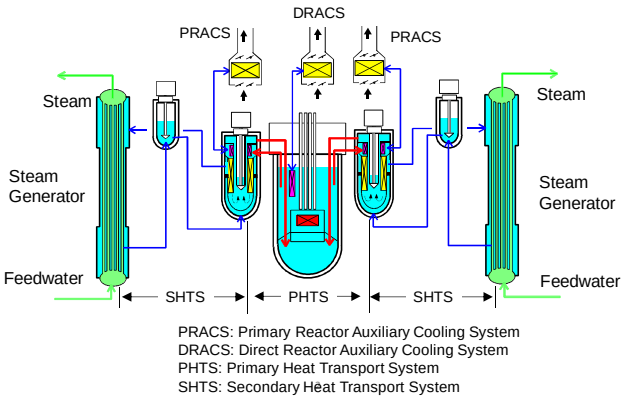


Fig. 5 Outline of the reactor heat transport system and decay heat removal system in JSFR at the beginning of the FaCT Phase-I

2.5 PLOHS Events

PLOHS is a failure in maintaining decay heat removal under the adequate reactor sodium level condition after reactor shutdown. The DHRS in JSFR consists of a single train of Direct Reactor Auxiliary Cooling System (DRACS) and two trains of Primary Reactor Auxiliary Cooling System (PRACS) as shown in **Fig. 5**. This DHRS can be operated under fully passive condition, which means that it is required only to actuate the direct-current-power-operated dampers of the air coolers without pumps and blowers. The damper system has redundancy so that it does not lose its function even considering the single-failure criterion, i.e., each air cooler has two dampers in parallel so that an opening failure of a single damper causes less than a 50% reduction in the air flow rate. In addition, diversity is taken into account in the mechanical design of the dampers between DRACS and PRACS. JSFR is suitable for natural circulation cooling due to its simple and short piping connection and due to the low pressure loss of the core design, as well as the sufficient height difference between the core and the heat exchangers. Since both DRACS and PRACS have a sodium-sodium heat exchanger inside the reactor and PHTS, respectively, they are not affected by the abnormal conditions initiated in the SHTS and the steam-water systems.

In general, the success criterion of DHRS depends on the cooling time period after reactor shutdown as the decay heat decreases with time. Based on the conservative design basis evaluation of the DHRS capability, two out of three trains are required within the 24h period. After the 24h period the success criterion is relaxed so that at least one out of three trains of DHRS provide sufficient cooling capacity. In addition, in the JSFR concept at the beginning of the FaCT Phase-I, even when the DHRS lose its function, another cooling measure was available over all the time period for decay heat removal. This measure is forced circulation cooling by means of one or both of the two loops of the SHTS and the turbine bypass circulation system including steam generators when the offsite power is available. Based on the above condition, we evaluated the point estimation value of the PLOHS frequency to be ~$2x10^{-8}$/ry.

In the FaCT phase-I, there was a design modification that increases the PLOHS frequency. This design modification is a change in a steam generator operation sequence after reactor scram to reduce thermal stress by a severe thermal transient. After this modification, the steam generator is not utilized for decay heat removal. Considering this modification, the calculated PLOHS frequency increased up to ~$5x10^{-7}$/ry. Contributors to the PLOHS frequency were broken down by time phases with different success criteria. The dominant contributor occupied 99% of PLOHS frequency, and it was loss of two out of three trains of DHRS within 24h after reactor shutdown. Obviously this is because the success criterion within 24h period is severer than that after the 24h period. If the designer enhances the heat removal capacity of a single train of DHRS in this time period so as to become less-demanding success criteria, there is potential to reduce at most 99% of the total PLOHS frequency.

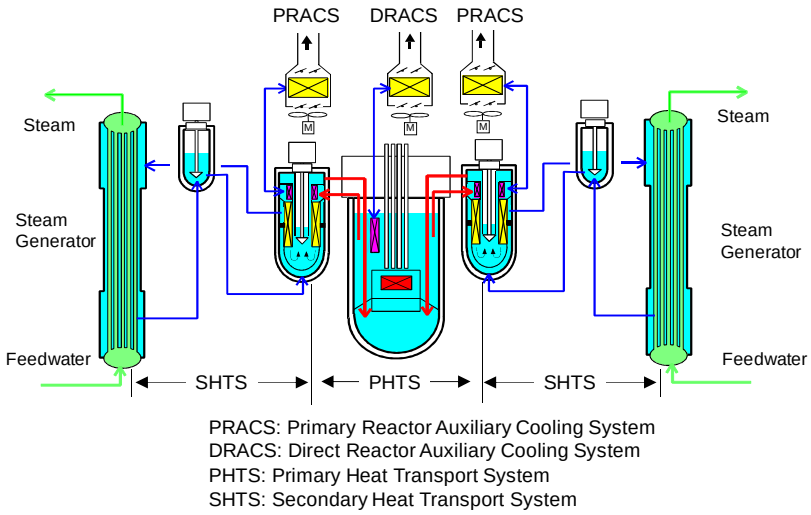


Fig. 6 Design improvement by introducing non-safety-related blowers at the air cooler inlet to enhance PRACS and DRACS capability

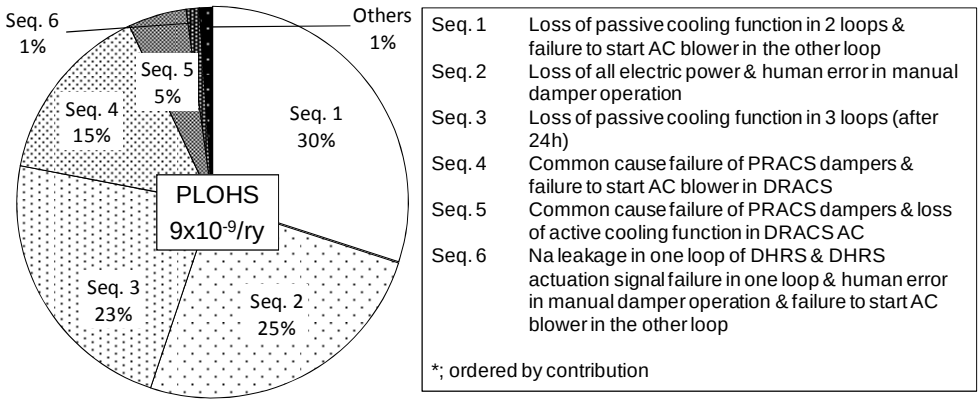


Fig. 7 PSA result: large contributors to PLOHS frequency broken down by combination of loss of mitigation systems

Based on this, the designer/analyst examined possibility of introducing non-safety-related blowers at the air cooler inlet as shown in **Fig. 6**. These additional blowers can enhance PRACS and DRACS capabilities resulting in significant safety improvement with lower cost increase. These capabilities were confirmed by the deterministic safety analysis. The updated PSA result showed quantitatively the reliability improvement in the decay heat removal (see in detail **Fig. 7**): i.e., introduction of the air cooler blowers in both PRACS and DRACS can reduce the PLOHS frequency to ~$9x10^{-9}$/ry.

According to the deterministic safety analysis with nominal analysis condition, a fully passive cooling operation mode by using a single train of PRACS and DRACS has capability of decay heat removal. If we consider this capability, the PLOHS frequency becomes smaller than the above result. In this case, however, phenomenological uncertainty associated with the passive cooling is not considered explicitly in a conventional PSA method. Sensitivity of the uncertainty and variability in key phenomena that are modelled in the deterministic safety analysis will be analyzed and if the sensitivity is significant, the uncertainty will be quantified and then we will improve the evaluation method of the passive safety reliability which considers uncertainty and variability in key phenomena.

3. Current status of reliability evaluation technology

Reliability evaluation technology is indispensible for the level-1 PSA. Our effort has been made on collection of reliability data (i.e., operating time and number of failure instances) and on quantitative estimation of both the initiating event frequency and component failure rate in the sodium cooling system. However, cumulative component operating time is still short, compared with the target reliability level. Particularly concerning the sodium coolant boundary, in addition to further collection of the empirical reliability data, another effort has been made to evaluate the sodium leak probability depending on leak magnitude.

In loop-type sodium-cooled fast reactors (SFRs), it is important to evaluate an effectiveness of accident management measures to prevent core damage sequences that are initiated from primary sodium leak at the primary sodium cooling system, in particular, except the reactor vessel. Its effectiveness depends on the leak magnitude (i.e., leak flow rate) because a leak event with small leak flow rate gives a long time margin to operators compared to large leak flow rate. The leak magnitude in this study is defined as the time-averaged volumetric leak flow rate (m^3/h), which depends on the internal pressure condition. It is required to consider an effect of the leak flow rate on maintaining the reactor sodium level. But there was no method to estimate quantitatively the sodium leak probability depending on the leak flow rate. Thus, since it was needed to develop the data and method, we have studied on the sodium leak probability depending on the leak flow rate. When a sodium leak occurs due to random failure, it is thought that the leak flow rate formulates probability distribution. In this case, the leak occurrence rate of the specific magnitude can be calculated with the equation (1):

$$\lambda_{spec}(/h) = \lambda_{general}(/h) \times P_{spec} \qquad (1)$$

$\lambda_{spec}(/h)$: Leak occurrence rate where the leak flow rate exceeds the specific rate
$\lambda_{general}(/h)$: Leak occurrence rate to all the range of the leak flow rate
P_{spec} : Probability where the leak flow rate exceeds the specific rate.

In this study, the probability distribution was statistically estimated by following the steps below.

Step 1 Investigate the information of sodium leak instances in domestic and foreign sodium-cooled fast reactor systems.
Step 2 Screen the leak instances by considering the leak cause in order to screen out the sodium leak due to abnormal operation such as inadvertent pipe cutting work.
Step 3 Classify the leak instances by considering the type of information related to the leak magnitude.
Step 4 Assume the probability distribution for the unknown quantitative parameter (e.g., leak duration time, internal pressure condition).

Step 5 Estimate the leak magnitude distribution.

As a result of steps 1 and 2, we obtained the information of more than 100 leak instances. After step 3, classification results were categorized as follows: (1) qualitative magnitude is known: e. g., "very slight leak", (2) total leak amount is known: e.g., "sodium leak of 1litter was found", (3) averaged leak flow rate is known, and (4) penetrated crack length is known. Most of the information of the leak instances was classified into (1) and (2). These two categories have incomplete information, but this information is valuable and indispensible. So, based on all these categories (1) to (4), we tried to estimate the sodium leak probability depending on the leak flow rate. This means that we needed to assume the leak duration time for most of the sodium leak instances as a probability distribution in order to estimate the leak flow rate. In the step 4, based on the investigation result, we estimated the probability distribution of the leak duration time. Since measures for the leak detection and leak termination are common among various SFRs, we judged that the estimated probability distribution of the leak duration time is applicable to all the sodium leak instances where the leak duration time is unknown. After the step 5, Probability distribution of leak magnitude was statistically estimated as shown in **Fig. 8**. P_{spec} in the equation (1) can be obtained from **Fig. 8**. The estimated approximation curve in **Fig. 8** is applicable to the leak flow rate in the range from ~0.001m^3/h to ~50m^3/h at the internal pressure of 872kPa-gage, which is equivalent to the internal pressure at the reactor inlet pipe during power operation of typical SFR. The estimation result has been already applied to evaluate the effectiveness of the accident management measures against the sodium-leak-related core damage sequences in Japan's prototype fast breeder reactor Monju. As well, this study also serves to evaluate the accident management effectiveness against the sodium-leak-related core damage sequences in JSFR.

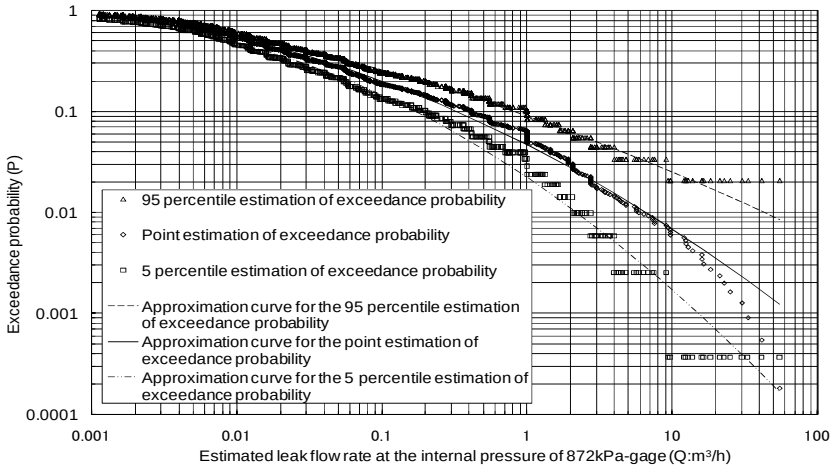


Fig. 8 Estimated probability distribution and approximation curve

4. Seismic margin evaluation

The seismic event is an important external initiator of the core damage. After the Niigata-ken Chuetsu-oki Earthquake in 2007, the postulated seismic load for the JSFR seismic design was reconsidered, and it became severer. In addition, it was decided to develop newly a horizontal seismic isolation system for the JSFR. In the FaCT phase-I, the site location of JSFR has not been determined yet, and so the seismic hazard cannot be quantified. Rather, the seismic margin of the JSFR should be evaluated by conducting a seismic fragility evaluation. So, we conducted the seismic fragility evaluation of principal structures and components in terms of core damage prevention **(Kurisaka, 2011)**. This evaluation was based on the seismic response analysis, which considered the seismic isolation effect and the hardening effect of the laminated rubber bearing in the seismic isolation system. In this analysis, we assumed the seismic ground motion 1 to 5 times as large as the postulated seismic load. Based on the seismic fragility evaluation result, the seismic margin was evaluated with two measures. One is a median Peak Ground Acceleration (PGA) and the other is a High Confidence Low Probability of Failure (HCLPF). The evaluation results are shown

in **Table 1**. These two measures shown in **Table 1** are normalized by the PGA of the postulated seismic condition Ss.

The median PGA is a PGA that gives a conditional probability of 0.5 in the median fragility curve. The median PGA of an event indicates that when an earthquake equivalent to the median PGA takes place, the event happens at a probability of 50%. It can be said that this event can be prevented against an earthquake up to the median PGA in a realistic estimation without any uncertainty and margin. Thus, if the median PGA is regarded as a measure that represents a seismic margin, it can be said that principal structures and components in JSFR have a seismic margin that is at least a factor of 3.

On the other hand, the HCLPF in this study is defined as a PGA that gives a conditional probability of 0.05 in the 95% non-exceedance fragility curve. The HCLPF of an event indicates that when an earthquake equivalent to the HCLPF takes place, the event happens at a probability not greater than 5% with a confidence level of 95%. **Table 1** shows principal structures and components in ascending order of the HCLPF. The smallest value in the normalized HCLPF is 1.19. This corresponds to the excessive reactivity insertion. The next smallest one is 1.55 for the buckling of the reactor vessel. The normalized HCLPF value of the seismic isolation system and reactor building are 2.80 and 4.56, respectively. As the term itself shows, the HCLPF in this study is a PGA that gives a low probability of failure with a high confidence level. If the normalized HCLPF value is greater than 1, it involves that there is a sufficient margin against the postulated seismic condition.

Principal Structures and Components to be Evaluated	Normalized Median PGA	Normalized HCLPF
Reactor Core (Excessive Reactivity Insertion)	3.03	1.19
Reactor Vessel	3.31	1.55
Pump-integrated IHX	3.96	1.59
Control Rod Insertion	5.16	1.64
PHTS Pipes	13.83	2.45
Seismic Isolation System	4.75	2.80
Reactor Building	7.00	4.56

*; Ascending order of the normalized HCLPF

Table 1. Seismic margin evaluation result

5. Conclusions

JAEA implemented the preliminary level-1 PSA of JSFR. Regarding the internal initiators, typical core damage sequences (i.e., ATWS, LORL and PLOHS) were evaluated. The ATWS event is caused by loss of the main and backup reactor shutdown systems. Owing to redundancy and diversity in these systems, the ATWS frequency became ~$1x10^{-8}$/ry. This value is sensitive to the control-rod-stuck probability having a large uncertainty. We confirmed that the SASS can be effective for the ATWS event and that its effectiveness depends on the reliability of the rod insertion. Concerning the LORL event, the dominant sequences became the multiple failures that include the isolation failure of the inert gas inside the backup structure. In these sequences, hot sodium leaks into the piping line of the inert gas circulation system, and the leaked sodium would give a heat shock to the pipe wall. In this study, we conservatively assumed that this causes dependent failure of the pipe wall and the sodium leak into the cell resulting in LORL. In the JSFR, the PLOHS event is caused by loss of DRACS and PRACS. Owing to redundancy and diversity in these systems, the PLOHS frequency became ~$9x10^{-9}$/ry. In addition, the probabilistic evaluation of the PLOHS event served to the design modification of DHRS. The PSA result showed that the total CDF becomes ~$2.3x10^{-8}$/ry. This is less than the both requirements on CDF and CFF; i.e., 10^{-6}/ry and 10^{-7}/ry, respectively. Based on this, we judged that JSFR can achieve the risk targets for internal initiators.

As part of development of reliability evaluation technology, we studied on the quantification of the sodium leak probability depending on the leak flow rate. Sodium leak instances in domestic and foreign SFRs were investigated, and then based on those instances the probability distribution of the sodium leak

flow rate was estimated at the first time in the world. This study serves to evaluate accident management effectiveness in the sodium-leak-related core damage sequences.

For the external initiators, the earthquake was examined as an important risk contributor in Japan. We evaluated seismic margin of the principal structures and components of JSFR, and confirmed that they have sufficient margin against the postulated seismic condition. However, the site location and the design specifications of the advanced seismic isolation system are not determined yet. From now, more efforts are needed in the JSFR seismic design work and related research and development activities.

6. References

Kirimoto, Y., Emukai, H., (2000), Component Reliability Data from 1982 to 1997 on 49 Japanese LWRs Accumulated in the Nuclear Component Reliability Data System, *Proc. the 5th International Conference on Probabilistic Safety Assessment and Management (PSAM5)*, Osaka, Japan.

Kotake, S., Mihara, T., Kubo, S., Aoto, K., and Toda, M., (2008), Development of Advanced Loop-Type Fast Reactor in Japan (1): Current Status of JSFR Development, *Proc. 2008 International Congress on Advances in Nuclear Power Plants*, paper 8226, Anaheim, USA.

Kurisaka, K., (1997), Development of LMFBR Component Reliability Database and Application in PSA, *Proc. 4th Japan-Korea PSA Workshop*, Yokohama, Japan.

Kurisaka, K. et al., (2001), Unreliability Analysis of the Self-Actuated Shutdown System (SASS) in the Unprotected Loss of Flow (ULOF) Event for a Large FBR, I32, 2001 Fall Meeting of the Atomic Energy Society of Japan (in Japanese).

Kurisaka, K. and Okamura, S., (2011), Preliminary Evaluation of JSFR Achievement Level to Risk Targets, *Proc. the 19th International Conference on Nuclear Engineering*, Makuhari, Japan.

U.S. NRC, (1983), PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, U.S. Nuclear Regulatory Commission Report, NUREG/CR-2300.

OECD/NEA Workshop on PSA for New and Advanced Reactors
On June 20-22, 2011

Study on preliminary level-1 PSA for Japan sodium-cooled fast reactor

JAEA
Kenichi KURISAKA
kurisaka.kennichi@jaea.go.jp

Background & Purpose

- JAEA has been developing JSFR in the FaCT project.
- It is needed to identify vulnerability in safety and to evaluate the achievement level of JSFR to the risk targets at the FaCT project Phase-I: JFY2006 to JFY2010.
- For this purpose, we have been applying level-1 PSA to JSFR.

Contents

- Level-1 PSA for internal events in power operation
- Current status of the related reliability evaluation technology
- Seismic margin evaluation as for external events

Risk Targets

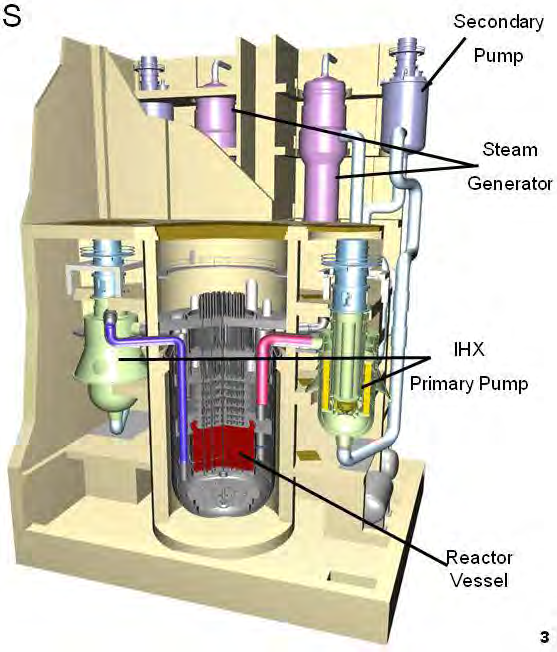
- JAEA established the development targets and design requirements from the developer's point of view.
- Safety development target: the safety level shall be equal to future LWRs and related fuel cycle system.
- One of the safety design requirements is to reach "risk target":
  1. Core damage frequency (CDF) should not exceed 10^{-5}/site-year,
  2. The frequency of loss of containment function in core damage conditions (i.e., CFF) should not exceed 10^{-6}/site-year.
- These targets consider multiple units in a site. If we assume 10 reactor units in a single site and if core damage accidents and loss of containment function in core damage conditions take place independently among their units, the requirements for a single reactor unit is described as follows:
  1. CDF should not exceed 10^{-6}/reactor-year (/ry),
  2. CFF should not exceed 10^{-7}/ry.

2

Schematic view of JSFR NSSS

Large-scale loop-type MOX fuel

Plant parameters	
Power output	1500MWe / 3570MWt
Number of loops in PHTS	2
Primary coolant temperature	550℃ / 395℃
Primary coolant mass flow rate	1.8×10^4 kg/s
Secondary coolant temperature	520℃ / 335℃
Main steam temperature and pressure	497℃ / 19.2MPa



3

Preliminary Level-1 PSA for internal events in power operation

- Standard PSA method was applied, but the model is very simple because JSFR is still in conceptual design phase.
- Typical initiators were selected: e.g., LOF, TOP, LOHS.
- ETs/FTs were developed.
- CCF were considered for active components having the same design specifications.

4

Data sources for parameter estimation

- **Key parameters in level 1 PSA:**
  initiator frequency, component failure rate
- **Sodium fluid components:**
  Japanese SFRs JOYO and MONJU, U.S. SFRs EBR-II and FFTF (data stored the database system named CORDS)
  - **Control rod insertion reliability:**
    MONJU CRDM mockup test data
  - **Sodium-heated SG tube reliability:**
    Various foreign SFRs
- **The other Water/Steam fluid components, electrical components:**
  Japanese light water reactors

5

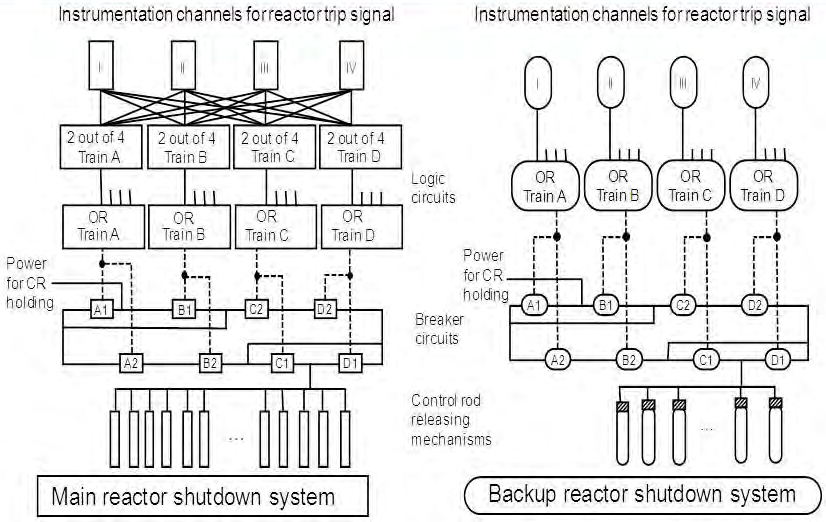
Types of Core Damage Sequences in JSFR

- **Anticipated Transients Without Scram (ATWS)**
  Failure in rapid reactor shutdown under abnormal transient condition (i.e., Loss of off-site power)
- **Loss Of Reactor Level (LORL)**
  Failure in making up the reactor sodium level under primary heat transport system (PHTS) leakage condition
- **Protected Loss Of Heat Sink (PLOHS)**
  Failure in maintaining decay heat removal under the adequate reactor sodium level condition after reactor shutdown

6

Schematic diagram of RSS assumed in this study

➢ JSFR is equipped with two reactor shutdown systems (RSS). Each device composing the RSS adopts a design specification different between the two RSSs.

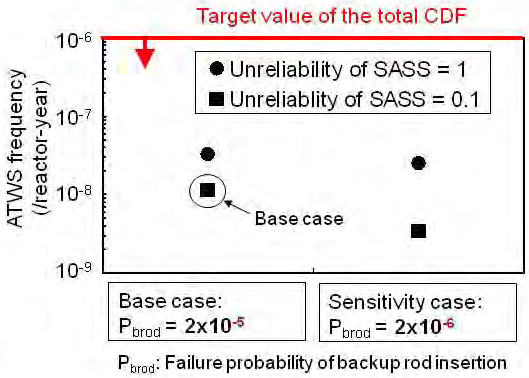


7

OECD/NEA Workshop on PSA for New and Advanced Reactors on June 30-

ATWS frequency quantification results

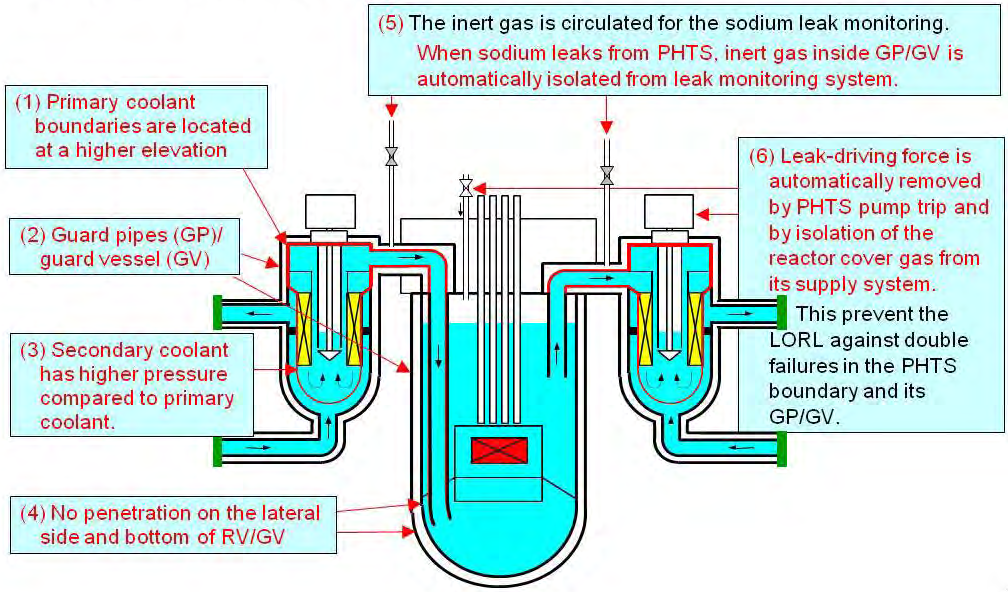
- ✓ The ATWS event is caused by loss of the main and backup RSSs.
- ✓ Owing to redundancy and diversity in the RSSs, the ATWS frequency became ~1x10^{-8} /ry.
- ✓ The result is sensitive to the control-rod-stuck probability having a large uncertainty.
- ✓ SASS can be effective for the ATWS event .
- ✓ Its effectiveness depends on the reliability of the rod insertion.



8

OECD/NEA Workshop on PSA for New and Advanced Reactors on June 30-22

Key safety design features to prevent LORL event

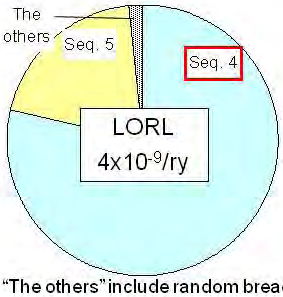


9

OECD/NEA Workshop on PSA for New and Advanced Reactors on June

LORL event tree model

PHTS leakage	A	B	C	D	E	Seq. No.	Plant status
Success						1	OK
						2	OK
						3	OK
						4	LORL
						5	LORL
Failure						6	OK
						7	LORL
						8	LORL



"The others" include random breach of both reactor vessel and its guard vessel.

A: Integrity of leak-tight backup structure
B: Isolation of inert gas inside the backup structure
C: Integrity of the inert gas circulation system boundary
D: PHTS pump trip *1
E: Reactor cover gas isolation

Identified active safety functions required.

*1: required only upon the PHTS leakage at the downstream of PHTS pump

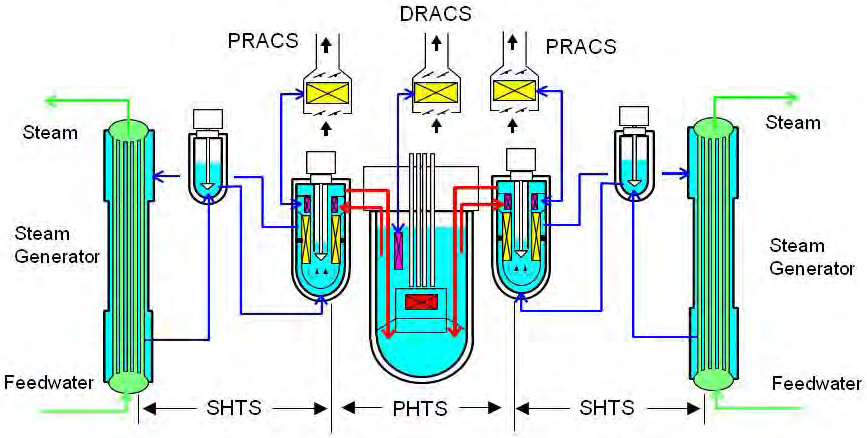
In Seq.4, hot sodium leaks into the piping line of the inert gas circulation system.

- Leaked sodium would give a heat shock to the pipe wall.
- This causes dependent failure of the pipe wall (conservative assumption).
- The sodium leaks into the cell resulting in LORL.

10

OECD/NEA Workshop on PSA for New and Advanced Reactors on June

Outline of decay heat removal system (DHRS)

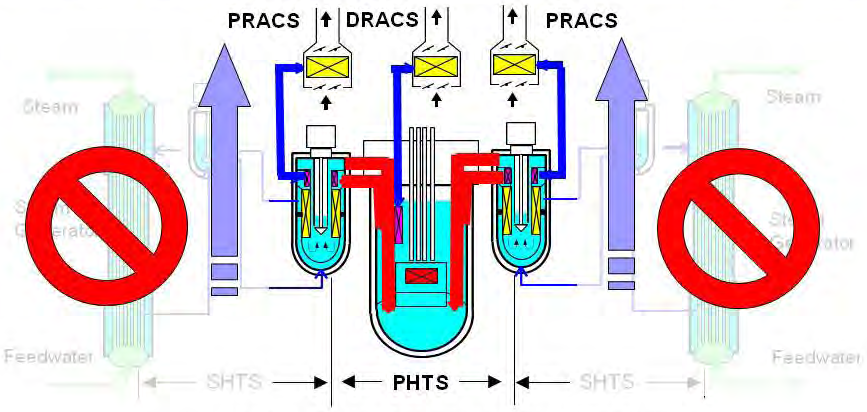


PRACS: Primary Reactor Auxiliary Cooling System
DRACS: Direct Reactor Auxiliary Cooling System
PHTS: Primary Heat Transport System
SHTS: Secondary Heat Transport System

11

Under *Loss of Off-Site Power* condition

Success criterion (S.C.) based on conservative DB evaluation of DHRS capability:
(< 24h) : 2 out of 3 trains of DHRS, (> 24h) : 1 out of 3 trains of DHRS

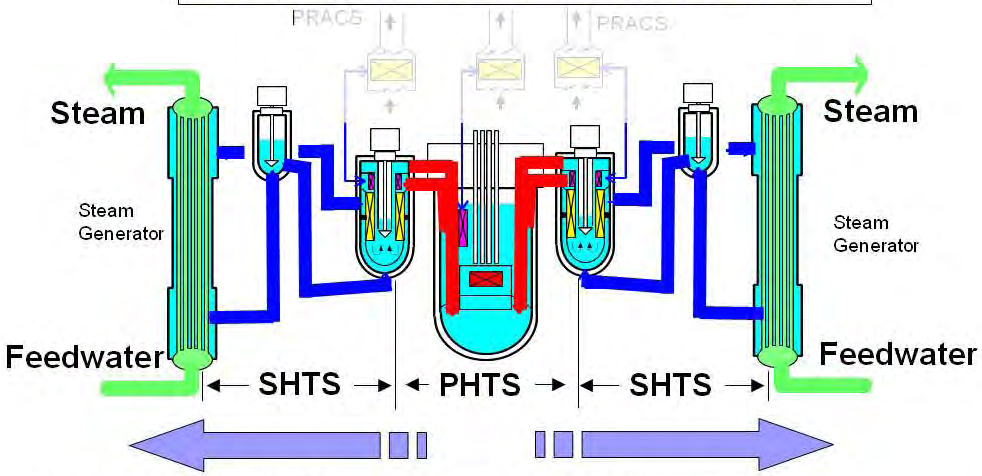


PRACS: Primary Reactor Auxiliary Cooling System
DRACS: Direct Reactor Auxiliary Cooling System
PHTS: Primary Heat Transport System
SHTS: Secondary Heat Transport System

Original design at the beginning of FaCT Phase-I:

NSSS was available for DHR when ***off-site power available***

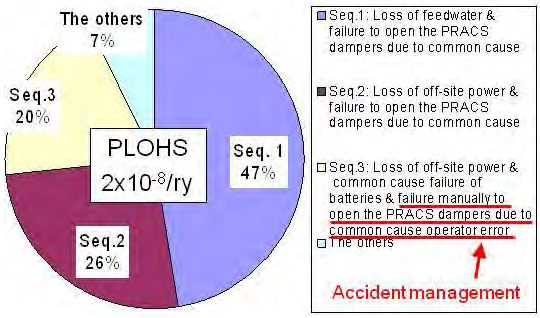
S.C. of NSSS: 1 out of 2 loops in a forced circulation



NSSS includes PHTS, SHTS and Water/Steam system

PLOHS frequency quantification result

- PLOHS frequency < the target value of CDF.
- The top 3 sequences occupy >90%, and include initiators that causes loss of main heat transport system (i.e., loss of DHR by SG lines).
- CCF of PRACS dampers are a dominant contributor in PLOHS.
- Dampers are powered by the battery sources.
- CCF of the batteries appears in the seq. 3.
- AM of manual operation of dampers was considered.

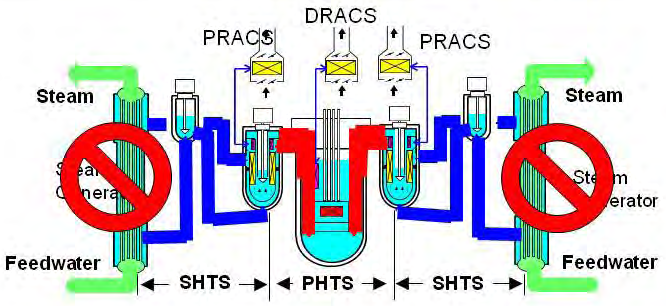


14

Change in SG operation sequence

In the FaCT phase-I, SG operation sequence after reactor scram was changed to reduce thermal stress by a severe thermal transient.
After this change, the SG is not utilized for decay heat removal.

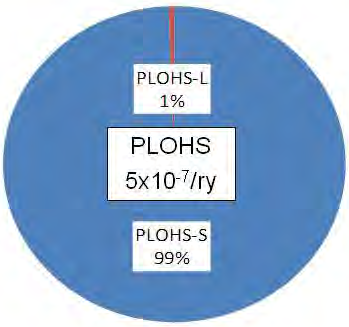
Success criterion (< 24h) : 2 out of 3 trains of DHRS
(> 24h) : 1 out of 3 trains of DHRS



15

PSA result after change in SG op. seq.: Contribution to PLOHS frequency of time phases with different success criteria

- The dominant sequence represents loss of two trains of DHRS within 24h after reactor shutdown.
- Enhancement of heat removal capacity of a single train of DHRS in this time period has potential to reduce 99% of total PLOHS frequency.



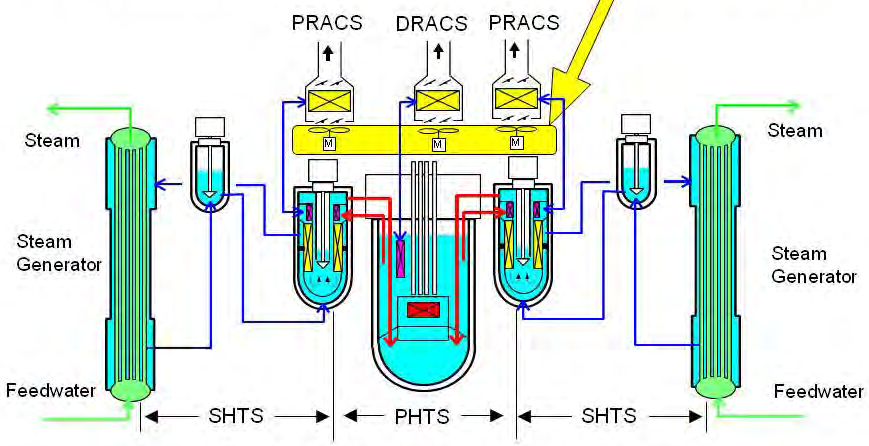
PLOHS-S	PLOHS sequences that occurs within 24h after reactor shutdown
PLOHS-L	PLOHS sequences that occurs after successful decay heat removal of 24h within the mission time of 1 month

*; ordered by contribution

PLOHS: Protected Loss Of Heat Sink, which includes insufficient heat removal capacity.

16

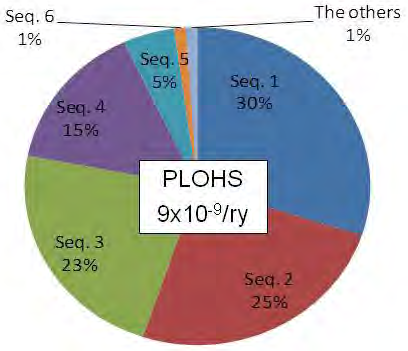
Design improvement: Non-safety-related AC blowers to enhance PRACS and DRACS capability



PRACS: Primary Reactor Auxiliary Cooling System
DRACS: Direct Reactor Auxiliary Cooling System
PHTS: Primary Heat Transport System
SHTS: Secondary Heat Transport System

17

PSA result: Major contributors to PLOHS frequency classified by combination of loss of mitigation systems



Seq. 1	Loss of passive cooling function in 2 loops & failure to start AC blower in the other loop
Seq. 2	Loss of all electric power & human error in manual damper operation
Seq. 3	Loss of passive cooling function in 3 loops (after 24h)
Seq. 4	Common cause failure of PRACS dampers & failure to start AC blower in DRACS
Seq. 5	Common cause failure of PRACS dampers & loss of active cooling function in DRACS AC
Seq. 6	Na leakage in one loop of DHRS & DHRS actuation signal failure in one loop & human error in manual damper operation & failure to start AC blower in the other loop

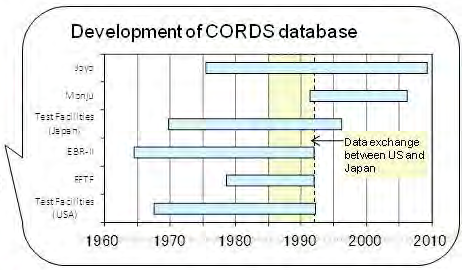
*; ordered by contribution

PSA showed quantitatively that introduction of AC blowers in both PRACS and DRACS can improve reliability of decay heat removal significantly.

18

Current status of reliability evaluation technology

- Reliability evaluation technology is indispensible for the level-1 PSA.
- Our effort has been made on collection of reliability data (i.e., operating time and number of failure instances) and on quantitative estimation of both the initiating event frequency and component failure rate in the sodium cooling system.
- However, cumulative component operating time is still short, compared with the target reliability level.



Frequency of sodium leak in PHTS, DHRS
Estimation : 10^{-2}~10^{-3}/ry
Target level :~10^{-4}/ry

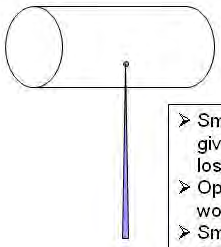
- Particularly concerning the sodium coolant boundary, in addition to further collection of the empirical reliability data, another effort has been made to evaluate the sodium leak probability depending on leak magnitude.

19

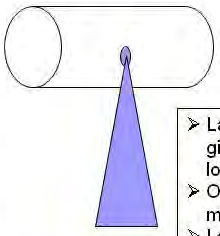
OECD/NEA Workshop on PSA for New and Advanced Reactors on June

Evaluation of sodium leak probability depending on leak magnitude

- In a loop-type SFR, it is important to evaluate an effectiveness of operator's recovery action to prevent primary-sodium-leak-related core damage sequences.
- Its effectiveness depends on the leak magnitude (see below).
- It is required to consider an effect of the leak magnitude on maintaining the reactor sodium level. But there was no method nor data to estimate quantitatively the sodium leak probability depending on the magnitude.
- It was needed to develop the method and data.



- Small leak from small hole gives long time margin to loss of safety.
- Operator's recovery action would be effective.
- Small leak may occur more frequently than large leak.



- Large leak from large hole gives little time margin to loss of safety.
- Operator's recovery action may be not effective.
- Large leak may occur less frequently than small leak.

20

OECD/NEA Workshop on PSA for New and Advanced Reactors on June

Outcome in this study

Sodium leak instances in SFRs in the world were investigated.
Based on these instances, the probability distribution of the sodium leak magnitude was estimated at the first time in the world.

What is the probability depending on leak magnitude?

Leak occurrence rate of the specific magnitude can be calculated with the following equation:

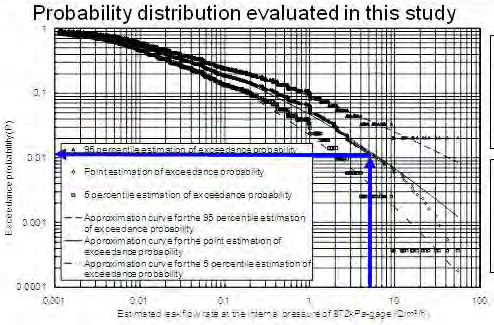
$\lambda_{spec}(/h)=\lambda_{general}(/h) \times P_{spec}$

$\lambda_{spec}(/h)$: Leak occurrence rate where the leak flow rate exceeds the specific rate

$\lambda_{general}(/h)$: Leak occurrence rate to all the range of the leak flow rate

P_{spec} : Probability where the leak flow rate exceeds the specific rate.

Probability distribution evaluated in this study

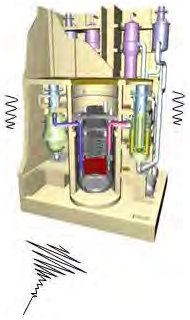


P_{spec} can be obtained from the left figure; e.g., the probability, where the magnitude exceeds ~5m^3/h at the internal pressure of 872kPa-gage, is ~0.01.

*) the leak magnitude in the this study is defined as the time-averaged volumetric leak flow rate (m^3/h), which depends on the internal pressure condition.

21

Seismic margin evaluation

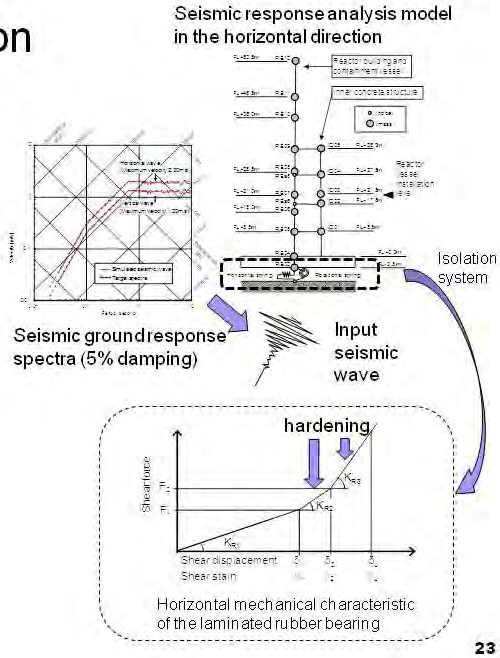


- ✓ The seismic event is an important external initiator of the core damage in Japan.
- ✓ After the Niigata-ken Chuetsu-oki Earthquake in 2007, the postulated seismic load for the JSFR seismic design was reconsidered, and it became severer.
- ✓ In addition, it was decided to develop newly a horizontal seismic isolation system for the JSFR.
  - ■ Laminated rubber bearings and oil-dampers.
- ✓ Currently, the site location of JSFR has not been determined yet.
  - ➢ The seismic hazard cannot be quantified.
  - ➢ Rather, the seismic margin of the JSFR should be evaluated by conducting a seismic fragility evaluation.
- ✓ So, we conducted the seismic fragility evaluation of principal structures and components in terms of core damage prevention.

22

Seismic fragility evaluation

- ✓ Seismic fragility was evaluated based on the seismic response analysis.
- ✓ Input wave: we assumed the seismic ground motion 1 to 5 times as large as the postulated seismic load.
- ✓ Seismic isolation characteristics: we considered the seismic isolation effect and the hardening effect of the laminated rubber bearings in the seismic isolation system.
- ✓ Seismic fragility evaluation method:
  - □ Probabilistic seismic response analysis was applied for principal structures.
  - □ Safety factor method was applied for principal components.



23

Seismic fragility and margin evaluation result (1)

- ✓ Based on the median seismic fragility curve, the seismic margin can be evaluated by a median Peak Ground Acceleration (PGA).
- ✓ The median PGA is a PGA that gives a conditional probability of 0.5 in the median fragility curve.
- ✓ The median PGA of a failure event indicates that when an earthquake equivalent to the median PGA takes place, the failure happens at a probability of 50%. So, it can be said that this failure can be prevented against an earthquake up to the median PGA in a realistic estimation without any uncertainty and margin.

- ✓ When we evaluate the seismic margin by the median PGA, it can be said that principal structures and components in JSFR have a seismic margin that is at least a factor of 3.

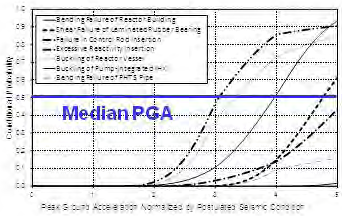


Fig. Median fragility curves for the principal structures and components

Seismic fragility and margin evaluation result (2)

- ✓ Based on the 95% non-exceedance seismic fragility curve, the seismic margin can be evaluated by a High Confidence Low Probability of Failure (HCLPF).
- ✓ HCLPF in this study is defined as a PGA that gives a conditional probability of 0.05 in the 95% non-exceedance fragility curve.
- ✓ HCLPF of a failure event indicates that when an earthquake equivalent to the HCLPF takes place, the failure happens at a probability not greater than 5% with a confidence level of 95%.

- ✓ As the term itself shows, HCLPF in this study is a PGA that gives a low probability of failure with a high confidence level.
- ✓ If the normalized HCLPF value is greater than 1, it involves that there is a sufficient margin against the postulated seismic condition.

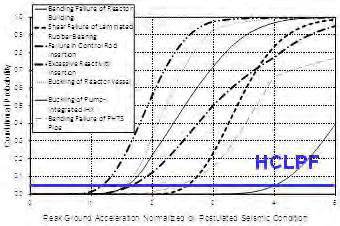


Fig. 95% non-exceedance fragility curves for the principal structures and components

Conclusions

JAEA implemented the preliminary level-1 PSA of JSFR.

1. Internal events

- ✓ Typical core damage sequences (i.e., ATWS, LORL and PLOHS) were evaluated.
- ✓ The PSA result showed that the total CDF becomes ~2.3×10^{-8}/ry. This is less than the both requirements on CDF and CFF; i.e., 10^{-6}/ry and 10^{-7}/ry, respectively. Based on this, we judged that JSFR can achieve the risk targets for internal initiators.
- ✓ The PSA also served to the safety design modification of DHRS.

2. Development of reliability evaluation technology

- ✓ We studied on the quantification of the sodium leak probability depending on the leak flow rate in addition to failure rate estimation of sodium-related components.
- ✓ Sodium leak instances in SFRs in the world were investigated. Based on those instances the probability distribution of the sodium leak flow rate was estimated at the first time in the world.
- ✓ This study serves to evaluate the effectiveness of operator's recovery action in the sodium-leak-related core damage sequences.

26

Conclusions

3. External events

- ✓ Earthquake is examined as an important risk contributor in Japan.
- ✓ We evaluated seismic fragility and seismic margin of the principal structures and components of JSFR, with considering the mechanical characteristic of the horizontal seismic isolation system.
- ✓ It was confirmed that they have sufficient margin against the postulated seismic condition.

27

Risk-informed analysis as a support to the preliminary design of the CEA GFR2400

F. Bertrand[1], C. Bassi[1], F. Bentivoglio[2], A. Messié[2], P. Azria[1]and M. Balmain[3]

1 CEA, DEN, DER, F-13108, Saint-Paul-Lez-Durance, France, frederic.bertrand@cea.fr

2 CEA, DEN, DER, F-38054, Grenoble, France, fabrice.bentivoglio@cea.fr

3 EDF, R&D Division, Industrial Risks Management Department, F-92140, Clamart, France, michel.balmain@edf.fr

Abstract

The integration of safety issues in the early phase of the design of a 4th generation reactor of the concepts is expected. For this purpose, probabilistic insights are increasingly employed in the safety demonstration in combination with the deterministic approach in the frame of a so-called risk informed approach. The present paper deals with the safety assessment of the preliminary design of the GFR2400 developed by CEA and how it has been improved in order to fulfil deterministic criteria as well as to reach a risk level comparable to the generation III reactors. Considering the results obtained with a preliminary level 1 PSA (L1PSA) model, it emerged that an increased reliability of the DHR function in high pressure conditions (not corresponding to a LOCA) was suitable to reduce the overall core damage frequency. On the other hand, some small break LOCA situations were not adequately mitigated according to the line of protection deterministic method. Both issues have been solved by design improvements. In addition, this final L1PSA model, characterized by success criteria based on transient calculations performed with the CATHARE2 code and performed in a perimeter extended to all representative internal initiating events (IEs) at full operating power, permitted to propose design evolutions that did not increase significantly the CDF. In the same time, those evolutions enabled the DHR system to increase its redundancy level as required in the deterministic approach. Finally, a modified design has been reached implying a more extended covering of various accidental situations by means of a progressive DHR operating strategy.

Keywords GFR2400, Risk-informed, Preliminary design

1. Introduction

The present paper is aimed at underlining in what the risk-informed analysis carried out on the 2400 MWth french gas-Cooled Fast Reactor developed at a pre-conceptual design stage by the CEA has permitted to improve the safety design of the reactor. After a brief presentation of the Gas cooled Fast Reactor (GFR) as designed at the end of 2007 and taken as the reference in the first step of the studies presented here (initial design), the safety approach adopted is then presented. The following part of the paper is dedicated to the deterministic study insights provided by the line of protection method (LOP) and the transient analysis. Then, the main results of the level 1 PSA (L1PSA) elaborated to support the reactor design are presented. Finally the design evolution retained

(according to the conclusions of both the PSA and the deterministic analysis) and their benefits in term of safety case and in terms of design (advanced design) are analyzed in the last part of the paper.

2. Elements on initial reactor design and its DHR strategy

The detailed GFR design is presented for instance in reference (Malo et al., 2008), and only the useful features to the understanding of this paper are presented here.

2.1 Main design options

The initial design options presented here result from a pre-viability design report released at the end of 2007. The operating point of the 3-loops reactor at full nominal power enables to convert the 2400 MWth delivered by the core in 1100 MWe, partly by secondary circuit turbomachineries (auxiliary alternators: 3 x 130 MWe) and partly by a steam turbine (main alternator: 1 x 730 MWe) settled in the ternary circuit (Fig 1). The resulting cycle efficiency is very close to 45 %. The secondary circuit is filled with a mixture of helium (to favour the heat exchanges) and nitrogen (to favour the efficiency and the design of the turbomachineries); the ternary circuit is filled with water, vaporized in 3 steam generators according to a classical Rankine cycle. The primary system arrangement (Fig 2) includes the reactor vessel, the 3 main primary loops (PCS loops) and their heat exchangers (IHX) as well as the DHR loops permitting to cool the core in accidental situations. Actually, there are three loops, so-called, Reactor High Pressure cooling system (RHP) and a loop for the low pressure situations (RLP). The secondary side of the DHR loops, each one being able to remove 100 % of the decay heat after the reactor scram, is filled with water pressurized at 10 bars. These secondary DHR loops are cooled via an exchanger immersed in a pool. Each pool associated to a loop can remove the residual power during 24 hours without being refilled. Moreover, all the previous components are enclosed in a close containment (CC) which keeps the primary inventory in case of Loss Of Coolant Accident (LOCA).

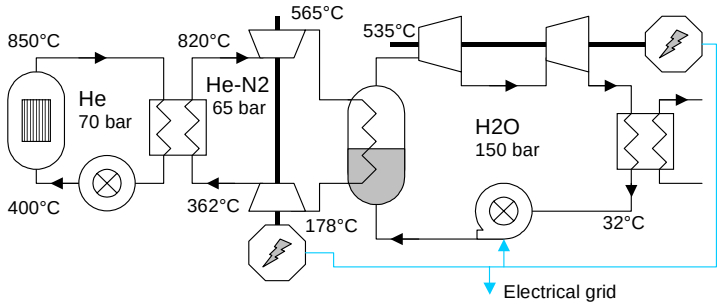


Figure 1: Nominal operating point of the GFR

At the hot spot of the core, the clad temperature is equal to 1000°C and the fuel temperature is about 1380°C in nominal conditions. The fuel plates are arranged in baskets superposed in hexagonal tubes (TH) permitting to differentiate the flow rate depending on the power factor distribution within the core. The height of the core is of 2,35 m and its diameter is of 3,8 m, thus corresponding to a power density of about 90 MW/m3. The head loss across the core has been minimized at a value of 1,4 bars at the nominal regime in order to favour natural circulation in DHR regime.

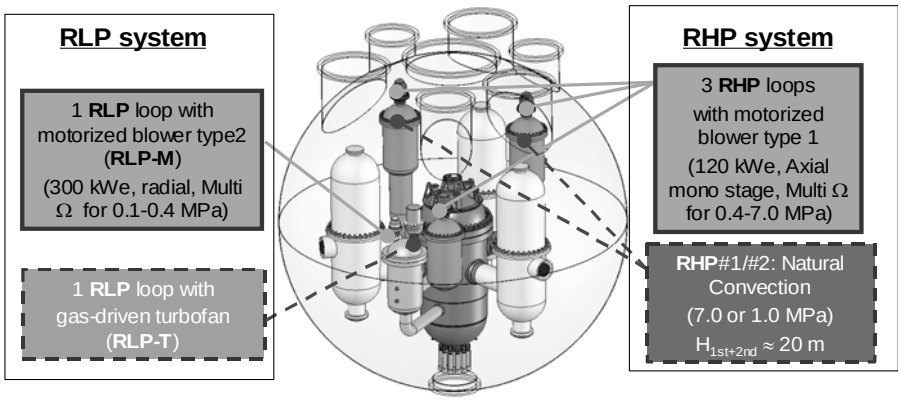


Figure 2: Arrangement of the primary circuit components (from Bassi et al., 2010)

2.2 Initial strategy for the decay heat removal (DHR)

Considering the power density of the GFR core and its low thermal inertia (compared to the HTR) and that of the coolant as well (compared to the SFR), the decay heat removal relies on a gas circulation (natural circulation as far as possible) across the core but not on solutions based on thermal inertia plus conduction/radiation. The DHR operating depends on the accidental situation to face (Fig 3). The selected combination of systems takes into account the two main accidental situation families: the pressurized situations (intact primary boundary) and the depressurization situations resulting from a LOCA. In addition, the situation related to a primary pressure reaching around 0.1 Mpa, corresponding to a combination of LOCA and a leak of the CC, has been considered only after 24 hours.

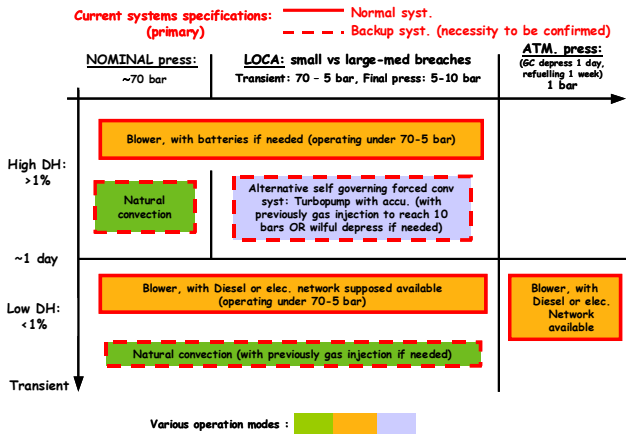


Figure 3: Sketch of the initial DHR operation (from Malo et al., 2007))

3. Risk-informed approach retained for the GFR2400

Beyond a fundamental set of safety objectives defined by IAEA (IAEA Safety Standards Series NS-R-1) for all nuclear plants, as fourth generation reactors, the GFR must include specific qualitative objectives aimed to increase public confidence in their safety (IAEA Safety Report Series No. 46). Among others, the need of minimal emergency protection action of the population around the site is

aimed. The general safety objectives can be declined as release targets according to different operating conditions as well as in term of probabilistic targets (p.e, core damage frequency, CDF).

3.1. Governing principles

The governing principles of the safety approach are grounded on the defense in depth principle (DiD), the existence of physical barriers, the safety functions aimed at protecting these barriers and the ALARA principle regarding the radiation protection of the facility's staff. The physical barriers enabling the fission product to be confined are, successively, the cladding of the fuel assembly, the primary circuit boundary and finally the containment.

3.2. Safety analysis methodology

The adequacy of the provisions retained in the design can be judged using a variety of deterministic and probabilistic methods and this is further discussed in this section. In general terms, the plant is deterministically designed against the identified list of the operating conditions using well-established design criteria to ensure suitable safety margins. These margins are built thanks to various pessimistic assumptions regarding the availability of the safety components/systems (p.e, single aggravating failure, reactor initial state and lack of power) and regarding the physical uncertainties. L1PSA has also been performed to verify that there are no vulnerable areas in the design with the potential for high-risk sequences (Bassi et al., 2010). In this way, L1PSA can identify any requirement for additional preventative or mitigative design features. PSA enables weak points in the design of the reactor to be identified, due to its broad framework and its exhaustive purpose. As a result, a homogenous safety design should result from a valuable use of PSA results avoiding a family of sequences contributing too greatly to the overall risk number. This study has been performed using an iterative process with the design. Finally, the PSA could help to locate the IEs and the resulting sequences in the risk domain for IEs which are questionable and/or difficult to categorize. The development and the integration of the PSA results alongside the deterministic safety analysis has begun in the conceptual phase, once the basic design have been defined even if the knowledge of reliability data implied to pay a particular attention to the uncertainties on data. However, valuable results without respect to absolute quantification can be used by differentiating relative results in order to prioritize the design studies and improvements of the reactor. A particular point of interest is also that it contributes to the demonstration that sequences leading to important and/or early releases are practically eliminated. Moreover, regarding severe accidents, it provides a preliminary assessment of the safety improvement resulting from the planned mitigation measures as well to prioritize the R&D efforts.

3.3. Interactions between safety assessment and design process

The classical methodology and rules used in the deterministic safety analysis briefly described in the previous sub-section are usually used and presented in the safety case. Regarding the GFR2400, the design was not yet consolidated (especially at its initial stage) and the reference architecture and dimensionning of the system could be revised on the basis of the results of the safety studies. Moreover, the performance of the safety systems has been assessed first with simplified transient calculations and simplified deterministic rules. By the way, the safety studies carried out by taking into account an adequate set of transients and combination of deterministic and probabilistic criteria was use to provide improvments, simplifications and verification of the reactor design according to the process described on Figure 4 (Devictor et al., 2005).

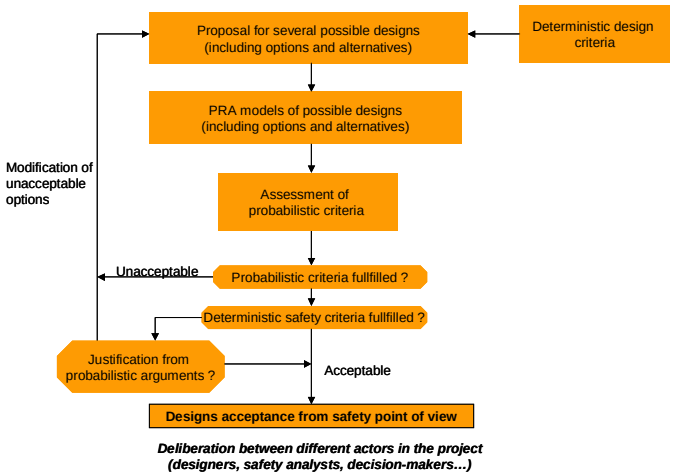


Figure 4: Sketch of the interaction between design process and safety insights

4. Feedback of safety preliminary analysis on initial DHR system design and operation

The preliminary analysis performed on the initial stage of the design and with the DHR strategy presented above are already presented in a detailed way by Bertrand et al. (2008) and Malo et al. (2009) regarding the overall approach and results ; moreover, detailed results of the first version of the GFR2400 PSA dedicated to the initial design are available in (Bassi et al., 2008). Therefore, only specific insights that permitted to point out the features to improve in the design are reported here.

4.1 Deterministic approach insights

The transient analysis, performed thanks to the CATHARE2 code permitted to assess the provisions foreseen in order to cope with the acceptance criteria of the reactor (on the fuel, the cladding and on the vessel and the IHX) as well as to assess the performance of the DHR loops. Several single aggravating failures have been considered in the calculations. A static qualitative approach of the initial strategy proposed in Figure 3 indicates that the core can not be cooled by any system if the CC is not tight within the first 24 hours after a LOCA because the systems foresseen in this situation are not dimensionned for the residual power level of the first 24 hours after the occurence of the break. In an intermediate stage of the design presented by Bassi et al. (2010), a single loop operating in forced convection was foreseen. However, in case of break located on this loop combined with the tightness failure of the CC, the system could not fulfil the acceptance criteria in case of an aggravating event associated to the failure of the intact RLP loop (Fig. 3). However, transient calculations have shown that as soon as the depressurisation transient is over, even a loop affected by a LOCA can cool efficiently the core. Whatever the level of pressure (high or low), the single failure criterion is respected with only 2 loops as soon as only the cold-duct is broken ; the double-ended breach of the cross-duct (cold and hot ducts) belongs to the beyond design domain whose situation are not subject to any additional aggravating event. Moreover, the LOP application has indicated that the control of a small break LOCA classified in the 3rd category of operating conditions combined with the failure of the forced convection (complex sequence of 4th category) is not enough protected by the systems. The CATHARE2 calculations have confirmed that this 4th category situation would induce a core degradation. As a conseqence, in case of failure of the forced convection means, it is proposed to cool the core with a natural convection flow driven, thanks to a gas release from three nitrogen accumulators (Bertrand et al., 2008). In this illustration (Fig. 5), those accumulators are triggered when the primary pressure reaches 20 bars and a final pressure in

the close containment around 10 bar is sufficient if the accumulators are filled with nitrogen. This gas being more dense, the mass flow rate is higher than with helium assuming the same mole number of gas.

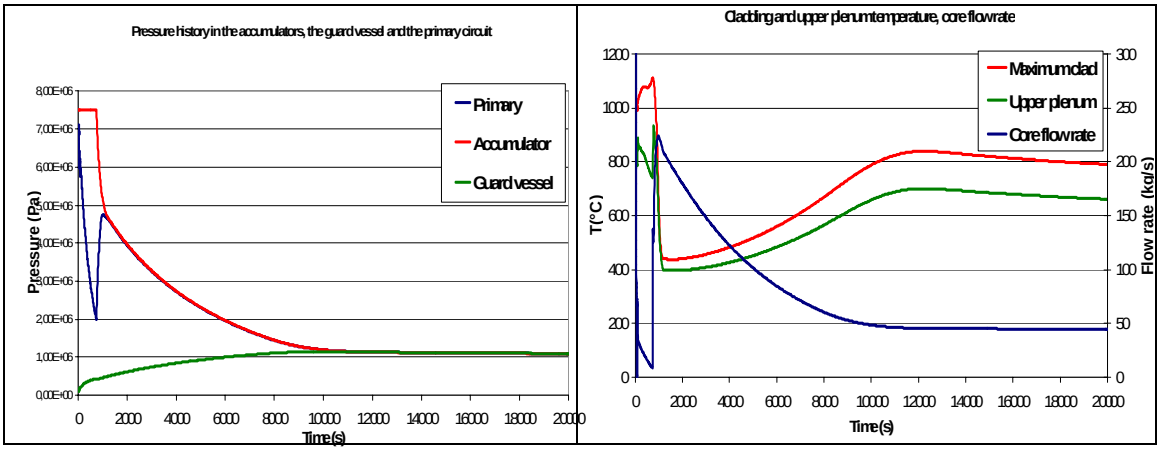


Figure 5: Control of a 2 in LOCA in natural circulation by means of nitrogen injection

Moreover, the study of the bounding large break LOCA equal to 10 inches combined with the failure of the starting of a DHR blower (aggravating event) would lead to a core degradation if the valve of the loop associated to the blower that does not work stays open. Such a flow path configuration would lead to a large by-pass of the core by a reverse flow in the open DHR loop. The feedback on design is to foresee that the blower and the valve are not supplied on by the same Diesel generator. The PSA enabled the reliability of such an additional provision to be checked.

4.2 PSA insights on the initial design

The main benefits of the use of PSA during the design process are related to the identification of plant vulnerabilities, of inter-systems dependencies and potential Common Cause Failures (CCFs), and to the examination of risk benefits from different design options. The probabilistic insights will help with the design optimization of safety systems (particularly in terms of redundancy and diversification), and with the checking of the design homogeneity from safety standpoint and, in the near future, from cost to safety benefit concern. The IEs and their occurrence frequencies, considered in this fist version of the PSA (Bassi et al., 2008) are consistent with those investigated in the deterministic approach presented before; an inadvertent reactor trip which is a category 2 IE has also been studied. The failure of the various systems have been modelled with fault trees connected to event trees modelling the accidental sequences, thus permitting the whole quantification of the Core Damage Frequency (CDF) as usual in a L1PSA. When support calculations of the sequences were not performed, the final state leading to core damage was considered to be the loss of a main safety function. The various sources of uncertainties were taken into account as follows :

- the reliability of natural convection thanks to a specific methodology based on uncertainties propagation in thermalhydraulic calculations ;

- the technological uncertainties on very innovative components thanks to a risk factor taking into the possible unability to design or to manufacture the component ;

- the physical uncertainties due to the risk for a component to not fulfill its mission.

Thanks to its large scope, the PSA permitted to screen all the combination of flow-path configurations leading to a core by-pass. As a result, it enabled the configuration aforementionned

to be identified and to be corrected by a design provision. Moreover, starting from a reference configuration (large core by-pass) or architecture of support systems, successive modifications were performed in the probabilistic model according to the preponderant minimal cut-sets (MCs) screening. In the light of the MCs set, it appears that (Fig. 6):

- the increase of voting systems redundancy (impact on scram and DHR actuation) leads to a CDF reduction by a factor of 2 (case#1 vs. reference design);
- the diversification of the signal leading to the DHR actuation enables a factor of 9 to be gained, compared to the first alternative design (i.e. case #1); in the model, a triple instrumentation for core inlet temperature measurement is added;
- a slight decrease of CDF (case#3 vs. case#2) with a redundancy implementation for electrical supply of the DHR isolating valve in order to avoid a failure to close when an electrical train is lost.

The first lessons emerging for the design and for the demonstration of safety robustness are that DHR systems for pressurized situations should be made more robust. However, some kinds of dependencies for ensuring the mission success of the DHR system still exist, demonstrated by the contribution of common cause failures for primary to secondary DHR circuits exchangers and isolating valves. This dependency is increased due to the dual convection scheme through these dedicated loops (i.e. valves and exchangers are common for the forced and natural convection modes). Some elementary (i.e. technological) and/or integrated (i.e. strategy improvement) solutions could be implemented: respectively increased diversification for valves and exchangers, and/or by incorporating the possibility of using the normal loops in the first place in the DHR strategy.

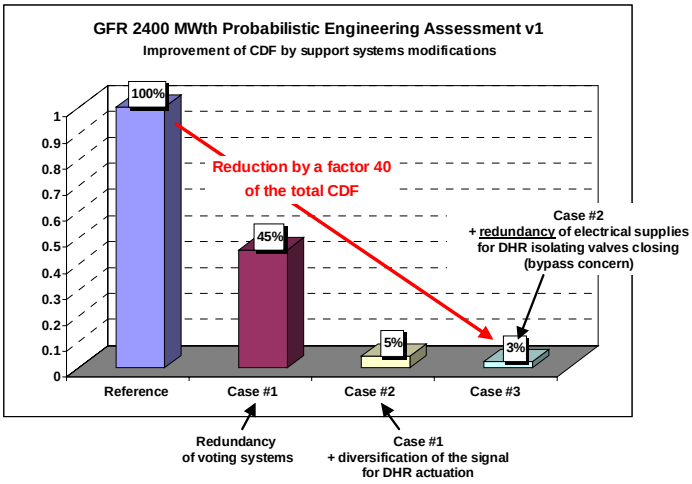


Figure 6: Risk reduction process implemented thanks to the PSA

5. Safety assessment of advanced design

Considering the already significant number of loops connected to the reactor vessel, the need for further diversification of the DHR system (underlined by the first version of the L1PSA) has been addressed by considering the possibility to use the normal loops as a first line of defence instead of adding supplementary loops. The DHR operating depends on the accidental situation to face (Figure 7 and Figure 8). The selected combination of systems takes into account the two main accidental situation families: the pressurized situations (intact primary boundary) and the depressurization situations resulting from a LOCA. The means represented in the upper part of the sketch are used in

priority if available (depending on the pressure range considered), the means represented below being used if those above have failed. In addition, the situation related to a primary pressure reaching around 0.1 MPa, corresponding to a combination of LOCA and of a leak of the CC, has been considered. It is worth noticing that the DHR based on natural circulation with a heavy gas for small breaks relies on the presence of the CC insuring a back-up pressure of about 1 MPa. This CC permits also to dimension DHR blowers with a low power, compatible with an emergency electrical power supply, delivered by Diesel engines.

5.1 Deterministic approach insights

Only one loop being available in the DHR system, both for the powered forced convection as well as for a turbine driven blower, there was no redundancy in the RLP system. Especially in case of failure to open this loop in case of failure of the CC, no system would remain available to cool the core. Therefore, a second loop has been added in the RLP that fulfils the single failure criterion knowing that, as soon as the depressurization is over, the flow rate in the loop would be equal to its nominal flow rate according to first transient calculations.

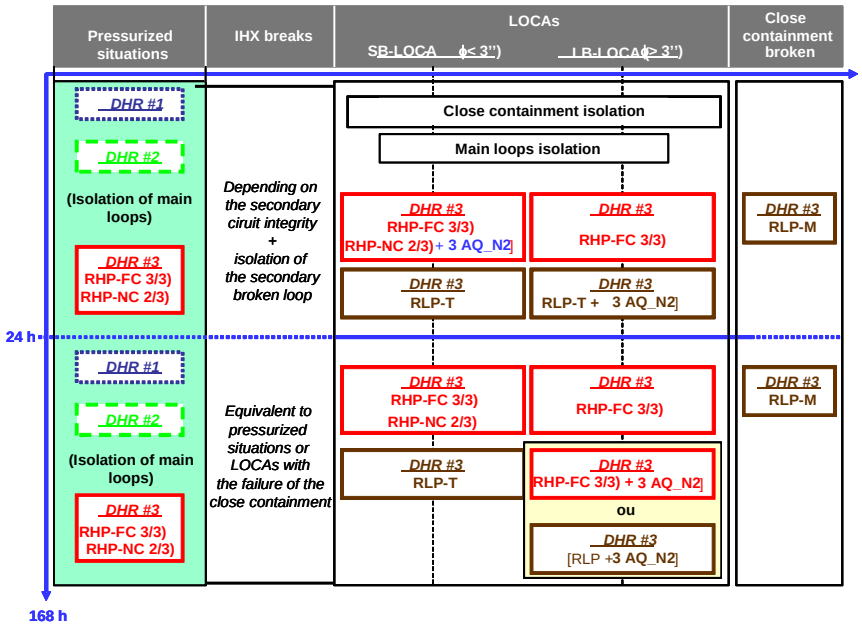


Figure 7: Sketch of the DHR operation (DHR#1 in blue on Fig.8,
DHR#2 in green on fig. 8, DHR#3 (dedicated means in CC) on Fig.8)

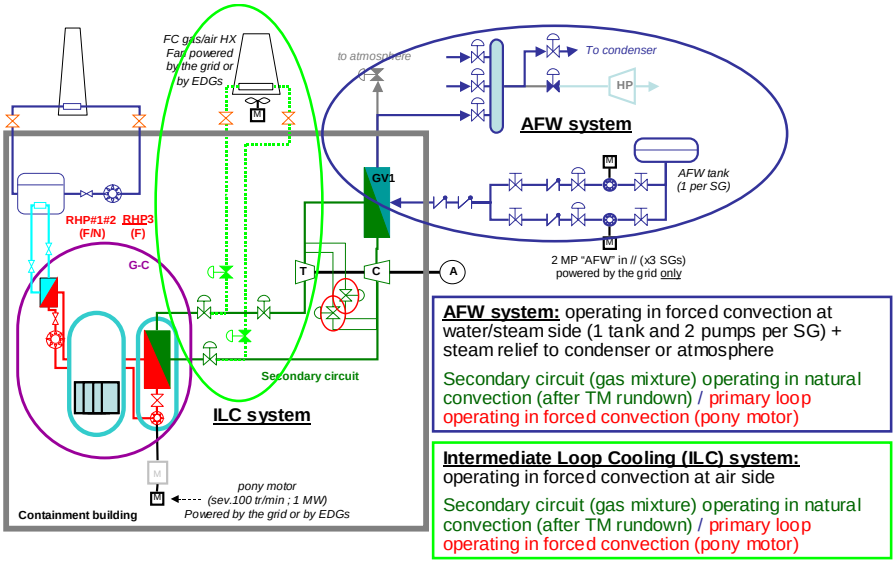


Figure 8: Sketch of various DHR means

5.2 PSA insights

In order to illustrate the complementarities of the insight mentioned above by considering the level of redundancy of a sub-system contributing to the DHR, the possibility to simplify the RHP system and to replace the turbine driven blower by a motorized blower has been investigated and quantified from a risk impact point of view (Bassi et al., 2010). The reduction of the technological uncertainty resulting from the innovative feature of the turbine driven blower compensate the increase of the CDF due to CCFs by adding another motorized RLP (Fig. 9). Finally, the gain is about 2 % on the overall CDF. On the contrary, the suppression of a loop (the dual loop) on the RHP system has been assessed to induce an increase of the CDF of about 26 %; this increase appeared acceptable considering the overall risk level and the simplification of the primary circuit. The interest to have a dual operating loop able to perform natural and forced convection does only reduce the risk of about 2 %. Finally, the overall CDF is of the same order of magnitude of that targeted for generation III reactors ; more precisely, the mean reference value of the CFD is around 1.5 10^{-6} /(y.r) including a well-balanced risk contribution of various IE families (Bassi et. Al, 2010) with the heaviest one being the small break LOCA reaching 22 % of the whole risk.

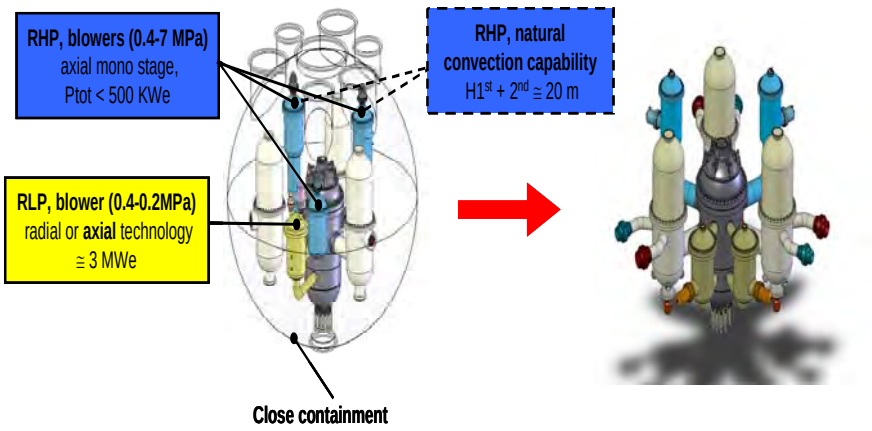


Figure 9: Design evolution thanks to the risk-informed analysis

6. Conclusions

The preliminary design of the GFR2400 has been carried out by using a combination of the classical deterministic safety approach with a L1PSA performed in order to go with the design process in the frame of a so-called risk-informed analysis. The L1PSA has been carried out in order to match with the pre-dimensioning process and its associated potential showstoppers. As a consequence, its first version was focused on the events affecting the primary circuit, namely the two typical situations (LOCA and pressurized situations) already studied in the transient analysis. The main lessons learnt from the preliminary risk-informed analysis carried out at this early stage of the design has led to reinforce the redundancy in the signal elaboration able to actuate the safety systems and to prevent the wrong flow path configurations. In particular, the systematic consideration of all the possible sequences leading to core by-pass through the L1PSA enabled the various configurations to be investigated by means of transient calculations. Moreover, the lack of progressiveness of the safety architecture required improvements in order that the GFR be more protected from frequent events than from hypothetic events. The answer provided to this issue has led to retain provisions in order to remove the residual heat thanks to the normal loop and to foresee nitrogen injection in the primary circuit in order to be able to control the SB-LOCA in a natural convection regime.

Finally, the extended analysis carried out on the advanced stage of the design of the reactor and its evolved DHR strategy, permitted to confirm the design options retained (possibility to remove the heat with the normal loops operating in natural convection) but also to simplify some sub-systems when possible (suppression of one dedicated RHP loop and suppression of the turbine driven blower) and to reinforce some others when necessary (addition of one RLP motorized loop). Some points would need further investigations in order to consolidate the safety margins, like the possibility to control some unprotected transients with the normal loops and like the actuation of the natural circulation in case of LOCA. By assuming that the results obtained up to now will be confirmed by more in-depth studies, the CDF obtained for the GFR2400 would close to that of EPR™. The approach briefly presented here has been tested for the GFR2400 and considering its interest for design and safety, its application is foreseen for the future SFR prototype under development at CEA by roughly following the same principles.

References

Assessment of Defence in Depth for Nuclear Power Plants, IAEA Safety Report Series No. 46, 2005.

C. BASSI et al., (2010), Level 1 probabilistic safety assessment to support the design of the CEA 2400 MWth gas-cooled fast reactor, Nuclear Engineering and Design,Vol. 240, Issue 11, November 2010, pp. 3758-3780.

C. BASSI et al., (2008), Application of PSA in support to the design of CEA 2400 MWth gas-cooled fast reactor, Proceedings of PSA08, Knoxville TN, USA, September 7-11 2008.

F. BERTRAND et al., Preliminary Safety Analysis of the 2400 MW Gas-Cooled Fast Reactor, proceeding of ICAPP 2008, Anaheim, USA, June 8-12, 2008.

N. DEVICTOR et al., (2005), CEA program of work to carry out a level 1 PSA on the gas-cooled fast reactor, Proceedings of PSA'05, San Francisco, CA USA, September 11-15 2005.

JY. MALO et al., (2007), The DHR system of the GFR, preliminary design and safety analysis, Proceedings of ICAPP 2007, Nice, France, May 13-18, 2007.

JY. MALO et al., (2008), Gas Cooled Fast Reactor 2400 MWth, end of the preliminary viability phase, Proceedings of ICAPP 2008, Anaheim, CA USA, June 8-12, 2008.

Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series NS-R-1, 2000.

RISK-INFORMED ANALYSIS AS A SUPPORT TO THE PRELIMINARY DESIGN OF THE CEA GFR 2400

F. Bertrand[1], C. Bassi[1], F. Bentivoglio[2], A. Messié[2], P. Azria[1] and M. Balmain[3]
frederic.bertrand@cea.fr

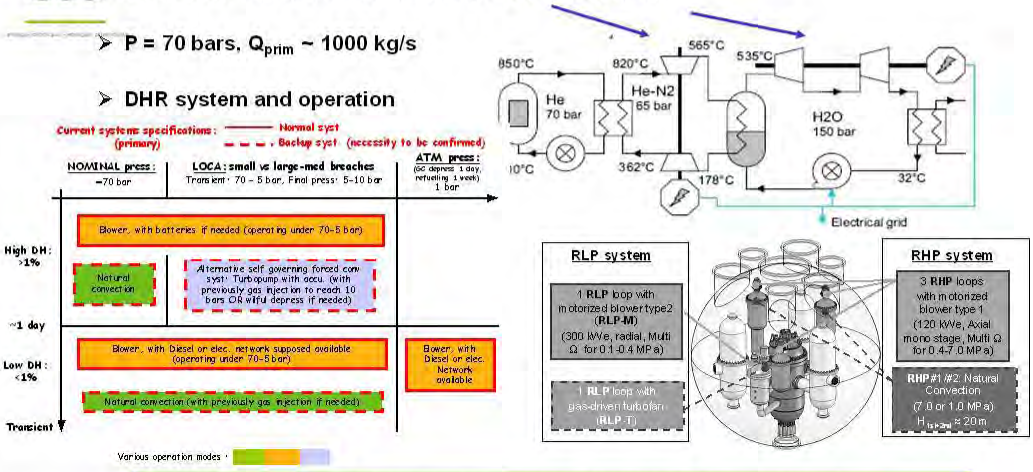
1- CEA, DEN, SESI, Cadarache, F-13108 Saint-Paul-lez-Durance, France
2- CEA, DEN, DER, F-38054, Grenoble, France
3- EDF, R&D Division, Industrial Risks Management Department, F-92140, Clamart, France

Outline

- Main features of the GFR 2400 (as designed at the end of 2007)
- Risk-informed (RI) approach retained for the analysis of the GFR2400
- Feedback of the RI analysis on the early system design and operation
- RI analysis on the so-called advanced design
- Conclusions and prospect

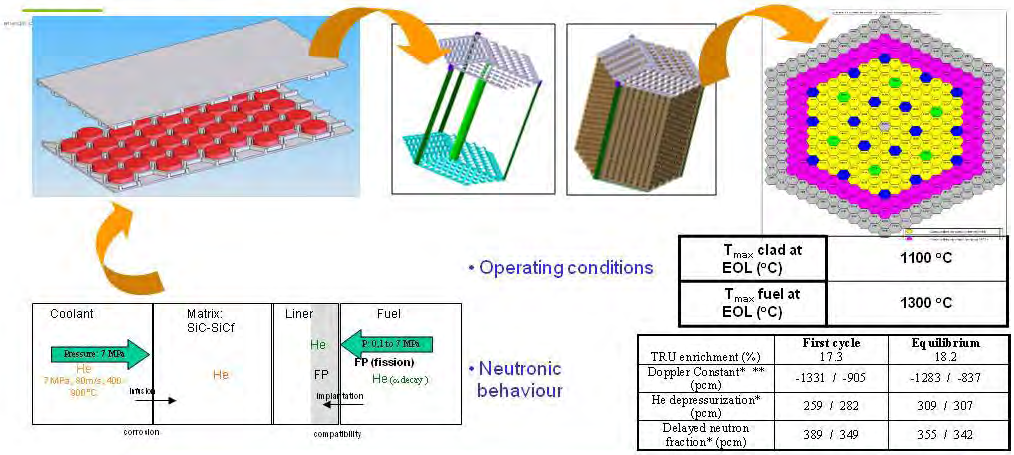
Main features of the GFR 2400 (early design of 2007) (1/2)

- Main features of the GFR 2400 systems
- PCS : 2400 MW th → 1120 MWe = 3 x 130 + 730 MWe
- P = 70 bars, Q_{prim} ~ 1000 kg/s
- DHR system and operation



Main features of the GFR 2400 (design of 2007) (2/2)

- Main core features
  - Core design : power density 91 MW/m^3, 246 fuel assemblies + 24 CR assemblies
  - $h_{fis}/D \sim 0.4 \rightarrow h_{fis} = 2.35$ m



- Operating conditions

T_{max} clad at EOL (°C)	1100 °C
T_{max} fuel at EOL (°C)	1300 °C

- Neutronic behaviour

	First cycle	Equilibrium
TRU enrichment (%)	17.3	18.2
Doppler Constant* ** (pcm)	-1331 / -905	-1283 / -837
He depressurization* (pcm)	259 / 282	309 / 307
Delayed neutron fraction* (pcm)	389 / 349	355 / 342

Overview of the risk-informed approach retained (1/2)

1- High level governing principles

- ✓ Defence in depth, Principle of physical barriers, safety functions

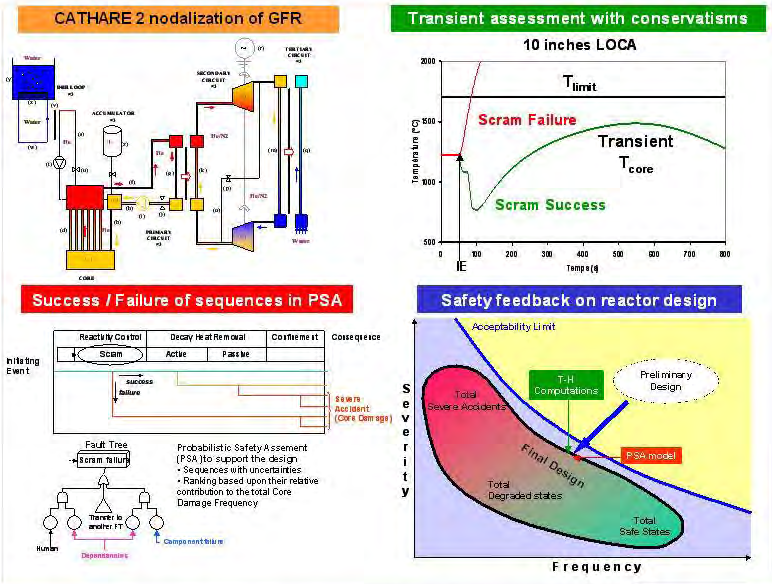
2- Preliminary analysis of operating conditions in a deterministic frame

- Objectives : assessment of the performance and of the robustness of the DHR system (DBA), including cross failures (DEC)
- Situations considered :
- DBAs : 100 % NP + IE + single aggravating failure
- DEC : → 100 % PN + IE (DEC)
  → Complex sequences → 100 % PN + IE (DBA) + multiple failures

3- Level 1 PSA as a support to the reactor design

- Identification of plant vulnerabilities, system interdependencies and CCFs
- Risk benefits of various design options, optimization of redundancy and diversification
  - IEs consistent with the deterministic analysis (LOOP, LOFA, LOCA, reactor trip)
  - All EIs taken into account in the last version of the PSA (for advanced design)

Interaction between design process and safety assessment (2/2)



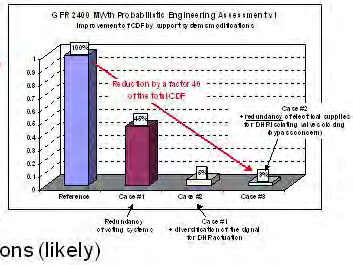
Feedback on early design and on operation (1/2)

- **Deterministic approach insights on the initial design**

- A system dimensioned to cool the core in case of failure of the close containment has to be foreseen (RLP performance to reinforce)
- The failure of a DHR RHP blower combined to the fail open of this loop leads to an unacceptable core by-pass→ Fail safe option (reliability has been checked with the PSA)
- Better mitigation of SB-LOCA thanks to natural convection (nitrogen injection) → LOP insight

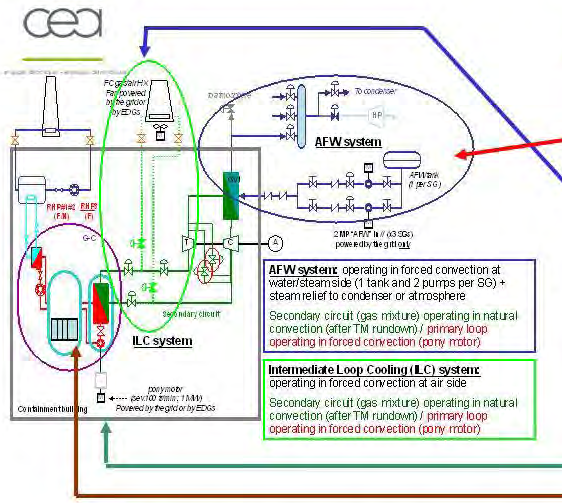
- **PSA insights on the initial design**

- Level of redundancy and of diversification of the signal actuating the DHR system to reinforce
- Assessment and reduction of core-by pass risk
- Necessity to diversify the DHR system due to loop and heat exchanger dependencies in forced flow and natural flow regimes for pressurized situations (likely)



Feedback on early design and operation (2/2)

- Evolution from early to advanced design



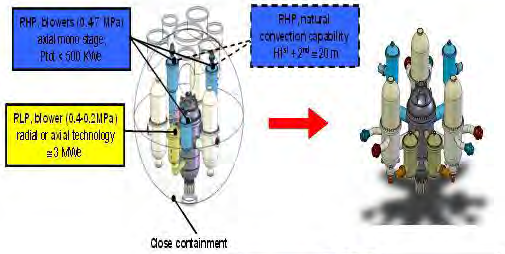
→ Use of normal loops to remove the decay heat when available

- Ternary circuit and SG adaptation
- Dedicated gas/gas loop with an air cooler (cold source diversification)
- Addition of pony motors to the primary blower and secondary loops operating in natural convection after turbomachinery rundown
- 3 nitrogen accumulators triggered around 15 bar

Feedback on DHR system advanced design

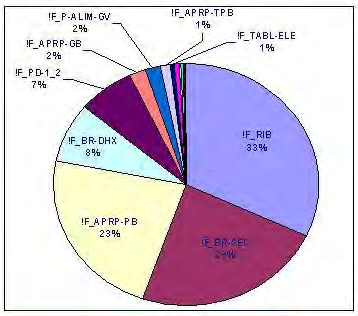
- Deterministic approach insights

- Addition of a RLP loop (single failure criteria)
- Control of unprotected loss of flow without loss of core geometry thanks to normal loops



- PSA insights

- Acceptable increase of risk (CDF) if a RHP loop is suppressed (design simplification)
- Negligible risk reduction for RLP diversification
- Well-balanced design versus the various IEs
- CDF roughly of the same order of magnitude than generation III reactors (risk reduction of 1000 compared to early design and DHR strategy)
- Severe accidents R&D priorization and possibility to perform a L2PSA



Conclusion and prospects

- Risk-informed analysis as performed for the GFR2400 has proven its benefits on design process on the following point :
  - Building of the safety architecture by comparing various options with a quantitative single criterion (CDF)
  - Early consideration on uncertainties
  - Early interest on signal elaboration and system triggering, requirements on support systems and not only on performance assessment of systems
  - Assessment of passive systems integrated in the PSA

- Prospects
  - Application of this approach to other CEA GEN IV reactor design
  - Integration of human reliability on the basis of a dedicated approach developed at CEA

Overview of VHTR's PSA Approach in Korea

Seok-Jung HAN

Integrated Safety Assessment Division, Korea Atomic Energy Research Institute, 1045 Daedeokdaero, Yuseonggu, Daejeon, 305-353, Korea, hanseok@kaeri.re.kr

Abstract

Probabilistic safety assessment (PSA) is a key issue of the safety evaluation of VHTR, which is useful tool to show the probabilistic nature of the safety performance. An inherent PSA approach applied to VHTR should be developed in order to consider its safety features (no severe core damage and small radiation release). The identified issues to develop a PSA approach were introduced; the definition of the end states of accident sequences (risk metrics), the identification of initiating events, and the modeling of accident sequences. Additional technical issues, especially the radiation release characteristics, should be resolved in order to complete the proposed approach. Further study will be engaged for this purpose. Although the current approach is incomplete, it provides overall insights to be able to understand VHTR's PSA.

Keywords: very high temperature reactor (VHTR), probabilistic safety assessment (PSA), risk metrics

1. Introduction

A very high temperature reactor (VHTR), which is a generation IV's reactor for providing a high temperature heat source such as process heat to generate hydrogen or electricity generation, is under development now in Korea (Chang, 2007). A primary candidate of VHTR is a gas-cooled graphite reactor with three layers ceramic coated fuel elements, which has good characteristics of the fuel performance and the inherent safety. The safety features of VHTR are mentioned as simplified safety functions with no severe core damage and the absence of large release of radioactive materials in any accident conditions.

The evaluation of safety performance is a key issue of VHTR's development. It is expected that the probabilistic safety assessment (PSA) to show the probabilistic nature of the safety performance would play an essential role of the safety evaluation. The reasons to perform PSA for a developing reactor are (Yang, 2006):

- to show an outline of overall risk profile and its aspects (such as a vulnerability),
- to prepare the regulation and licensing requirements and
- to provide the risk information to improve the safety design.

For VHTR's PSA, technical issues will be identified and resolved. This paper introduced the current state of the development of VHTR's PSA approach and research activities in Korea.

2. Safety characteristics of VHTR

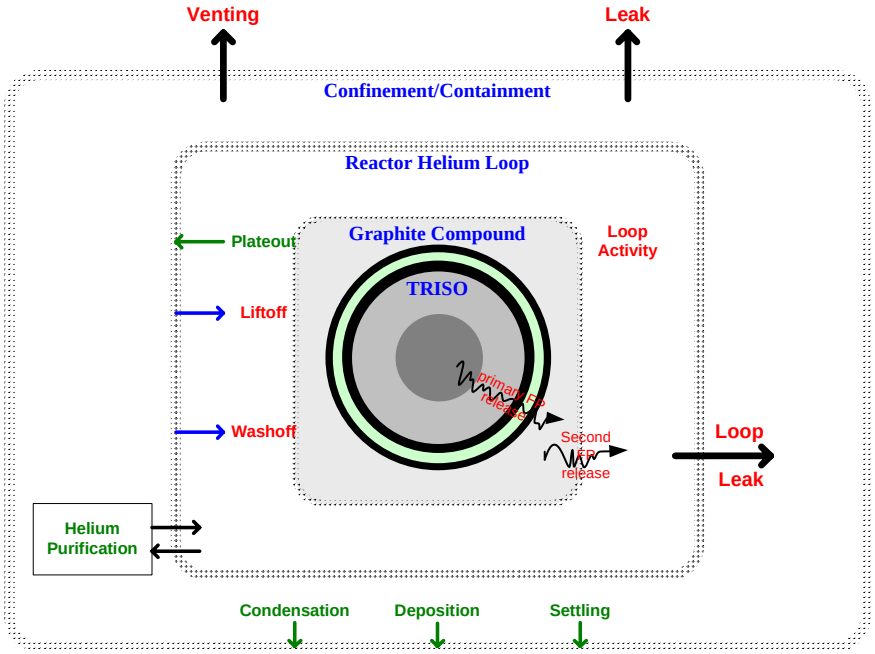
In order to understand VHTR's PSA approach, the safety characteristics and overall behavior under accident conditions of VHTR should be recognized. The safety characteristics of VHTR are large different to those of light water reactors (LWR) (Table 1). These are basically due to the fuel performance of VHTR known as tri-isotropic-coated fuel particles (TRISO) that are made in three layers of ceramic coated fuel particles and thermo-fluid behavior of gas type coolant.

1. Table 1. Safety features of the VHTR

1.	2. Safety function	3. VHTR	4. Remarks
5. Prevention	6. Inherent safety features	7. - Low power density 8. - Strong negative feedback 9. - Strong fuel configuration (TRISO) 10. - Large heat capacity (of graphite core)	11. ATWS / Return to Power
	12. Reactivity control	13. Reactor control & protection system	14. ATWS
	15. Coolant makeup	16. Helium supply system	17. Leak & pressure conserve function (no need inventory makeup when coolant loss)
	18. Auxiliary cooling	19. Direct vessel cooling system	20. Heat bypass to ground (optional)
	21. (Individual) long term cooling	22. N/A	23. Indirect cooling & no steam generator
24. Mitigation	25. 10CFR50.46 ECCS Rule	26. N/A	27. Gas-cooled vs. liquid-cooled
	28. Containment 29. (10CFR50 App. A)	30. Confinement (competitive option) 31. Emergency air purification system	32. Small radiation releases in any accident conditions

The types of reactor core design of VHTR are divided by the types of fuel assembles: block and pebble. Basically, fuel assembles form a compound of graphite with TRISO fuel elements. It is noted that the performance of TRISO makes the essential safety features of VHTR. TRISO has a good performance under hypothetical accident conditions (IAEA, 1997 and USNRC, 2004). In these reports, the mechanical failure of TRISO during accident conditions was very lower than the current reactors. They reported that the release rate of radioactive materials was increased according to the increase of the TRISO temperature, but the release rate was restricted. According to these characteristics, it is expected that the large release of fission products and related severe accident phenomena such as a core melt in LWR could not happen in VHTR.

The behaviors of radioactive materials under accident conditions would be affected by the four types of safety barriers and related physical phenomena as shown in Fig. 1 (McEachern et al., 2003). For these reasons, it is expected that the release rates in any accidents conditions be so small comparing with LWR.



2. **Fig. 1. A basic diagram of radioactive source terms behavior in VHTR (McEachern et al., 2003)**

The two essential features to be considered in PSA are as follows:

- No severe core damage.
- Small radiation release characteristics in any hypothetical accident conditions.

These features make it difficult to apply the typical PSA approach to VHTR, so a specific PSA approach are required.

3. Basic features of VHTR's PSA

As aforementioned, the typical PSA approach is hard to be applied in VHTR's PSA because of the inherent safety features of VHTR (Framing, 2005). The essential features to be considered in VHTR's PSA comparing with LWR's can be summarized as Table 2.

Table 2. Comparison of risk characteristics between VHTR and LWR

Features		VHTR	LWR
Physical	Barriers	TRISO → Fuel compounds → Helium gas → Containment	Fuel pallet → Cladding → Coolant → Containment
	Release amount	Small	Large
	Duration	Slow & long term release	Immediate & early release
Assessment	Critical end state	Release categories of radioactive materials (a few of release states)	Severe core damage
	Criteria	Release rate of radioactive materials	Success/fail

Because the plant states of VHTR cannot be simplified as failure or success, the essential terminologies, i.e., the definition of the end states of accident sequences (core damage state), are inapplicable to VHTR's PSA. As a result, the typical PSA frame (the classification of level 1, level 2 and level 3 PSA) should be replaced into an adequate frame for VHTR's PSA.

In VHTR's PSA, the end states of accident sequences should be rearranged by the consequential risk, because the final goal of PSA is to reveal consequential risk profile according to the environmental

release of radioactive materials. In other words, the end states of accident sequences should be defined as a few of release categories of radioactive materials (Fleming, 2005). For this reason, a tentative PSA approach for VHTR would replace three levels of the implementation procedure of the typical PSA as two levels of procedure as shown in Fig.2. This approach consists of the sequence level PSA and the consequence level PSA. The sequence level PSA combines the level 1 and level 2 PSA in the typical PSA approach, in which the end states of accidents are defined by the release categories of radioactive materials called a radiation (source term) release categories.

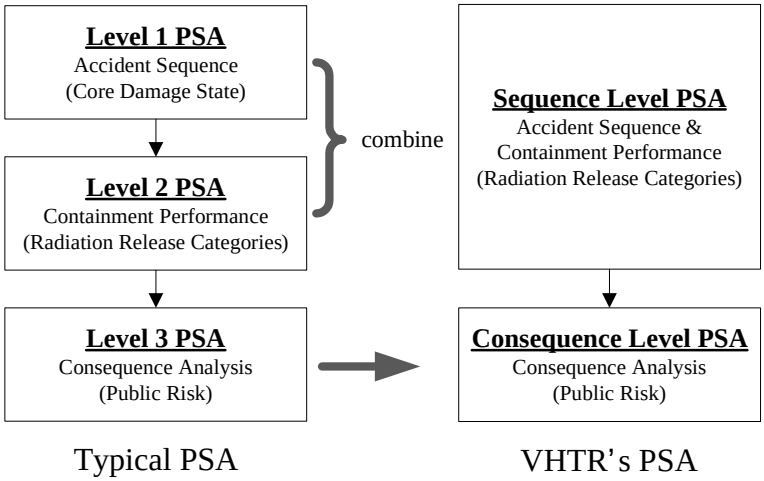


Fig. 2. Basic features of VHTR's PSA approach comparing with LWR's approach

Even though the approach follows the aforementioned basic features, it requires detail methods to perform an assessment. For this purpose, this paper introduced major considerations:

- Definition of the end sates of accident sequences (construction of risk metrics),
- Identification of initiating events
- Modeling of accident progression
- Estimation of (passive) safety functions related with accident sequences model
- Remaining works

4. PSA approach

4.1 Definition of End States of Accident Sequence (Risk Metrics)

The essential issue to evaluate PSA approach is to define the end states of accident sequences, because plant states of VHTR during accident conditions are ambiguous to be defined as success or fail (Flaming, 2005). A simple method is to directly apply the radiation release categories to indicate the end states of accident sequences. In this approach, the sequence states are too large to effectively show the risk profile. It makes an obstacle to understand the risk-information to imagine the probabilistic nature of safety aspects. This is an ineffective way to describe the risk profile according to the plant states as that in the typical PSA.

An effective way to resolve this is to adopt the binning technique that the radiation release categories are combined as a reasonable small size of plant states. Table 3 shows the two step combined methods. The derived radiation release categories (16 categories in the example case) are combined as less small number of plant damage states (5 states). Plant damage states are also combined as the core heatup states which are determined by the violation of the core safety design criterion (fuel design temperature criterion T_{max} = 1,600°C). Because of VHTR safety characteristics, the core heatup states does not have a robust meaning to indicate the plant states, but it could be helpful to understanding of the risk profile of VHTR.

Table 3. Proposed risk measures for VHTR's PSA

Radiation release category	Plant damage state	Core heatup state
IC, IP	Normal (E)	Normal
IT, IF, SPNR	Subtle Release (D)	
SPNB, SFNR, LPNB	Noticeable Release (C)	
SFNB, SFAR, SFAB, LPAB, LFNB, LFAB	Considerable Release (B)	Unfavorable core heatup
DX, DU	Significant Release (A)	

It is noted that detailed information of radiation release characteristics in order to evaluate specific criteria of radiation release categories and plant damage states are required. However, the current state of art of this information is scarcely known to us. Researches and developments of physical phenomena and models for the radiation release are restrictedly available now. The quantitative development of radiation release categories is a future work to obtain the details of this information. This paper showed a qualitative classification of risk metrics as a preliminary study to be applied in VHTR's PSA (Table 3).

4.2 Identification of Initiating Events

Initiating events analysis is a major part of PSA. Especially, the identification of initiating event of new design reactors plays an essential role in the evaluation of risk profile. However, it is difficult to identify initiating events according to the realistic nature of new reactors because of the lack of the operation experience and the incompleteness of the design details.

A master logic diagram (MLD) method as a logical approach is adopted as the primary method. The logic diagram approach uses a logical decomposition technique, which is a means to decompose a major factor (i.e., a risk impact) to subsidiary details by a deductive inference until the initiators can be found step by step.

A difficulty of this method is to decide on the last decomposition stages to find concrete forms of initiating events. These depend on the required decomposition stages. In the design stage, because of the incompleteness of the design details, there is a limitation to apply this method. However, because this method takes a logical deductive approach, it can freely use under the lack information of design details.

The present study adopted a logic diagram that can describe the accident initiators having a radiological potentiality according to the conceptual design of a VHTR. The major factors associated with the radiological potential consist of as follows:

- a failure of the reactivity control,
- a failure of the heat removal,
- a failure of the coolant boundary,
- an unfavorable chemical reaction in the reactor core due to the ingression of water or air,
- a mechanical impact from the periphery like a turbine blade breakdown, and
- an environmental impact to reactor core like a seismic event.

Each factor can be classified as subsidiary items that can describe detailed factors. This logic diagram can be used in the definition of the initiating events. The logic diagram in the current state only has a crude frame but interactive activities with the concept designer and safety analyzer should create a precise definition of initiating events. Primarily, a basic frame of five levels was constructed as follows:

- Level 1 (risk impacts): Radiation material release from the system
- Level 2 (radiation sources): ex-core material, core material
- Level 3 (threaten factors-potentiality-energy): power, heat balance, mechanical failure, chemical reaction

- Level 4 (disturbance elements): boundary failure
- Level 5 (initiators): preliminary form of initiators

Currently, the design details of VHTR were not provided, so the detailed aspect of the logic diagram is incomplete. The final logic diagram will be constructed when the design details would be finalized. The present diagram showed the crude and overall aspects for the process of the identification of initiating events (Fig.3 and Table 4).

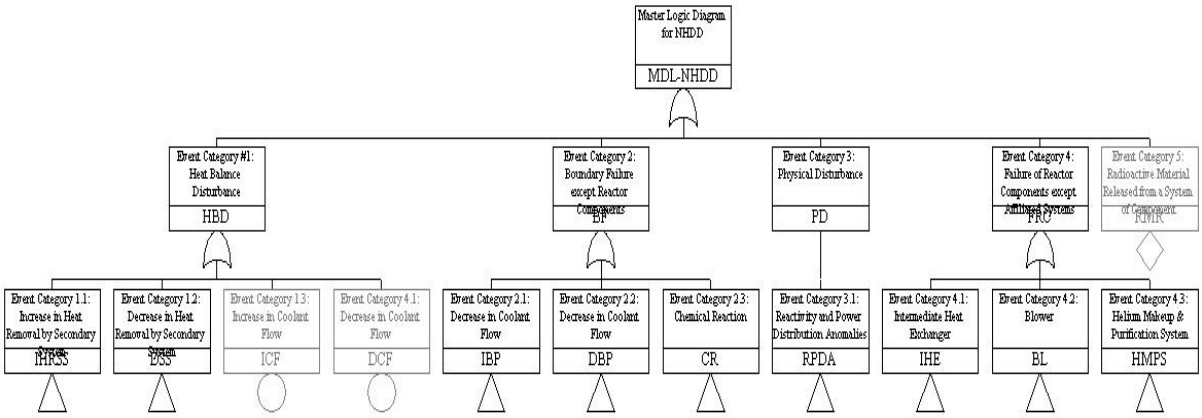


Fig. 3. A logical diagram for identifying initiating events (level 3)

Table 4. Identified initiating events by the logic diagram approach for VHTR

No.	Index	Initiator	Type
1	PBMA	Primary Blower Miss-Acceleration	Transient
2	PBL	Primary Blower Locked	Transient
3	PIHB	Primary IHX Blocking	Transient
4	SBMA	Secondary Blower Miss-Acceleration	Transient
5	SSVAO	Secondary Safety/Relief Valve Accidental Open	Transient
6	SBF	Secondary-side Boundary Failure	Transient
7	SIHB	Secondary IHX Blocking	Transient
8	SBB	Secondary Blower Blocking	Transient
9	ITC	Increase Third-side Cooling	Transient
10	DTC	Decrease Third-side Cooling	Transient
11	HMSOC	Helium Makeup System Over Charging	Transient
12	PIHIF	Primary IHX Interface Failure	LOCA
13	PLB	Primary Leak in Boundary	LOCA
14	PISB	Primary Interface System Break	LOCA
15	PSVAO	Primary Safety/Relief Valve Accidental Open	LOCA
16	CFCP	Catastrophic Failure of Coolant Piping	LOCA
17	CFRS	Catastrophic Failure of Reactor Structure	LOCA
18	TM	Turbine Missile	LOCA
19	ATWS_C	Control Rods Withdraw with/without Power Operation	ATWS
20	ATWS_S	Shutdown Rods Withdraw with/without Power Operation	ATWS
21	LOOP	Loss of Off-site Power	Transient
22	GTRN	General Transient	Transient

It is noted that initiating events frequencies should be estimated to quantify accident sequences. There is no effective method to estimated events frequencies because of the lack of information. In the preliminary study, the initiators frequencies were assigned by subjective manner. It is necessary that it will be refined continually for the initiating events analysis by using update information of the progress of the system's design.

4.3 Modeling of Accident Sequences

To successfully obtain the risk aspects under the incomplete design configuration, plant behaviors to describe the accident sequences should be modeled with an adequate level of depth. An effective way to achieve this is to model system behaviors by using event tree approach by using functional description. The proposed functional description approach to model accident sequences consists of two stages:

(1) main logic (event tree) models for accident sequences by functional description and
(2) supporting logic models to estimate functional heading events in the main logic models (to replace fault tree models).

The major advantage of the functional description is to minimize an effort to model the system performance by using fault trees to describe heading events in the main logic model. Fault tree models require a sufficient level of depth of system details to describe the system performance, but supporting logic models as an alternative instead of fault tree model could simplify the modeling of system performance under incomplete information. The supporting logic models by functional description are useful tools until system designs are completed.

To assess the feasibility of the proposed approach, an example application for the event tree modeling has been performed as following section. The event tree as an essential part of accident sequence analysis has been modeled using a function form.

An example model of accident sequences is shown in Table 5. Essential safety functions of VHTR consist of three functions:

1. reactor trip
2. residual heat removal
3. containment

3. Table 5. Main logic models with heading description for VHTR

Accident progression					
Initial state			Safety functions		Radiation release
Initiating event	RCS boundary	Chemical reaction	Reactor trip	Residual heat removal	Containment status

It consists of (1) initial status, (2) safety functions, and (3) radiation release. Initial status includes a three heading, safety function includes reactor trip failure and residual heat removal failure, and radiation release has a confinement status. These headings are modeled by functional description, so each design features was indirectly incorporated into these headings, which are described by a supporting logic tree.

It is noted that the branches of heading cannot simply assign success or failure of safety functions because of VHTR safety characteristics. The branches of a heading should be divided by plant states. The purpose of accident sequence analysis is to identify the integrated behavior of a nuclear system and to assign its integrated plant states, i.e., the end states of accident sequences. To consider these unfavorable features, it is necessary that multiple branches of the heading for safety functions should be considered. This means that the states of a safety function are divided into several states. The application of multiple states approach to this logic tree was described in next section the estimation of passive safety system.

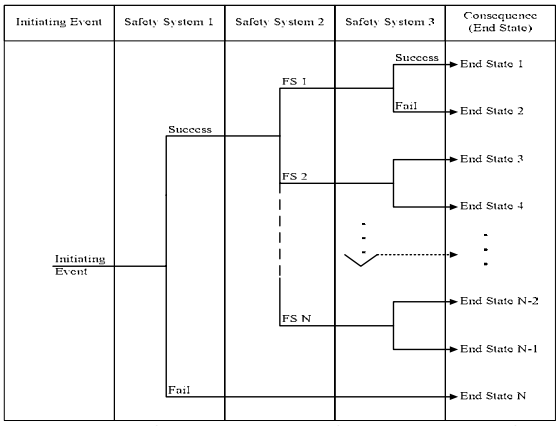
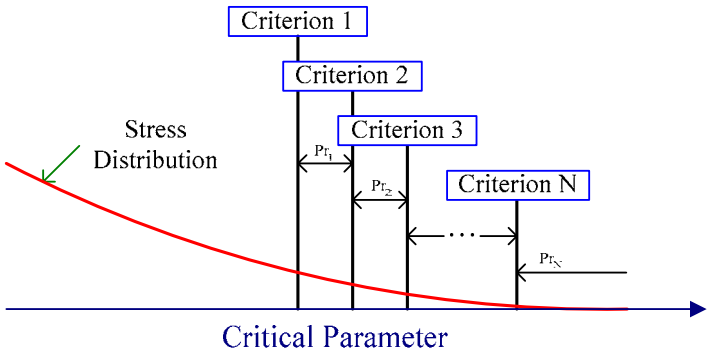


Fig. 3. A conceptual diagrams of multiple branches for the evaluation of accident sequences

4.4 Estimation of Residual Heat Removal Systems

In VHTR's PSA, the plant states are determined by the radiation release characteristics. The behavior of safety functions, residual heat removal system that major candidate in VHTR is a passive safety cooling system such as a reactor cavity cooling system (RCCS), should be estimated by multiple states. For this purpose, multiple failure states model for a passive safety system was proposed (Han, 2010).

The conceptual diagram of multiple states to apply the system states is shown in Fig. 4. In VHTR, the basic mechanism of radiation release from fuel elements depends on the fuel temperature behavior. To estimate environmental radiation release, it is necessary to evaluate plant transport phenomena based on their feature as shown Fig. 4.



4. **Fig. 4. A conceptual diagram to show multiple failure criteria**

Although these factors are required in the estimation of radiation release, major characteristics can be expressed by the fuel performance. The detailed information for this topic is described in our other research papers(Han, 2010a, b). By using this approach, the essential safety function such as a passive heat removal system could be modeled for the estimation of multiple states.

5. Further Works

Aforementioned basic approaches by using a multiple states concept will be adopted to evaluate VHTR's PSA, but additional technical issues are required to apply the proposed PSA approach. Most of all, the information of the radiation release characteristics with physical phenomena to divide the plants states as shown in section 4.1 is required. However, this information is still unavailable. The complete form of the proposed approach will be finalized when the available information to determine the plant states with an adequate level of depth can be obtained.

As a example, preliminary results of the accident sequences for the unfavorable core heatup are shown

in Fig.4, which were modeled by the two states of accident sequences, i.e., the violation of the fuel temperature design criterion, T_{max} > 1,600℃ as the VHTR's safety design criteria. It is noted that these probabilistic aspects were not show the complete risk profile because the quantification criteria does not meaningful information on the radiation risk of VHTR as noted in Introduction and Section 2. To provide meaningful risk information, the plant states should be carefully determined by the radiation release characteristics.

5. Table 6. An example results of the unfavorable core heatup criterion for a VHTR

No.	Index	Initiating event	Type	Initiating event frequency (/yr)	Unfavorable core heatup (> 1,600℃)
1	GTRN	General Transient	Transient	1.41E+00	4.20E-05
2	LOOP	Loss of off-site power	Transient	1.00E-02	1.30E-06
3	PBMA	Primary blower miss-acceleration	Transient	1.00E-04	1.30E-08
4	LOF	Loss of coolant flow	Transient	1.10E-04	1.45E-08
5	SBMA	Secondary blower miss-acceleration	Transient	1.00E-04	3.01E-09
6	LOSC	Loss of secondary cooling	Transient	1.30E-04	3.91E-06
7	HMSOC	Helium makeup system over charging	Transient	1.00E-04	3.16E-09
8	PBFOCR	Primary boundary failure without chemical reaction	LOCA	3.10E-04	9.33E-09
9	PBFWCR	Primary boundary failure with chemical reaction	LOCA	2.00E-05	2.60E-09
10	CBF	Catastrophic blower failure	LOCA	1.00E-05	1.30E-09
11	CRWD	Control rods withdraw with/without power operation	ATWS	2.00E-07	6.02E-12
			Sum		4.72E-05

Finally, it is denoted that remaining technical issues for VHTR's PSA as follows will be studied concurrently to the development of VHTR's PSA approach:

- Reliability database (including Initiating Events DB) for VHTR
  - Specific DB
  - Expert Opinions
- Evaluation of source terms
  - Establishment of PSA Methodology
  - Design of Containment/Compartment
- Reliability of passive (safety) systems
  - Definition of passive system reliability
  - Quantification
- Human reliability
- Reliability of digital I&C system, etc

However, the studies of these issues with a sufficient level of depth depend on the development of VHTR. In the current development stage, it is expected that a continuous research is necessary to achieve a VHTR's PSA.

References

CHANG, J. et al, (2007). A study of a nuclear hydrogen production demonstration plant, Nuclear Engineering and Technology, Vol. 39, No. 2, pp.111-122.
FLEMING, K. N., (2005). Challenges and opportunities in the performance of PRAs on new reactors, Proceedings of PSA ’05, San Francisco CA.
HAN, S. and Yang, J., (2010a). A quantitative evaluation of reliability of passive systems within probabilistic safety assessment framework for VHTR, Annals of Nuclear Energy, Vol. 37 (3), pp. 345-358.
HAN, S. and Yang, J., (2010b), A study on multiple failure states criteria for assessing reliability of passive systems for innovative reactor, PSAM10, Seattle, Washington, USA, 7-11 June.
IAEA, (1997). Fuel performance and fission product behaviour in gas cooled reactors, International Atomic Energy Agency, TECDOC-978, Vienna.
McEachern, D. et al, (2003). GT-MHR: fuel design, manufacturing, performance, presented at ANS Gas Reactor Technology Course, General Atomic, June 5-6.
OH, K.M. et al, (2008). The approaches on the determination of F-C criteria in risk assessment of new reactors, Transactions of the Korean Nuclear Society Autumn Meeting.
USNRC, (2004). TRISO-coated particle fuel phenomenon identification and ranking tables (PIRTs) for fission product transport due to manufacturing, operations, and accidents. U.S. Nuclear Regulatory Commission, NUREG/CR-6844.
YANG, J. & LEE, W., (2006). Development of risk-informed design framework of VHTR in Korea, Trans. of the KPVP, Vol. 2. No. 2, pp. 9-16.

OECD/NEA Workshop on PSA for New and Advanced Reactors
June 20-24, 2011
OECD Conference Centre, Paris, France

Overview of VHTR's PSA Approach in Korea

June 20, 2011

Seok-Jung HAN

KAERI Korea Atomic Energy Research Institute

Contents

1. Introduction

- Very High Temperature Reactor (VHTR)
  - A Generation IV's reactor for providing a high temperature (900 °C ~ 1,000°C) heat source (process heat; electric generation)
  - Gas-cooled graphite reactor with ceramic coating fuel element (TRISO)
  - Good characteristics of fuel (TRISO) and inherent safety

- PSA for Developing Reactor
  - Outline of risk profile and aspects
  - Preparation of regulation and licensing requirement
  - Design improvement by risk-information for safety enhancement

- Objectives
  - Current state of VHTR's PSA approaches
  - Research activities in Korea

2

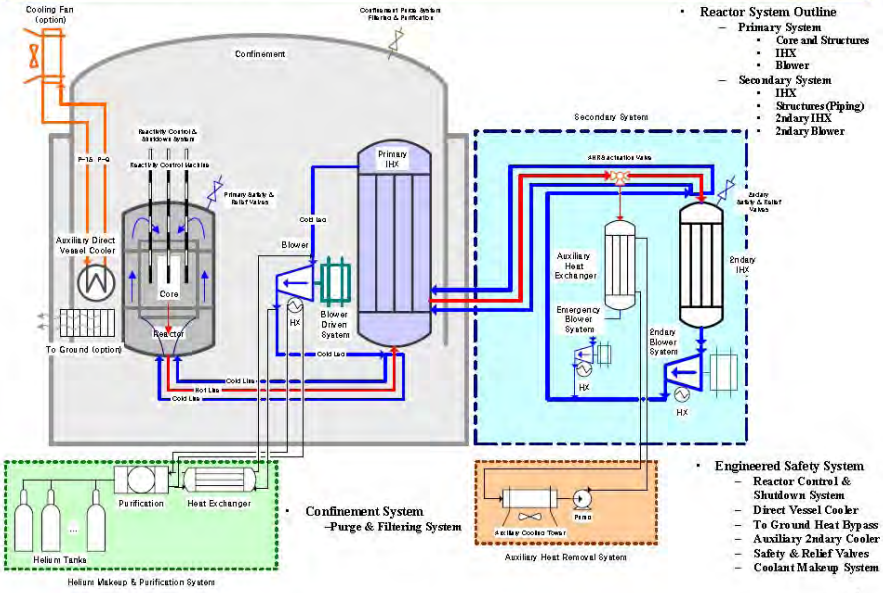
2. Safety Characteristics of VHTR (1/2)

- **Enhanced fuel performance: No melt of fuel elements (TRISO)**
- **Gas Coolant (→ Liquid)**
  - No coolant makeup function (10CFR50.46 ECCS Rule (DBA) is not applicable to VHTR)
- **Simplified Safety Functions**
  - Reactivity Control
  - Residual Heat Removal
  - Protection of Radiation Release
- **Simplified Residual Heat Removal**
  - Indirect Cycle (Intermediate Loop): No loss of secondary-side function

	Basic Safety Functions	Features	Remarks
Protection	Inherent Safety Features	Low Power Density Strong Negative Feedback Strong Fuel Configuration (Coated Particle) Large Heat Capacity of Graphite Core	
	Reactivity Control	Reactor Control & Protection System	ATWS / Return to Power
	Coolant Makeup	Helium Supply System	Leak & Pressure Conserve Function
	Auxiliary Cooling System	Auxiliary Cooling System Direct Vessel Cooling System Heat Bypass to Ground	
	Long Term Cooling	N/A	Possible Indirect Cooling
Mitigation	10CFR50.46 ECCS Rule*	N/A	Not Applicable
	General Design Criteria (10CFR50 App. A)	Single Failure Criteria	Not Applicable to Passive System (with loss of off-site power)
	Containment (10CFR50 App. A)	Confinement Purge System Emergency Air Purification System	LWR ← → GCR Not Applicable

3

Note: A Conceptual Diagram of VHTR



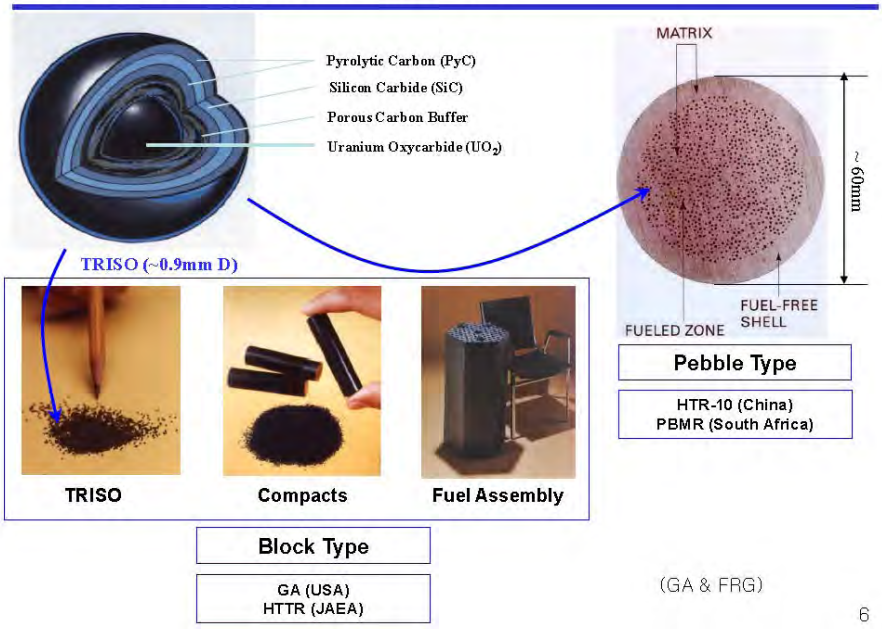
4

Note: Design Outlines

- Reactor System Outlines (Configuration)
  - Reactor Types (Helium Coolant & Graphite Reactor)
    - Pebble Bed
    - Block (Prismatic)
  - Primary Component Configuration
    - Primary Intermediate Heat Exchanger
    - Primary Blower
      - Compressor & Electric Motor Power
      - Compressor & Turbine Power
    - Primary Coolant Makeup & Supply System
    - Primary Pressure Control System
      - Safety & Relief Valve
  - Secondary Component Configuration
    - Secondary Intermediate Heat Exchanger
    - Secondary Blower
      - Compressor & Electric Motor Power
      - Compressor & Turbine Power
    - Secondary Coolant Makeup & Supply System
    - Secondary Pressure Control System
      - Safety & Relief Valve
- Engineered Safety System Outline
  - Reactor Control & Shutdown System
  - Emergency Core Cooling System
    - Direct Vessel Cooler
    - Heat Bypass to Ground
    - Auxiliary 2ndary Cooler
  - Safety & Relief Valves
  - Coolant Makeup System
- Confinement System Outline
  - Purge & Filtering System
- Note: Structure is assumed well-worked. I&C, Supply Systems, Balance of Plan (BOP), & Electric Power System do not considered.
  Other options are not considered.

5

Note: Basic Features of VHTR TRISO



(GA & FRG)

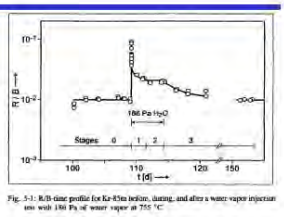
6

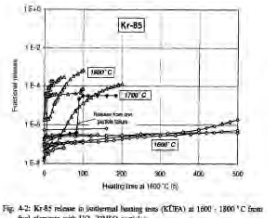
Note: Performance of TRISO Fuel Element

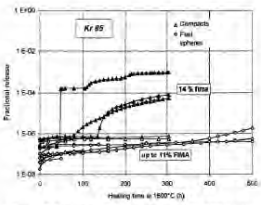
- Fuel Performance (Source Term)
  - Major mechanism of source term release is a diffusion (not a defection or melting).
  - Major Parameters: Temp., Duration, Burnup

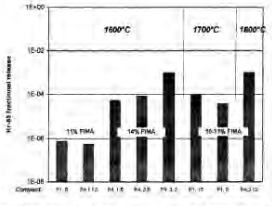
$$Fr_R = f(Temp., Duration, Burnup, etc)$$

  - hard to define criteria of core damage for design or assessment
- References
  - Fuel performance and fission product behaviour in gas cooled reactors, IAEA, TECDOC-978, November 1997
  - TRISO-Coated Particle Fuel Phenomenon Identification and Ranking Tables (PIRTs) for Fission Product Transport Due to Manufacturing, Operations, and Accidents, U.S. NRC, NUREG/CR-6844, July 2004

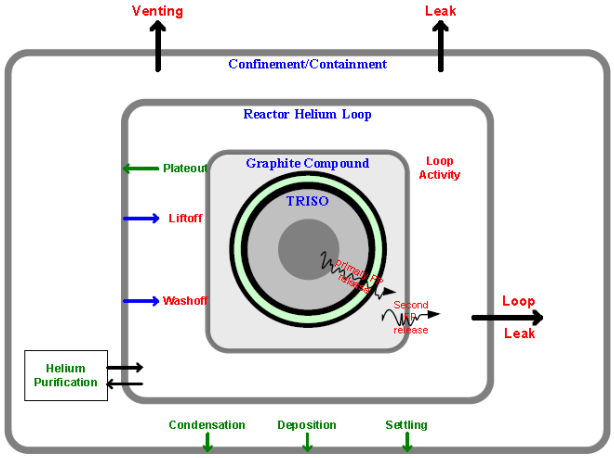








Note: A basic diagram of source terms behaviors in VHTR (McEachern et al., 2003)



8

Safety Characteristics of VHTR (2/2)

- The two essential features to be considered in PSA are:
  - No severe core damage
  - Small radiation release characteristics in any hypothetical accident conditions

- **A specific approach are required for VHTR's PSA**.
  - Safety features make it difficult to apply the typical PSA approach to VHTR.

9

3. Basic Features of VHTR's PSA

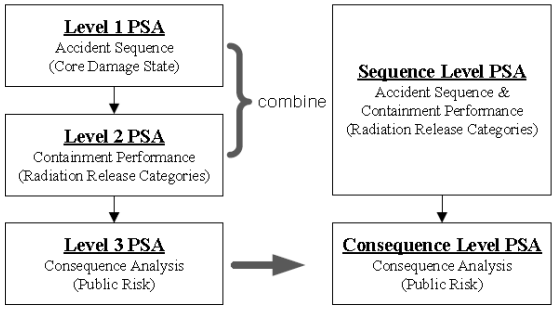
- Basic approach to quantify the risk
  - ET/FT methods
  - Consequence analysis methods
- Not applicable to terminology of the typical PSA
  - End states of accident sequences
    - Core damage state (CDF) for level 1 PSA → X
    - Containment state (LERF, LLRF) for level 2 PSA → X
  - Typical PSA framework is not applicable to VHTR's PSA

Table 2. Comparison of risk characteristics between VHTR and LWR

Features		VHTR	LWR
Physical	Barriers	TRISO → Fuel compounds → Helium gas → Containment	Fuel pallet → Cladding → Coolant → Containment
	Release amount	Small	Large
	Duration	Slow & long term release	Immediate & early release
Assessment	Critical end state	Release categories of radioactive materials	Severe core damage
	Criteria	Release rate of radioactive materials	Success/fail

10

Basic Approach to VHTR's PSA



Major Consideration of Approach Development

- Definition of end states of accident sequences (risk metrics)
- Identification of initiating events
- Modeling of accident progression
- Estimation of safety functions
- Remaining works

- K.N. Fleming proposed two-step approach (PSA`05) :

	LWR	GCR & VHTR
Accident sequence evaluation structure	• Level 1/Level 2/Level 3	• Integrated event trees span from initiating event to release categories with no staging
End states definition	• Core damage state: a considerable fuel elements in core is damaged. • Radiation release categories: LERF & LLRF	• Core damage state (not applicable) • Radiation release categories

11

4.1 Definition of End Stats of Accident Sequence (Risk Metrics)

PSA	Mode & Interface	Factor or State	Measure (Indicator)		Remark
Consequence Level PSA	Health Effect	Early Fatality	Exposure Dose		Direct Measure/Indicator
		Late Fatality	Exposure Dose		Direct Measure/Indicator
	Source Term	Source Term Release Category	Release Amount		Nuclide Release Faction
Sequence Level PSA			Source Term Release Category		Interface Measure
	Plant Damage	Plant Damage State	PDS Frequency	Significant Release	Proposed Measure
				Considerable Release	
				Noticeable Release	
				Subtle Release	
				Normal	
		Core Heatup State	Unfavorable Core Heatup Frequency		(Proposed) Supporting Measure

Proposed Approach for VHTR PSA

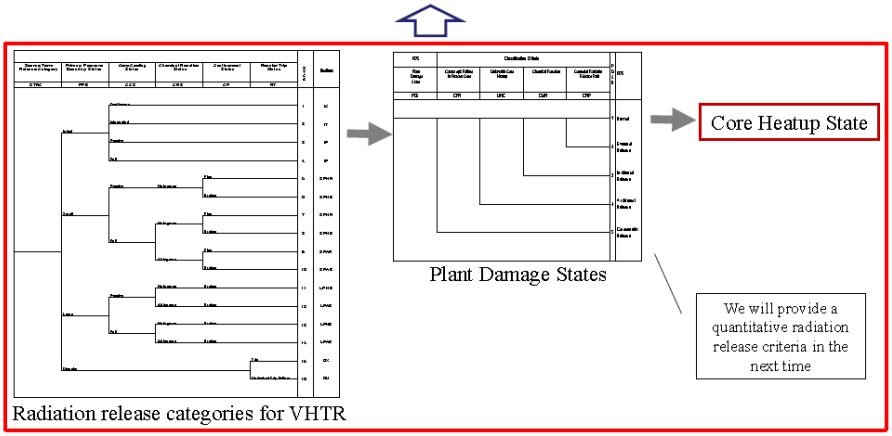
LWR Risk Metrics

PSA	Mode & Interface	Factor or State	Measure	Remark
Level 3	Health Effect	Early Fatality	Exposure Dose	Direct Measure/Indicator
		Late Fatality (Cancer Fatality)	Exposure Dose	Direct Measure/Indicator
	Source Term	Source Term Release Category	Release Amount (Bq, Ci, ...) Source Term Release Category	Nuclides Release Fraction Interfacial Measure
Level 2	Containment Damage	Containment Damage State	(Large) Early Release Frequency (Large) Late Release Frequency Small Release Frequency, etc	Basic Measure/Indicator
Level 1	Plant Damage	Plant Damage State	PDS Frequency	Interfacial Measure
	Core Damage	Core Damage State	Core Damage Frequency	Basic Measure/Indicator

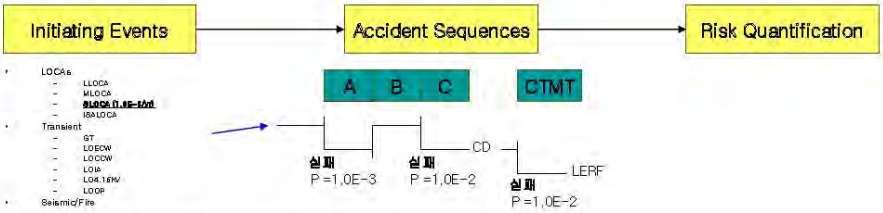
Proposed Risk Measures for VHTR's PSA

Relationship between end state definitions

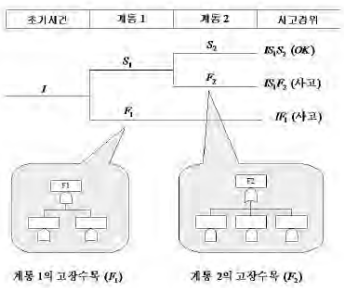
Radiation Release Categories	Plant Damage States	Core Heatup States
IC, IP	Normal (E)	Normal
IT, IF, SPNR	Subtle Release (D)	
SPNB, SFNR, LPNB	Noticeable Release (C)	
SFNB, SFAR, SFAB, LPAB, LFNB, LFAB	Considerable Release (B)	Unfavorable core heatup
DX, DU	Significant Release (A)	



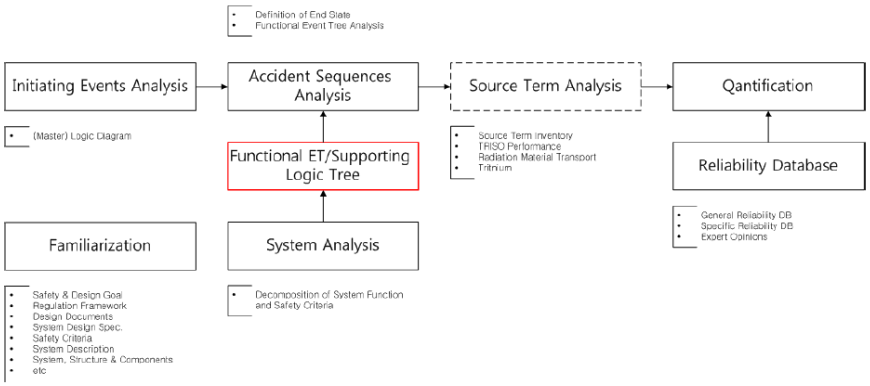
Note: Event Tree/Fault Tree Approach



- Event Tree (ET) Analysis:
  - Accident Progression by System Behavior (System Characteristics) from an Initiator
    - System Functions
      - Safety Functions
      - Mitigation Functions
    - System, Structure and Component
    - Operator Actions
    - Maintenance
- Fault Tree (FT) Analysis:
  - Estimation of system performance on demand by Fault Logic



Note: PSA Procedure based on Proposed Risk Metrics

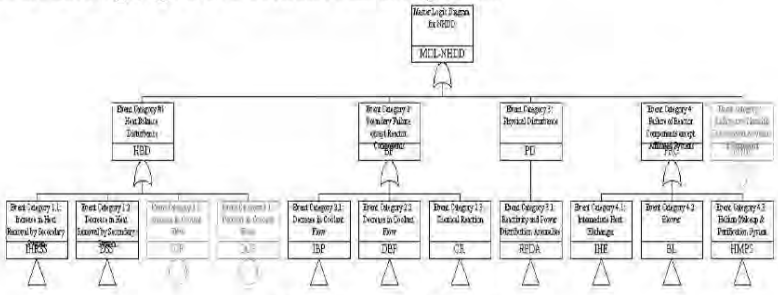


- System Analysis
  - Fault Tree Technique (not applicable to conceptual design stage)
  - → Function-based decomposition logic tree technique
  - → Supporting Logic Tree

15

4.2 Identification of Initiating Events

- Objective:
  - To identify the complete set of initiating events to obtain the overall aspect of risk profiles.
- Approaches:
  - Logical method (Master Logic Diagram) : Logical decomposition technique from top requirement.
  - Physical or technical disturbance of heat or reactivity balance (reactor trip induced events).
- 11 initiators groups for 22 identified initiating events



Master Logic Diagram

16

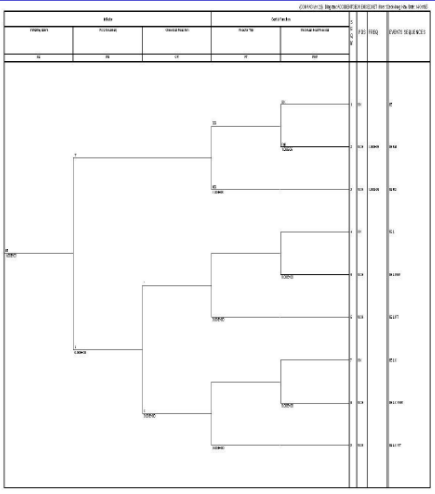
Note: Identified Initiating Events

No.	Index	Initiator	Type
1	PBMA	Primary Blower Miss-Acceleration	Transient
2	PBL	Primary Blower Locked	Transient
3	PIHB	Primary IHX Blocking	Transient
4	SBMA	Secondary Blower Miss-Acceleration	Transient
5	SSVAO	Secondary Safety/Relief Valve Accidental Open	Transient
6	SBF	Secondary-side Boundary Failure	Transient
7	SIHB	Secondary IHX Blocking	Transient
8	SBB	Secondary Blower Blocking	Transient
9	ITC	Increase Third-side Cooling	Transient
10	DTC	Decrease Third-side Cooling	Transient
11	HMSOC	Helium Makeup System Over Charging	Transient
12	PIHIF	Primary IHX Interface Failure	LOCA
13	PLB	Primary Leak in Boundary	LOCA
14	PISB	Primary Interface System Break	LOCA
15	PSVAO	Primary Safety/Relief Valve Accidental Open	LOCA
16	CFCP	Catastrophic Failure of Coolant Piping	LOCA
17	CFRS	Catastrophic Failure of Reactor Structure	LOCA
18	TM	Turbine Missile	LOCA
19	ATWS_C	Control Rods Withdraw with/without Power Operation	ATWS
20	ATWS_S	Shutdown Rods Withdraw with/without Power Operation	ATWS
21	LOOP	Loss of Off-site Power	Transient
22	GTRN	General Transient	Transient

17

4.3 Modeling of Accident Sequences

- Basic Assumptions
  - No treat multiple initiators
  - Core damage → Unfavorable Core Heatup (UCH) (> 1600°C)
- Description
  - Transient behavior
  - Required safety functions
- Heading Events
  - Initial States
  - Safety Functions
  - Radiation Protection



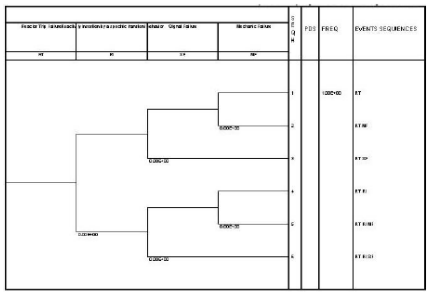
Accident Progression					
Initial Status			Safety Function		Radiation Release
Initiator	Rx Boundary	Chemical Reaction	Rx Trip	Residual Heat Removal	Confinement Status

18

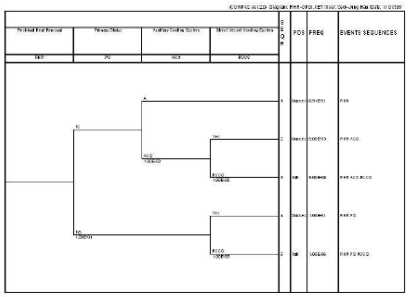
Note: Supporting Logic Tree (SLT)

- **SLT for Reactor Trip**
  - Reactivity related transient by specific Event
  - Mechanical failure
  - Electrical failure
- **In LWR experience, reactor protection system reliability was estimated as 1.20E-4/d ~ 5.00E-7/d.**

	Electrical	Mechanical	Remark
Prime R1.0	5.38E-07	5.00E-06	Cutsets generation with no treat
KSNP	6.62E-06	5.00E-06	Referred from CE Report
SECY-83-293	2.00E-05	1.00E-05	
SECY-83-293*	8.70E-05	4.30E-05	LWR experience
NUREG/CR-5500	??	1.70E-05	



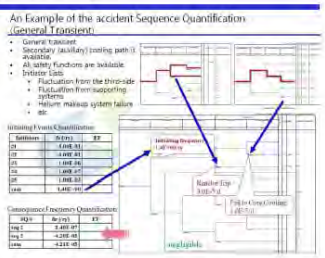
- **SLT for Residual Heat Removal**
  - Primary Status (Boundary Failure)
  - Auxiliary Cooling Path : ~1.00E-3/d (referred from RCCS estimation in PBMR PSA)
- **Reactor Cavity Cooling System : ~1.00E-4/d (referred from RCCS estimation)**
- **It does not consider the effect from other systems**
  - Electrical
  - Support system
  - Compartment cooling system



Supporting Logic Tree for Residual Heat Removal

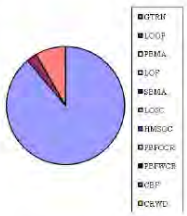
Note: Tentative Study for Unfavorable Core Heatup (UCH)

- A tentative study has been performed for the UCH (T_{peak} > 1,600°C) state.
  - UCH does not a representative measure of VHTR risk, but this provided useful insights for the improvement of PSA approach.
  - Key points of improvement:
    - UCH → Plant Damage State → STC
    - Estimation of Essential Safety features



Estimation of "Unfavorable Core Heatup" Sequences

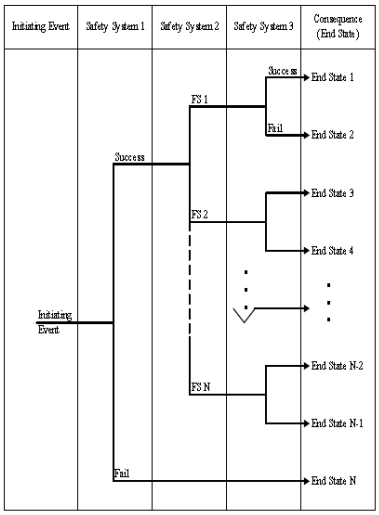
No.	Index	Accident Sequence	Type	Initiating Event Frequency (1/yr)	Unfavorable Core Heatup (> 1,600°C)
1	GTRN	General Transient	Transient	1.41E+00	4.20E-05
2	LOOP	Loss of Off-site Power	Transient	1.00E-02	1.30E-06
3	PBMA	Primary Blower Miss-Acceleration	Transient	1.00E-04	1.30E-08
4	LOF	Loss of coolant flow	Transient	1.10E-04	1.45E-08
5	SBMA	Secondary Blower Miss-Acceleration	Transient	1.00E-04	3.01E-09
6	LOSC	Loss of secondary cooling	Transient	1.30E-04	3.91E-06
7	HMSOC	Helium Makeup System Over Charging	Transient	1.00E-04	3.16E-09
8	PBFOCR	Primary Boundary Failure without chemical reaction	LOCA	3.10E-04	9.33E-09
9	PBFWCR	Primary Boundary Failure with chemical reaction	LOCA	2.00E-05	2.60E-09
10	CBF	Catastrophic Blower Failure	LOCA	1.00E-05	1.30E-09
11	CRWD	Control Rods Withdraw with/without Power Operation	ATWS	2.00E-07	6.02E-12
			Sum		**4.72E-5**



20

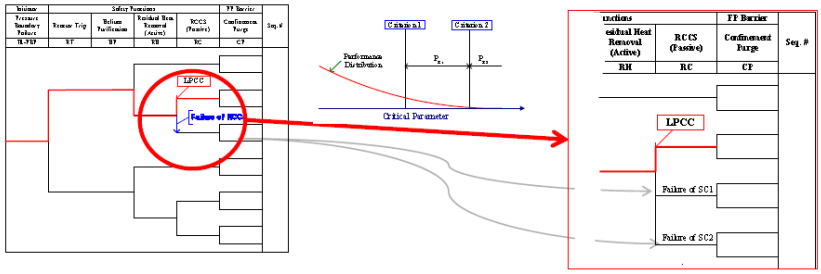
Application of Plant Damage States (Branches of Heading Events)

- Branches of heading events should be divided as multiple states to improve PSA approach.
  - The heading events cannot simply assign success or failure of safety functions (VHTR safety characteristics).
- Branches should be divided by plant states.
- The application of multiple states approach to this logic tree is related with the estimation method of passive safety systems.



21

4.4. Estimation of Passive Safety Systems



- Example of Two Failure States Criteria to Estimate RCCS
  - PSA for considering inherent safety features of VHTR

Criterion	EP Model	SSI Model*	Meaning of criteria	
			Single criterion approach	Multiple (double) criteria approach
1st	$T_S = T_{S_1}$ =1600 °C	A specific probability distribution	System failure	A small release of radioactive materials compared with the normal state
2nd	T_{S_2} =1700 °C	A specific probability distribution	Not applicable	A large release of radioactive materials compared with the normal state

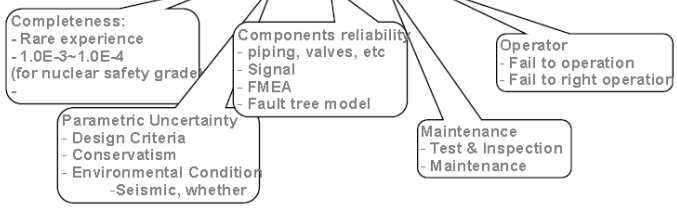
22

Note: Estimation of Passive Safety Systems (1/2)

- Extraction of Reliability Structure
  - Operational Demand
  - Failure Modes and Effect
- Basic Model
- Functional Failure

- Operational Demand
  - Start Time and Operation
  - Duration (Mission Time)
- Failure Modes and Effect
  - Hardware Failure
    - Component Reliability
  - Functional Failure
    - Criteria: Multiple Failure States
    - Uncertainty
  - Maintainability
  - Operator Action

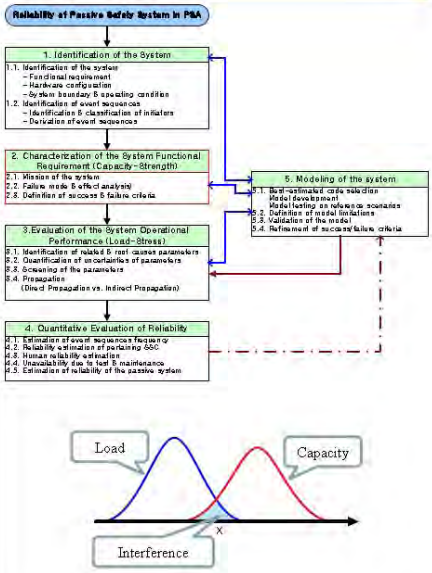
$$R_{PS} = \prod_i R_i = R_c \cdot R_p \cdot R_r \cdot R_m \cdot R_o$$

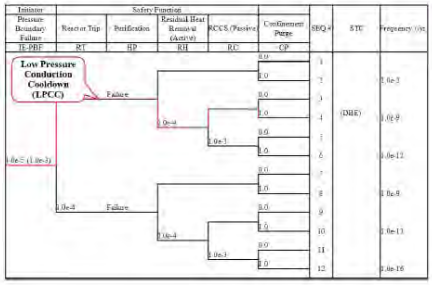


23

Note: Estimation of Passive Safety Systems (2/2)

- Estimation of Functional Failure
- Basic Approach: SSI method
  - Failure Criteria
    - Ambiguity of safety characteristics of VHTR
  - System Operational Performance
    - Uncertainty Propagation





24

5. Further Works

- Technical issues
  - Evaluation of source terms
  - Reliability database (including Initiating Events DB) for VHTR
  - Reliability of passive (safety) systems
  - Human reliability
  - Reliability of digital I&C system
- The studies of these issues with a sufficient level of depth depend on the development of VHTR.

25

Concluding Remarks

- Overall aspects on a development of VHTR's PSA were introduced.
  - Key issues to develop PSA approaches was identified and proposed the resolve methods.
    - PSA frame (Sequence Level PSA and Consequence Level PSA)
    - Required Risk Metrics
    - Identification of Initiating Events
    - Modeling of Accident Sequence with Tentative Fault Logic Tree
    - Estimation Approach to Passive Systems
  - Tentative study for UCH was presented to obtain useful insights for the improvement of PSA approach.
    - To extend the end state to more representative risk measures
- It is expected that further study is required to achieve a VHTR's PSA.
  - Resolution of Remained issues
  - Tentative Application of Proposed Approach

26

Thank you for your attention!

27

Safety Assessment for Generation IV Nuclear Systems

Timothy J. Leahy
Co-Chair, Generation IV International Forum Risk and Safety Working Group
Idaho National Laboratory, Idaho Falls, ID, USA

Abstract

The Generation IV International Forum (GIF) Risk and Safety Working Group (RSWG) was created to develop an effective approach for the safety of Generation IV advanced nuclear energy systems. Recent RSWG work has focused on the definition of an integrated safety assessment methodology for evaluating the safety of Generation IV systems. The methodology, called ISAM, is an integrated "toolkit" consisting of analytical techniques that are available and matched to appropriate stages of Generation IV system concept development. The integrated methodology is intended to yield safety-related insights that help actively drive the evolving design throughout the technology development cycle, potentially resulting in enhanced safety, reduced costs, and shortened development time.

1. Introduction

The Generation IV International Forum (GIF) Risk and Safety Working Group (RSWG) was created to promote a homogeneous and effective approach to assuring the safety of Generation IV nuclear energy systems. The six Generation IV reactor concepts that have been selected by the GIF members potentially present a diverse set of design and safety issues. A number of these issues differ significantly from those presented by the earlier generations of light water reactors. The overall success of the Generation IV program depends on developing, demonstrating, and deploying advanced system designs that exhibit excellent safety characteristics. While the RSWG recognizes the excellent safety record of nuclear power plants currently operating in GIF member countries, it believes that advanced technologies and a coherent safety approach in which safety is "built in, not added on" to the basic designs of nuclear systems hold the promise of making Generation IV energy systems even safer than the current generation of nuclear plants.

The Generation IV Technology Roadmap identifies three specific safety goals for Generation IV systems guides the Generation IV research and development program. The intent of the safety goals is to stimulate the development of innovative energy systems that will achieve enhanced safety compared to that of the current plants, and to motivate and guide the research and development necessary to achieve that enhanced level of safety. These safety goals are:

1. *Generation IV nuclear energy systems will excel in safety and reliability.*
2. *Generation IV nuclear energy systems will have a very low likelihood and degree of reactor core damage.*
3. *Generation IV nuclear energy systems will eliminate the need for offsite emergency response*.

The early work of the RSWG focused on defining a safety philosophy for Generation IV systems that is founded on lessons learned from current and prior generations of nuclear technologies, and on identifying the characteristics that may help achieve Generation IV safety goals. More recently, the RSWG has focused on development of a methodology that will be used to assess and document the safety of Generation IV systems. Current work is focused on trial applications of the methodology, validation, and development of application guidance for designers.

2. An integrated philosophy of safety

An effective and homogeneous approach to the safety of Generation IV systems must be based on a coherent and well-founded safety philosophy. The RSWG has recommended that the following principles should underlie such a safety philosophy:

- Opportunities exist to further improve on nuclear power's already excellent safety record in most countries. As a starting point, the RSWG recognizes that the level of safety that has been attained by the vast majority of operating nuclear power plants (Generation II) in most countries of the world is already very good. Relative to Generation II systems, applicable quantitative safety objectives for third generation (e.g. AP1000 and EPR) nuclear power plants are very ambitious and provide a further improved level of safety. The RSWG believes that further enhancement in the level of safety associated with Generation IV technologies is possible through advanced technologies and early application of an integrated safety assessment methodology that yields insights that can help identify improvements to the developing design. Such improvements will focus on safety provisions that will be ***"built-in"*** to the fundamental design rather than ***"added on"*** to the system architecture.

- Potential safety improvements should simultaneously be based on several elements. These include the notion of "optimal risk reduction"; the adoption of ambitious safety objectives that will drive the research required to attain those objectives; the application of innovative technologies; an emphasis on accident prevention backed up by mitigation; the development of robust safety architecture; and improved means of demonstrating the system's safety robustness.

- The diversity of the Gen IV systems and the need for a homogeneous strategy applicable for the design and the assessment of these systems justify an updated safety approach. The traditional approach to safety is one that has consisted largely of prescriptive requirements based largely on "engineering judgment." The notion of the "design basis accident" as a bounding case underlies much of the historical safety basis for nuclear plants that began operation in the sixties and seventies. Advancements and analytical methods developed since then support an updated safety approach. Such an approach must include formal consideration of risk and safety issues throughout the design process, and must provide for prevention and mitigation relative to a broad spectrum of potential accident initiators and conditions.

- The principle of "defense in depth" has served the nuclear power industry well, and must be preserved in the design of Generation IV systems. Defense in depth is the key to achieve safety robustness, thereby helping to ensure that Generation IV systems do not exhibit any particularly dominant risk vulnerability. Embodied within the principle

of defense in depth is the notion that safety margins must exist as an effective response to uncertainty.

- The Design Basis for Generation IV energy systems should cover the full range of safety significant conditions. The historical notion of a single bounding design basis accident must be replaced by a "spectrum" of possible accidents that, while of low probability, represents with high confidence the range of physical events and phenomenology that could conceivably challenge the plant. Specific efforts, both analytical and empirical, should be made for demonstrating the "practical elimination" of initiators, sequences or situations associated with the extremely low residual risk.
- The Generation IV design process should be driven by a "risk-informed" approach. The RSWG believes that safety and economics of Generation IV designs can be positively influenced by formally adopting, as a complement to deterministic methods, the use of PSA techniques and complementary tools as design drivers throughout the design process.

3. A methodology for assessing and documenting the safety of generation IV systems

A major focus of the RSWG's charter is the development and demonstration of an integrated methodology that can be used to assess and document the safety of Generation IV nuclear systems. This methodology, called the Generation IV Integrated Safety Assessment Methodology (ISAM), is described in this section.

It is envisioned that the ISAM will be used in three principal ways:

- The ISAM is intended for use throughout the concept development and design phases with insights derived from the ISAM serving to actively drive the course of the design evolution. In this application of the methodology, the ISAM is used to develop a more detailed understanding of design vulnerabilities, and resulting contributions to risk. Based on this detailed understanding of vulnerabilities, new safety provisions or other design improvements can be introduced relatively early.
- Selected elements of the methodology will be applied at various points throughout the design evolution to yield an objective understanding of risk contributors, safety margins, effectiveness of safety-related design provisions, sources and impacts of uncertainties, and other issues that are important to decision makers.
- The ISAM can be applied in the late stages of design maturity to measure the level of safety and risk associated with a given design relative to some safety objective or licensing criterion. In this way, the ISAM will allow evaluation of a particular Generation IV concept or design relative to various potentially applicable safety metrics or "figures of merit." This *post facto* application of the ISAM will be especially useful for regulators and other decision makers who require objective measures of safety for licensing purposes, or to support certain late-stage design selection decisions.

It is specifically not intended that the methodology be used to dictate design requirements, that it dictate compliance with quantitative safety goals, or that it in any other way constrains designers. The sole intent is to provide a useful methodology that contributes to the attainment of Generation IV safety objectives, that yields useful insights into the nature of safety and risk of Generation IV systems, and that permits meaningful evaluations of Generation IV concepts with respect to safety.

Attributes of an Effective Safety Assessment Methodology

In formulating a Generation IV safety assessment methodology, the RSWG has sought to incorporate the following attributes:

- The methodology must actively contribute to the development of designs that fulfill the safety objectives of Generation IV systems.

- The methodology should consist of, or be largely based on existing tools that are widely accepted for their validity. Thus, the methodology should minimize the need for developing new tools and the potentially lengthy period of validation that may be necessary.

- The methodology must be understandable, and efficient.

- The methodology must allow for the integration of a diverse range of multidisciplinary inputs including those that are primarily probabilistic and those that are primarily deterministic in nature, as well as those that are principally qualitative and those that are principally quantitative.

- Based on the desirability of offering a graded approach to technical issues of varying complexity and importance, practicality and flexibility must be reflected in the methodology.

- Throughout the development process, the safety assessment methodology must help designers understand design vulnerabilities, and how alternative design solutions can reduce or eliminate those vulnerabilities. In order to successfully fulfill this role, the methodology must yield information about which aspects of design contribute most to the level of risk associated with that concept or design. Thus, the methodology must serve to do more than just measure safety after the design is complete.

- Importantly, the methodology must provide information that permits an understanding of the level of uncertainty associated with the measured level of safety, as well as an understanding of the sources of that uncertainty.

- Based largely, but not exclusively, on a systematic understanding of sources and magnitudes of uncertainties, the methodology must help identify areas for additional research, data collection, and improved analytical models.

- Within a given concept, the methodology must support comparisons of potential alternative design options.

- Must yield information that allows comparison of a concept or design relative to established safety metrics or “figures of merit.”

- Must yield a mix of both qualitative and quantitative information that will support eventual licensing and regulatory processes.

- To the extent that is appropriate, the methodology should be consistent with other relevant guidance and documentation including the RSWG Safety Philosophy document (Ref. 1), the Generation IV Proliferation Resistance and Physical Protection methodology (Ref. 7), and other work including the US NRC NUREG-1860 (Ref. 2), the IAEA TECDOC-1570 (Ref. 3), and others.

ISAM Overview

The ISAM provides an integrated set of tools that reasonably fulfills the list of desired methodological attributes outlined above. The ISAM is conceived to achieve comprehensive system safety assessment based largely on full scope probabilistic safety assessment, and supported by other methods that may be more appropriate at earlier stages of concept development. The integrated methodology consists of five distinct analytical tools. It is intended that each tool be used to answer specific kinds of safety-related questions in differing degrees of detail, and at different stages of design maturity. By providing specific tools to examine relevant safety issues at different points in the design evolution the ISAM as a whole offers the flexibility to allow a graded approach to the analysis of technical issues of varying complexity and importance. The methodology is well integrated, as evidenced by the fact that the results of each analysis tool support or relate to inputs or outputs of other tools. Although individual analytical tools can be selected for individual and exclusive use, the full value of the integrated methodology is derived from using each tool, in an iterative fashion and in combination with the others, throughout the development cycle.

Figure 1 shows a notional task flow diagram of the ISAM, and depicts elements of the integrated methodology and the stages of design development in which those elements are expected to be most useful.

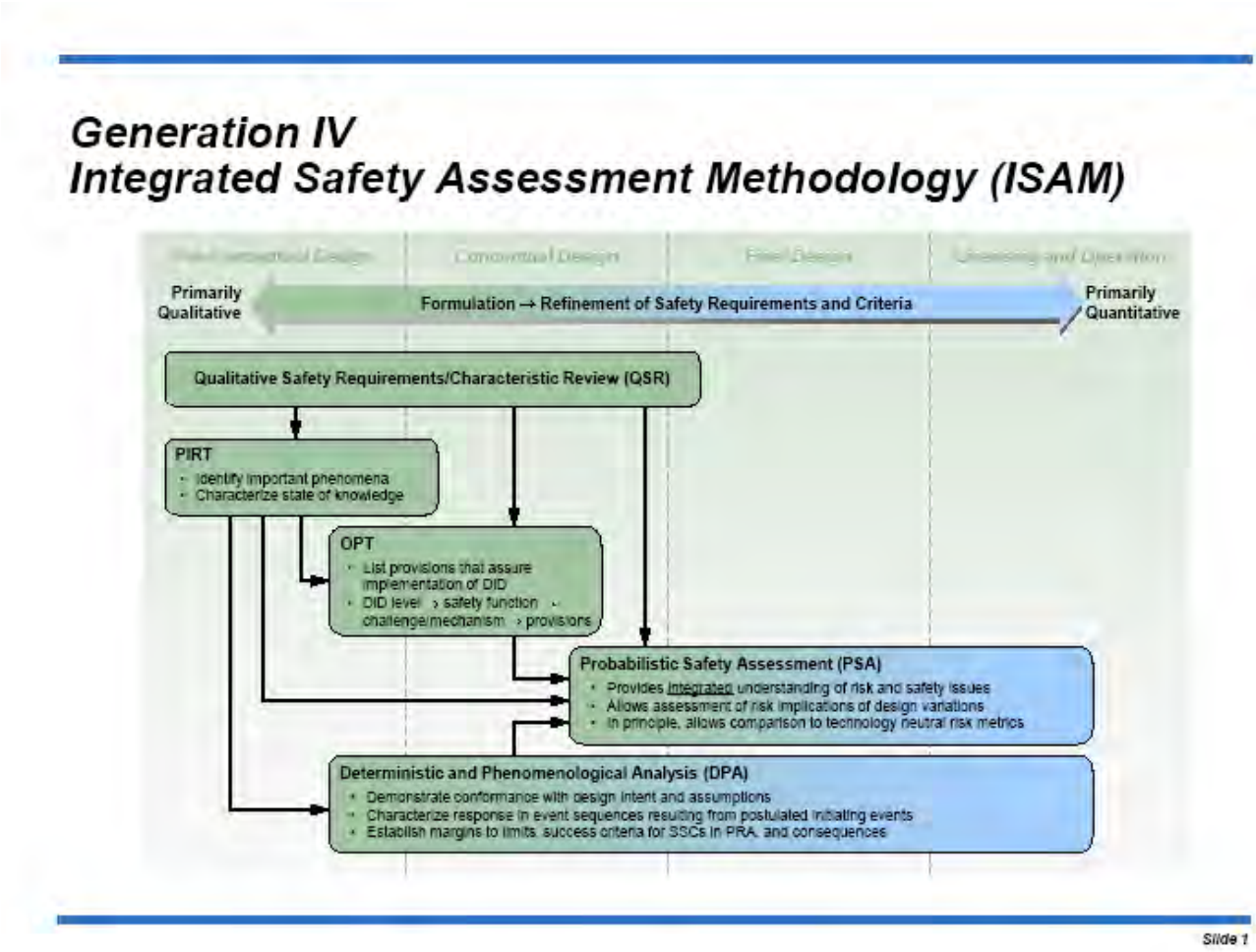


Figure 1 ISAM Overview

The ISAM consists of the following major elements:

- Qualitative Safety Features Review (QSR)

The Qualitative Safety Features Review is a new tool that provides a systematic means of ensuring and documenting that the evolving Generation IV system concept or design incorporates the desirable safety-related attributes and characteristics that are identified and discussed in the RSWG's first report entitled, "Basis for the Safety Approach for Design and Assessment of Generation IV Nuclear Systems." Although this element of the ISAM is specifically offered as an optional step, it is believed that the QSR provides a useful means of shaping designers' approaches to their work to help ensure that safety truly is "built-in, not added-onto" since the early phases of the design of Generation IV systems. Using a structured template to guide the process, concept and design developers are prompted to consider, for their respective systems, how the attributes of "defense in depth," high safety reliability, minimization of sensitivity to human error, and other important safety characteristics might best be incorporated. The QSR is not regarded as a tool that allows an analyst to determine whether or not a developing concept is "good enough," but rather, provides a measure of discipline to help ensure that certain desirable characteristics are incorporated into the design in its earliest phases. The QSR also serves as a useful preparatory step for other elements of the ISAM by promoting a richer understanding of the developing design in terms of safety issues that will be analyzed in more depth in those other analytical steps.

- Phenomena Identification and Ranking Table (PIRT)

The Phenomena Identification and Ranking Table is a technique that has been widely applied in both nuclear and non-nuclear applications. The PIRT provides a structured means of identifying and analyzing a wide variety of off-normal scenarios that potentially challenge the viability of complex technological systems. As applied to Generation IV nuclear systems, the PIRT is used to identify a spectrum of safety-related scenarios or phenomena that could affect those systems, and to rank order those scenarios on the basis of their frequencies and/or potential consequences.

The PIRT is used initially in the pre-conceptual design phase of a system's development, and is applied iteratively throughout the development process. It is to be used as an early "screening" tool to identify, categorize, and characterize phenomena and issues that are potentially important to risk and safety of a Generation IV system. The PIRT can be focused on very general issues, or on highly specific design issues, depending on the need. The method relies heavily on expert elicitation, but provides a discipline for identifying those issues that will undergo more rigorous analysis using the other tools that comprise the ISAM. As such, the PIRT forms an input to both the Objective Provision Tree (OPT) analyses, and the Probabilistic Safety Analysis (PSA) in identifying mechanisms and initiating events which will challenge the safety functions. In the case of the PSA, the PIRT is particularly helpful in defining the course of accident sequences, and defining safety system success criteria. The PIRT is also useful in helping to identify areas in which additional research may be helpful to reduce uncertainties.

- Objective Provision Tree (OPT)

The Objective Provision Tree is a relatively new analytical tool that is enjoying increasing use. The International Atomic Energy Agency (IAEA) has been a particularly influential

developer and proponent of this analysis tool. The purpose of the OPT is to ensure and document the provision of essential "lines of protection" to ensure successful prevention or mitigation of phenomena that could potentially damage the nuclear system. There is a natural interface between the OPT and the PIRT in that the PIRT identifies phenomena and issues that could potentially be important to safety, and the OPT focuses on identifying design provisions intended to prevent those phenomena or mitigate their consequences.

The OPT can be applied early in the pre-conceptual design phase, and iteratively through conceptual design. Note that the OPT is an entirely qualitative analysis method. As such, its purpose is to inform the design process and to help structure inputs that will eventually make their way into the PSA. The OPT can be extremely useful in helping to focus and structure the analyst's understanding of accident sequence phenomenology, sequence success criteria, and related issues. It will help providing the right requirements (e.g. requested performances and reliability) for the design of the implemented provisions.

- Deterministic and Phenomenological Analyses (DPA)

Classical deterministic and phenomenological analyses, including thermal-hydraulic analyses, computational fluid dynamics (CFD analyses, reactor physics analyses, accident simulation, materials behavior models, structural analysis models, and the like collectively constitute a vital part of the overall Generation IV ISAM. These traditional deterministic analyses will be used as needed to understand a wide range of safety issues that must guide concept and design development, and will form inputs into the PSA. These analyses typically involve the use of familiar deterministic safety analysis codes. It is anticipated that DPA will be used from the late portion of the pre-conceptual design phase through ultimate licensing and regulation of the Generation IV system.

- Probabilistic Safety Analysis (PSA)

As a widely accepted, integrative method that is rigorous, disciplined, and systematic, PSA forms the principal basis of the ISAM. As an element of ISAM, PSA is to be performed, and iterated, beginning in the late pre-conceptual design phase, and continuing through the final design stages addressing licensing and regulation concerns. The RSWG advocates the idea of applying PSA as the earliest practical point in the design process, and continuing to use it as a key decision tool throughout the life of the plant or system. Although the other elements of the ISAM have significant value as stand-alone analysis methods, to a significant degree, their value is enhanced by the fact that they serve as useful tools in helping to prepare for, and to shape, the PSA once the design has matured to a point where the PSA can be successfully applied.

To maximize its value within ISAM, the PSA should be performed as a "full scope" PSA that considers both internal and external events, and models potential accident phenomena from the hypothetical occurrence of an initiating event through the point at which accident progression is either arrested, or offsite consequences are realized.

One of the key strengths of the PSA is that it facilitates a systematic understanding of the uncertainties relating to the safety (or risk) of a Generation IV system. Uncertainties arise from a number of sources. The traditional response to these safety-related uncertainties has been the provision of additional "safety margin" in the design, often based largely on "engineering judgment," to provide assurance that in the event of any accident, severe loss or

damage will not occur. Adding such safety margins is, of course, expensive, and may also lead to an inappropriate focus on some aspects of design and operation to the detriment of other issues that may, in fact, be more important to safety. By facilitating a disciplined, systematic understanding of the sources and magnitudes of safety-related uncertainties, the PSA will play a key role in helping to ensure that cost and safety issues are more optimally balanced.

4. Conclusions

Advanced technologies and a safety approach driven by insights derived from an integrated safety assessment methodology hold the promise of making Generation IV nuclear energy systems even safer than the current generation of nuclear plants.

The ISAM is best thought of as a toolkit of useful analysis tools. Although the ISAM is focused to ultimately support completion of a full-scope PSA, the strength of the ISAM is that it offers tools that are tailored to answering specific types of questions at various stages of design development, and that the elements of the methodology complement and support one another in a way that contributes to a much more complete understanding of the range of safety issues. It is anticipated that using the elements of the ISAM in an integrated way will result in optimizing safety, reducing technology development cycle time, reducing development costs, and facilitating licensing of Generation IV systems. Future work will focus on additional applications of the ISAM at various stages of technology development for selected Generation IV reactor types, interactions with the GIF steering committees developing the six concepts, and development of guidance for ISAM applications.

References

1. *"Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems,"* Rev. 1, Generation IV International Forum, GIF/RSWG/2007/002, November 24, 2008.

2. *"Feasibility Study for a Risk-informed and Performance-Based Regulatory Structure for Future Plant Licensing* (NUREG 1860)." US Nuclear Regulatory Commission, December 2007.

3. "*Proposal for a Technology-Neutral Safety Approach for New Reactor Designs* (TECDOC-1570)." International Atomic Energy Agency, September 2007.

4. *"Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants* (TECDOC-1511)." International Atomic Energy Agency, July 2006.

5. *"A Risk-Informed, Performance-Based Regulatory Framework for Power Reactors* (NEI-02-02)." Nuclear Energy Institute, May 2002.

6. *"Policy Statement on the Regulation of Advanced Reactors."* NRC-2008-0237, US Nuclear Regulatory Commission, Federal Register. October 14, 2008.

7. "*Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems,"* Rev. 5, Generation IV International Forum, GIF/PRPPWG/2006/005, November 30, 2006.

8. "*A Technology Roadmap for Generation IV Nuclear Energy Systems,"* Generation IV International Forum, GIF-002-00, December 2002.

Status of GIF Risk and Safety Working Group Evaluation Methodology

Tim Leahy
RSWG Chair

20 June 2011

PSA for New and Advanced Reactors Workshop
OECD Headquarters
Paris FRANCE

A Little Background

- *Generation IV: "Reactors after next" – deployable in about 2030*
- *Achieve significant breakthroughs in safety, economics, non-proliferation, and waste characteristics*
- *International collaborative research programs involving Canada, China, Euratom, France, Japan, Republic of Korea, Russian Federation, Republic of South Africa, Switzerland, and USA. Non-active members are Argentina, Brazil, and UK.*
- *R&D focused on six diverse concepts including VHTR, SFR, LFR, SFR, SCWR, MSR. Each led by System Steering Committee.*

Slide 2

Purpose of the RSWG

- *"Promote a consistent approach on safety, risk, and regulatory issues between Generation IV systems"*
- *Advise and assist the Experts Group and the Policy Group particularly on matters of:*
  - *Generation IV safety goals and evaluation methodologies to be considered in the design*
  - *Interactions with the nuclear safety regulatory community, the IAEA, and relevant stakeholder*

Slide 3

A Viable Assessment Methodology Must Fulfill Multiple Purposes

- *Commensurate with design maturity, yields a complete and detailed understanding of relevant risk and safety issues*
- *Within a given concept or design:*
  - *guides the design process based on a detailed understanding of risk and safety*
  - *helps identify areas for additional research and data collection*
- *Promotes understanding of differences between concepts and designs based on risk and safety issues*
- *Allow evaluation of a concept or design relative to various safety metrics or "figures of merit"*
- *Support licensing and regulatory processes*

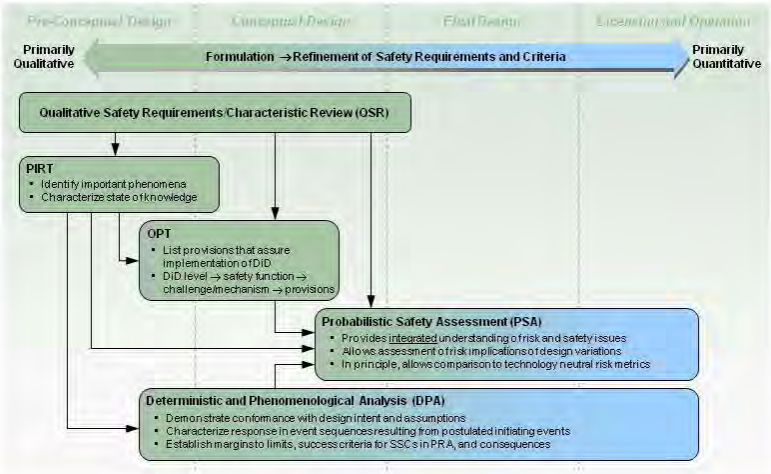
Slide 4

Desirable Characteristics of an Assessment Methodology

- *Consists of, or is largely based on, existing tools that are widely accepted for their validity. Minimizes need for development of new techniques.*
- *Practical and flexible - allows for graded approach to technical issues of varying complexity and importance. Offers analysis tools tailored to appropriate stage of design*
- *Identifies vulnerabilities and relative contributions to risk*
- *Allows for explicit consideration and characterization of uncertainty*
- *Supports integration of multidisciplinary inputs*
- *Combines probabilistic and deterministic perspectives*
- *Consistent with RSWG safety philosophy, PRPP methodology, and other relevant work (NUREG-1860, TECDOC-1570, etc)*

Slide 5

Generation IV
Integrated Safety Assessment Methodology (ISAM)



Slide 6

ISAM as a "Design Driver"

- *From earliest phases, developers must strive to reduce or eliminate vulnerabilities. Beginning in the "pre-conceptual" development phase, ISAM provides the systematic means to identify vulnerabilities and their magnitudes*
- *Uncertainties imply need for added safety margin*
- *ISAM can be used to assess effectiveness of design provisions - safety and cost optimization*
- *As design matures, ISAM is iteratively updated in a way that both reflects and guides ("drives") the evolving design*
- *Methodologically consistent with the notion that, in Gen IV systems, safety must be "built-in, not added-on"*

Slide 7

Validation of ISAM Approach

- *Representatives of national regulators, international nuclear industry, and IAEA have participated in ISAM development or commented on its appropriateness and utility*
- *Feedback has been strongly and quite consistently positive*
- *Limited applications of methodology elements to Japanese and French SFR concepts confirm value and "usability"*
- *More formal interactions with SSCs have commenced*

Slide 8

RSWG Engagement with SSCs is Key to Ensure Relevance

- RSWG/SSC Workshop - Joint Research Center, Petten NL
- Workshop included excellent participation by representatives of all six SSCs
- Purposes of the JRC workshop:
  - To provide detailed information regarding the ISAM and the elements that comprise it
  - To discuss the ISAM and its elements, and to obtain informal feedback from the SSCs regarding usefulness, appropriateness, and practicality
  - Briefings on the status of each system development activity with focus on primary safety issues and challenges

Slide 9

JRC Workshop Outcomes

- Representatives of all six SSCs gained a much fuller understanding of the ISAM, its purposes, and its application
- Overall, all six SSC representatives expressed strong support for ISAM and endorsed its value and practicality
  - Clear consensus to begin using it on a trial basis
  - At least two development teams are already doing so
- The only significant concern expressed by the SSCs related to resource requirements and expertise needed to apply the ISAM
- Draft ISAM document includes comments and perspectives discussed at the workshop

Slide 10

ISAM - Next Steps

- *As proposed by GIF Chair Sagayama, work with SFR SSC to use RSWG guidance in defining SFR design criteria*
- *Finalize Methodology Document in 2011*
- *More systematic, detailed applications (and evaluation) of ISAM by the SSCs*
- *Definition of RSWG role in supporting SSCs for ISAM application and documentation*
- *Proposed formal "pilot" of ISAM methodology for selected system(s) to be led by system development team with assistance from RSWG*
- *Continued interface with IAEA, INPRO, MDEP, PRPP, and others*

Slide 11

ASAMPSA2 project: Appliance of LWR PSA2 methodology to GEN IV reactors

H. Bonneville (1), C. Bassi (2), F. Bertrand (2), J.L. Brinkman (3), L. Burgazzi (4), S. Jouve (5), F. Polidoro (6), E. Raimond (1), F. Serre (2), L. Vinçon (5)

1) IRSN, 31, avenue de la division Leclerc BP 17. 92262 Fontenay-aux-Roses cedex. France. herve.bonneville@irsn.fr
2) CEA Cadarache – BP 1 13108 Saint-Paul lez Durance cedex. France. frederic.serre@cea.fr
3) NRG – Utrechtseweg 310, 6800 ES Arnhem. The Netherlands. brinkman@nrg.eu
4) ENEA – Via Martiri di Monte Sole 4, 40129 Bologna, Italy. burgazzi@bologna.enea.it
5) AREVA NP - 10, rue Juliette Récamier, 69006 Lyon. France. laurent.vincon@areva.com
6) RSE S.p.A. - Via R. Rubattino 54. 20134 Milano. Italy. polidoro@rse-web.it

Abstract

The European project ASAMPSA2 (Advanced Safety Assessment Methodology: level 2 PSA) of the 7th Framework Program aims at writing practical guidelines for conducting PSA level 2 studies on Light Water Reactors (PWR and BWR). The project includes also a supplemental task dealing with GEN IV reactors. Two main objectives are assigned to this task: 1) the verification of the potential compliance of L2PSA guidelines based on PWR/BWR reactors with Generation IV concepts; 2) a brief survey of the modelling needs to describe the new features of GEN IV reactor concepts in terms of performing a level 2 PSA.
Taking into account the ASAMPSA2 partners knowledge, the project has focused on four concepts: SFR, LFR, GFR and VHTR. For each of those concepts, a conceptual design was selected as reference: the European Fast Reactor (EFR) for sodium cooled fast reactors, the ELSY project for lead cooled fast reactor, the CEA GFR2400 project and the ANTARES project for VHTR.
As a first stage, relevant data for each concept have been collected when available. These included: 1) basic general parameters and design characteristics relevant for safety studies with a specific attention given to passive devices; 2) information about former PSA2 studies on such concepts; 3) expert reviews about accident phenomenology knowledge (like PIRT); 4) list of computational tools developed or used for accident progression studies with, if possible, some basic information about the tools (availability, level of development, validation, documentation).
In a second stage, the collected data were used to evaluate the compliance of the LWR guideline chapters with GEN IV concepts. The LWR guidelines may be divided into two main sections: chapters dealing with a specific phenomenon induced by core degradation and chapters dealing with general PSA methodology (like interface between PSA1 and PSA2, human risk assessment, system modelling and the role of expert opinion). The overall conclusion is that methodology is not very much affected by the reactor type contrary to what is related to the accident phenomena.

Keywords: GEN IV, ASAMPSA2, LEVEL 2 PSA

1. Brief survey of the ASAMPSA2 project

The European project ASAMPSA2 (Advanced Safety Assessment Methodology: level 2 Probabilistic Safety Assessment – L2PSA) of the 7th European Framework Program (EU-FP7) aimed at developing best practice guidelines for the performance of Level 2 PSA on Light Water Reactor – LWR. Pressurized Water Reactor – PWR – as well as Boiling Water Reactor – BWR – were considered. Specific concerns of the project were L2PSA methodology harmonization at EU level and methodology for uncertainty evaluation in a Level-2 PSA. As a result guidelines for both limited scope and fuel scope L2PSA, based on each of the 22 partners' practical experience, were issued.

A small part of the project was devised as an extension to GEN IV reactors with two objectives:

- to determine how far the L2PSA methodology guidelines are relevant for GEN IV concepts,
- to provide a basis for the development of new models or extension of existing models to describe the GEN IV reactors specific "mechanisms".

Although this Work Package goal is ambitious, only restricted human and financial means have been allotted.

Work started in February 2008 and has been concluded in November 2010. A draft report has been sent to a great number of organisations all around the world with an extensive questionnaire. Received answers have been analyzed and discussed during an open meeting held in last March. Based on this analysis and available time, improvements to the report will be operated before end of year 2011. Possibilities to extend the project are under discussions.

2. Applied methodology for GEN IV

During the work package kick-off meeting, it was agreed among participants to work along three steps.

The first step of the project was to select a reference design for each of the six pre-selected GEN IV concepts and to collect relevant data for each of those designs. Data availability for participants resulted in keeping only four of the six nuclear reactor concepts elected by the GEN IV forum as of special interest (sodium cooled fast reactor, lead cooled fast reactor, gas cooled fast reactor and very high temperature reactor). The molten salt reactor and supercritical water cooled reactor were set aside as nobody in the team had any involvement with these reactor types. Data considered as significant for safety issues (core features, containment features) were then collected for each of the four selected designs.

The **second step** has been the collection of a wide range of information connected with the following issues:

1. the identification of specific degradation mechanisms as the so-called core disruptive accidents for fast neutron reactors,
2. the specific provisions for prevention and mitigation of severe accidents with a special concern for passive systems which should be widely used for GEN IV reactors. An example of such systems is the Japanese FAIDUS to relocate molten fuel out of the core to ensure the reactor remains sub-critical,
3. the parameters which should be of importance for the source term evaluation. One may quote the sodium chemistry for instance and the possibility to generate new physical species by combination between fission products and sodium. Those products may be liable to more important retention than the isolated fission product,
4. the R & D needs if such evaluation was available,
5. the specificity of shut-down states as for instance the rotating plug for SFR to prevent contact between sodium and atmosphere due to its strong reactivity with air,
6. to try to get information about previous PSA2 studies conducted on similar concepts,
7. to make a first survey of available codes for PSA2 studies on such reactors (and reciprocally needs for codes).

Then once all those information had been collected as much as possible in the project frame, the **third step** has been to evaluate the relevance of the guidelines written for LWR for those GEN IV reactors.

3. The four reference designs selected

For the four selected concepts, the reference projects have been: the EFR project for Sodium Fast Reactor (SFR), the ELSY project for Lead Fast Reactor (LFR), the GFR 2400 CEA project for Gas Fast Reactor (GFR) and the AREVA ANTARES project for Very High Temperature Reactor (VHTR).

The **European Fast Reactor** (EFR) project was selected as a representative for SFR designs. The EFR project was a European project stopped in 1998 and aiming at embodying all the Western Europe know-how about sodium cooled fast breeders gathered at the time. It had been quite an advanced project (with teams having worked on it for around 10 years) ultimately cancelled when it became obvious it would not be possible to build a new SFR anywhere in Western Europe before long. It’s a

3600 MWth, fast neutron spectrum sodium cooled pool-type (so different from the MONJU loop type reactor and similar to the Super PheniX - SPX concept) reactor.

The **ELSY** project (Alemberti and al., 2011) was chosen as a representative for lead cooled fast reactors. The ELSY project - developed in the frame of the EU-FP6 by a consortium of organizations - aims to demonstrate the possibility to design a competitive and safe fast critical reactor using simple engineered technical features. The ELSY power plant is a pool-type reactor concept, sized at 600 MWe, and uses lead as primary coolant. With a core outlet temperature close to 480°C, the primary side cycle is consistent with a secondary side water-supercritical steam at 200 bars and 450°C providing a thermal efficiency above 40%. Lead was preferred to the lead/bismuth eutectics (LBE) since it is less expensive, less corrosive and of lesser radiological concern than LBE.

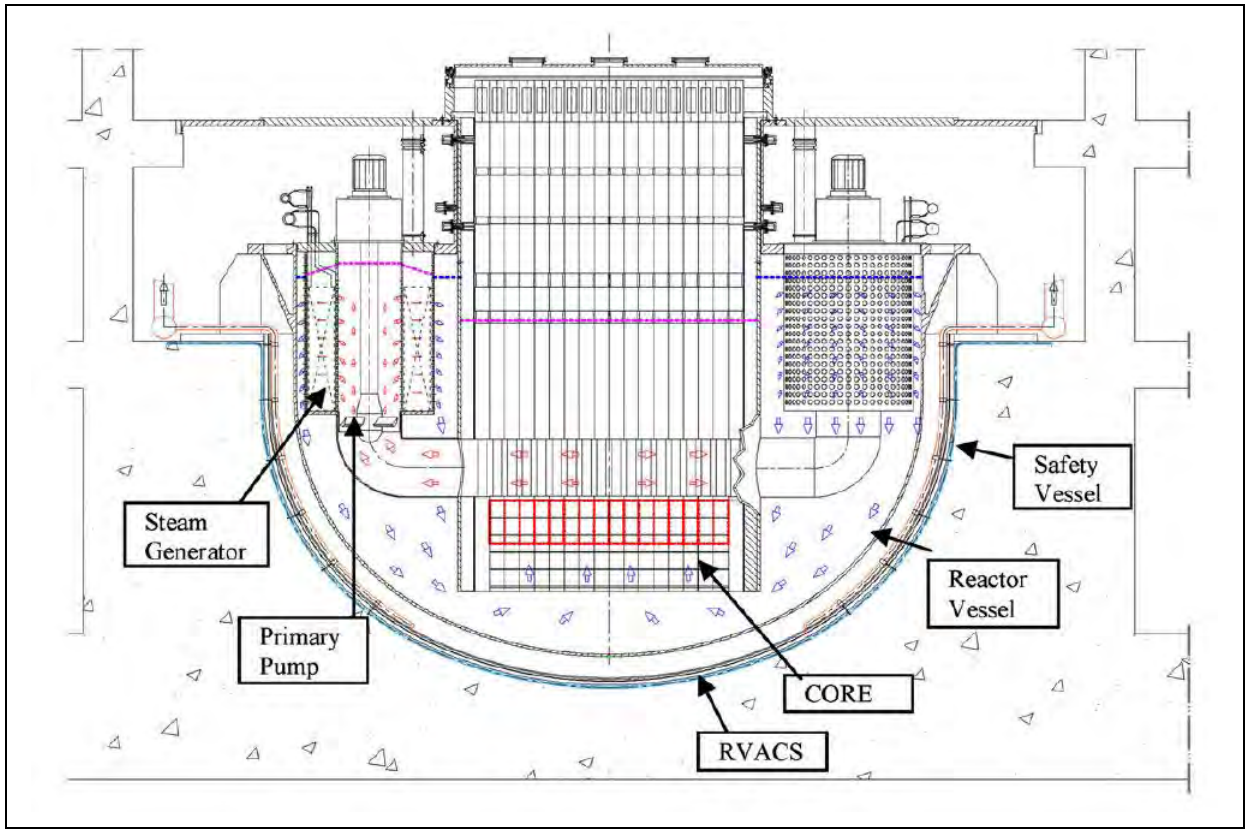


Figure 1 : sketch of the ELSY reactor concept

The **Gas cooled Fast Reactor** 2400 MWth (Dumaz and al., 2006) is a project developed by the CEA. As at least three papers presented during this OECD conference are dealing with this reactor, only limited information is provided here. No GFR prototype has ever been built although the idea to build such a reactor is rather old since it combines the advantages of the fast neutron reactors (high efficiency for electric production and possibilities of direct heat uses). As well the coolant is chemically inert (no corrosion or violent chemical reactions) and transparent which ease the monitoring, handling and repairing. However, since the helium density at low pressure is rather small, for core heat removal the reactor must be operated at high pressure contrary to the metal cooled reactors. It must be pointed out that loss of coolant accident doesn't lead to prompt criticity as in current SFRs. The reactor reference design in the project was a 2008 design with a very innovative fuel-plate concept displayed below with ceramic cladding. Some technological developments and component qualifications are still necessary to build an experimental reactor before building an industrial prototype.

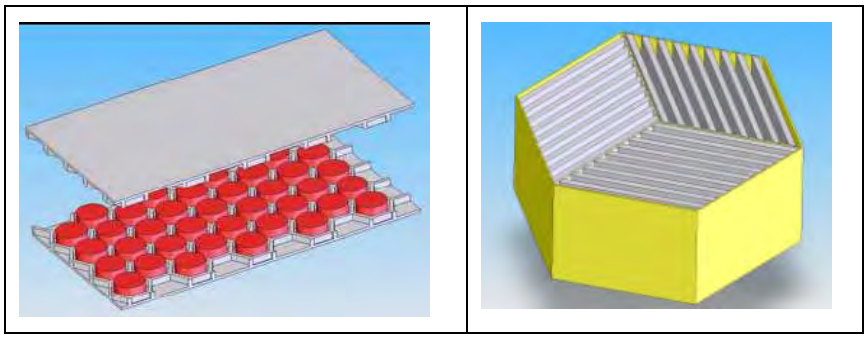


Figure 2: GFR reference fuel for the ASAMPSA2 project

The use of helium as a coolant means there are some similarities with the VHTR concept and a possibility to profit from some of the VHTR feedback.

For the AREVA **ANTARES** project (Gauthier and al., 2006) – a VHTR - some specificities of the concept may be summarized as follows:

1. it's a thermal reactor, the only one among the four projects, with graphite as moderator and helium as coolant,
2. it's an industrial project, so that access to the data remained quite limited,
3. it's a reactor design with a rather rich former history with at least five operational parent reactors having worked in the past and several projects being either built or having recently begun operation. This feature is a specificity shared with the SFR but which makes it distinct from the GFR and LFR.
4. it's a 600 MWth reactor, so rather a small reactor contrary to the three other projects.

For fuel packaging, the ANTARES project uses a prismatic bloc type core (UO2 fuel, TRISO coated particles) like the Fort Saint-Vrain reactor (USA) and different from the pebble bed concept built in Germany. The power cycle is an indirect cycle with the gas turbine located in the secondary circuit but still with a thermal efficiency of around 45 to 50% due to high temperature.

Examples of data we tried to collect for each of the four representative concepts are:

- for the primary circuit: nature of coolant, mass of the fluid, inertia of the circuit (fluid and structures), operating pressure, core inlet temperature, core outlet temperature (mean and maximum),
- for the secondary circuit: nature of coolant, mass or volume of the fluid, operating pressure and maximum temperature,
- for the containment: containment free volume, containment design pressure, maximum mass for H_2, CO and CO2 which is liable to be present in the containment,
- data needed for the assessment of the accident progression tree and related phases like main materials used for fuel, claddings, moderators and core structures and mass inventories for those materials.

Nota: in what follows, examples will be taken from one or the other design.

4. Specific provisions for prevention and mitigation of severe accidents consequences

In both PWRs and BWRs, several provisions are used in order to limit the consequences of Severe Accidents (SA). For PWR, such a provision is for instance the containment spray system, to reduce the containment pressure and remove the decay heat, or the use of igniters or catalytic recombiners for hydrogen control inside the containment.

For Generation IV reactors, different "devices" are specifically engineered for prevention and mitigation of Severe Accidents. They can be classified as:

1. a 3rd shutdown system. Such a system is implemented on some fast reactors and it could be self-actuated (a passive device not only for the rod insertion but also without the need of any signal: the actuation of the system is caused by effects induced by the transient like material dilatation in case of overheating of the coolant for instance) according to some GEN IV projects.
2. a specific design of the core assembly to promote the corium spreading and local recovery of cooling path. One may mention here the Japanese FAIDUS system which allows fuel ejection outside the core to prevent a Core Disruptive Accident (see below). Previous reactor designs (SNR 300, SPX, Monju and CRBR) have all designed some structures to resist the mechanical load due to a Core Disruptive Accident (CDA) in order to mitigate its short-term consequences.
3. a core catcher to collect the molten core materials is foreseen on several concepts. Both its location, inside or outside the core vessel and its composition are subjects under investigation among specialists. Collected material re-criticality is of specific concern. No core catcher is foreseen at the moment for ELSY and such a device is not relevant for VHTR (no core melting).
4. engineered safety features for containment like for instance specific filters before venting the containment to atmosphere in order to keep off-site doses within regulatory limits.

Severe accident management strategy will for sure play an important role but it needs a well-defined design to be developed.

5. Compliance and potential transposition of containment degradation modes

A short description of the major accidental transients liable to occur has been provided for each of the design based on the present knowledge. It is not possible to detail here those accident transients (and it was not the object of the work performed) but some features are useful to remind.

The Core Disruptive Accident, a accidental transient characterized by a prompt critical reactivity increase, was a central part in the safety analyses of previous SFRs and may occur in some other fast reactors. Such an accident is connected with coolant voiding effect or with fissile material compaction effects. It has a highly complex phenomenology with many possibilities in its development. The reactivity increase will end with material dispersion but may lead to fuel or steel vaporization and/or fuel-coolant interaction. A generally adopted solution is to design the primary vessel so that it can resist to a rather large amount of mechanical energy release. However it may be a challenge to demonstrate the mechanical load is well estimated.

On another hand, it must also be pointed out that for lead and sodium cooled fast reactors, the coolant choice induces a specific chemical risk absent with an inert gas as helium.

VHTR are very different reactors for which the reference accident scenario is a core heat-up accident, typically a loss of coolant flow without control rod fall. If all the active safety measures are failing for some reason, core temperature will rise but very slowly due to both the core huge thermal inertia (linked to the graphite weight) and the low power density. The reactor design is adapted so that

maximum fuel particle temperature should (in theory) not exceed some reference temperature (for the moment 1600°C is currently considered).

In the WASH 1400 report about severe accidents of Light Water Reactor (LWR), representative containment failure mechanisms were depicted by the so-called α, ß, γ, δ et ε-modes. A tentative extension of this commonly used terminology to GEN IV reactors has been proposed to help creating a common language for discussions (see Table 1 below) based on the potential transients. For instance, Core Disruptive Accidents (CDA) for fast reactors have been assimilated to the α mode as have been dust explosions on VHTR.

Table 1: transposition of LWR containment degradation loss to GEN IV reactors

Mode	SFR (EFR)	GFR (CEA design)	LFR (ELSY)	VHTR (ANTARES)
α-mode	Mechanical energy release in case of Core Disruptive Accident (recriticality in case of core degradation, Fuel Coolant Interactions - FCI)	Energy release due to recriticality in case of core degradation	Steam explosion due to Steam Generator Tube Rupture	Dust explosion (or δ-mode ?)
ß-mode	IHX, DHX tube rupture Secondary containment failure	Identical to LWRs, even if containment and related systems are not well known, IS-LOCA (IHX, DHX tube rupture) combined with the containment isolation failure, HSS failure	Steam Generator Tube Rupture, Containment Isolation failure	Identical to LWRs because of the thermal loading of the IHX (failure of the isolation valves)
γ-mode	Na fire	H2 / CO emission (following steam ingress in the “carbide” core)	H2, CO/CO2 emission (following MCCI)	H2 / CO emission (following steam ingress in the graphite moderated core)
δ-mode	Na vaporization (in case of LDHR)	H2 or CO slow deflagration, failure of the guard vessel → pressurization of the Containment Building	Over pressurization in containment building	Dust explosion (or α-mode ?)
ε-mode	Corium / Concrete Interactions (MCCI)	Fuel Coolant Interaction (FCI)	Molten Core - Concrete Interaction (MCCI)	Not relevant

6. Review of existing L2PSA applied to SFR, LFR, HTR or GFR

No evidence of any L2PSA for a GFR or LFR design has been found. Due to the "old history" of the concepts, such studies have been previously performed for SFR or HTR reactors and several documents are freely accessible.

No L2PSA was performed to our knowledge for the EFR concept. However, it should be emphasised that probabilistic studies were performed in the past for the US PRISM concept and the German SNR-300 reactor (GRS-51, 1982) whereas one is going on for the JSFR (and is the object of several papers in this meeting).

For HTR, evidence exist that PSA studies were formerly conducted for the American HTGR project by General Atomics, the German HTR-1160, the American MHTGR project (Everline, 1986) and the South-African PBMR.

7. Existing tools for severe accident analysis

Initially, it has been tried to identify those areas for which the phenomenology understanding is still too limited. For VHTR, PIRTs ordered by the NRC and in open access provide an up-to-date status of the art. Many information is also available for SFR and a summary has been given. No such survey is available to our knowledge for the two remaining concepts although some indications have been recorded. **Successively**, a tentative list of available codes for severe accident analysis is proposed. In many cases, the information collected is rather poor as participants may have only second-hand knowledge on several codes. Moreover, many of those codes are probably lost as they have not been used for years or have not been maintained. Anyway even a slight documentation about physical models coded may prove useful.

8. Screening of the compliance with L2PSA guidelines of LWR

8.1 Compliance with LWR phenomena and systems

Based on information collected a tentative scoring of LWR volume chapters with respect to their compliance with Gen IV reactors has been made. For each reactor and each chapter a score between 1 (high compliance) and 5 (no compliance) has been assigned depending on the evaluated relevance of the chapter for the reactor considered.

Not surprisingly, quite a large number of phenomena occurring in GEN IV reactors are not handled by the LWR guidelines (the CDA is a typical example) and, reciprocally, phenomena of importance in LWR are often absent in some or all GEN IV designs looked at. Even when similarities are present they may be quite limited. Two examples are given:

1) Molten Core Concrete Interaction is a phenomenon not to be expected for VHTR as the core should not melt. For fast reactors, it remains a possibility although due to the coolant and fuel specificities it should differ from what may occur on LWR. So scoring should be something as 5 i.e. "not relevant" for VHTR whereas it should be something average for other reactors (so a 3).

2) Hydrogen behaviour in the containment, risks associated to its detonation or explosion and the means to prevent such events to occur, the mechanical loads associated to such events and the containment answer to such loads are subjects much studied on LWR. A comparable problem is also present in GEN IV reactors even if the environment differs (containment volume, other chemical species present in the containment). So it may be assumed that past experience may prove useful for future.

What remains of interest in the ASAMPSA2-LWR work is mostly all the chapters dealing with non-phenomenological issues as human factor management, event-tree building techniques, how to make the binning between PSA1 and PSA2 etc.

8.2 L1PSA-L2PSA modelling structure

For Generation IV reactors the choice between performing a stand alone integrated L1/L2PSA model describing the accidental sequence from the initial event to the containment failure versus a L2PSA decoupled from the L1PSA should be discussed, knowing that Generation IV concept are not currently finalised. On the one hand an "integrated" model should be assimilated to a "simplified" model according the lack of knowledge and of operational feedback for these reactors but could lead to design improvement, especially for the containment building whose design is still subject to modifications. On the other hand, L1-L2 interface technique and building two decoupled models provide some advantages as:

- a capability of improvements and refinement of the models, thanks to the increase in the knowledge regarding physical situations or phenomena (through experiments, simulation...) for L2PSA.
- a decrease of the number of L2 representative initial states (and corollary the number of event trees in the L2PSA model) and therefore, a decrease of the amount of representative sequences that should be assessed by code calculations.

For the VHTR concept the question of making a distinction between L1PSA and L2PSA studies for VHTR may not be of concern:

- there is no core melting possibility with VHTR, the accident progression analysis is easier: a Level 2 analysis for a VHTR is straight forward and no change in methodology is needed.
- there is only a limited number of accident scenarios and safety systems so that it is worthwhile modelling the accident sequence up to external release using one event tree combining level-1 and 2 PSA and skip the plant damage state binning.
- some VHTR concepts as the South-African PBMR for instance have no containment which reduces the level 2 analysis significantly: no containment response analysis is needed.

8.3 Accident Progression Event Tree (APET) examples

Some attempts to build up simple APET trees have been committed. There should be seen as a preliminary step on the way to build up a L2PSA in the future.

For a **SFR**, the Level 2 PSA event tree might not be very large. The events that will be modelled will be the action of isolation of the containment and the reliability of the coolability of the corium spread on the core catcher.

For **ELSY** the reactivity increase accident implying the CDA (Core Disruptive Accident) conducting to lead boiling is not considered, given the high boiling point of the lead, with respect to sodium for example, that makes that kind of accident extremely unlikely. A potentially very severe accident is initiated by a Steam Generator Tube Rupture (SGTR), which can potentially lead to steam explosion, due to the interaction between hot molten lead and relatively cold water at high pressure. The violent expansion of this high-pressure steam bubble loads and deforms the reactor vessel and the internal structures, thus endangering the safety of the containment and the nuclear plant. The accident leads to radioactive releases into the containment due to failure of the top of the vessel. Missile emission due to the steam explosion can challenge the containment integrity (α mode). It has to be considered also the interaction of water/steam with materials potentially causing also the production of hydrogen, so that one can have early containment failure (γ mode), even if with a low likelihood. After rupture it's possible to have a have failure of the containment due to MCCI (ε mode); γ mode failure results as combustion of H2 and other burnable gases as CO and CO2 resulting from Molten Core Concrete Interaction; finally we can have late containment failure due to over-pressurization.

For **VHTR**, typical accidental tree for a loss of coolant flow accident may be found in older sources as for instance results of the PSA studies on the German HTR-1160 (FASSBINDER). Such an event tree

remains meaningful although some branches should be erased or added depending of the safety systems present on the design considered. If the safety heat removal devices do not work, core and fuel will heat up but at a rather slow pace due to the power density and huge graphite mass. At a certain time operators should depressurize the primary circuit which will enhance an important activity release inside the containment (a specificity of the VHTR is that a certain amount of contamination of the primary circuit has to be accepted so that depressurization will lead to a significant fission product transfer to the containment). Then the containment tightness and containment failure mode should be studied. The core is designed so that maximum core temperature should stabilize below a critical temperature above which fuel particle coating should fail. So the activity released inside the containment at depressurization time should remain the major contributor to the source term.

8.4 Miscellaneous

At the moment, no human reliability assessment is possible as no accident mitigation measures and procedures are defined on any of the reference concepts.

There is a clear will to use passive system on GEN IV reactors to a greater extent than was the case with LWRs. Failure assessment of such devices is a rather complex problem, combination of physics and human factors.

Several calculation tools exist. Their availability should be checked. In any case their level of validation and their applicability to the different concepts should be checked. The technical know-how to use those tools needs also to be rebuilt at least partly.

The role and extend of expert judgment will probably be significantly more important than with LWRs due to the limited feedback.

9. Conclusion

On a whole as projects on GEN IV reactors are just being restarted in the European environment, a lot of skills have to be rebuilt and designs to be more precisely defined before we can manage a complete L2PSA on any of the concepts. Simplified L2PSA may be performed at an early stage of design:

- to identify the major containment failure modes and the main phenomena contributing to containment failure,
- to estimate roughly the quantities of radioactive material released to the environment for different accident sequences,
- to help prioritising the R&D needs.

10. Glossary

BWR	Boiling Water Reactor
CRBR	Clinch River Brooder Reactor
FCI	Fuel Coolant Interaction
GFR	Gas Fast Reactor
IE	Initial Event
LBE	Lead Bismuth Eutectics
LFR	Lead Fast Reactor
LWR	Light Water Reactor
MCCI	Molten Core Concrete Interaction

PIRT	Phenomena Identification and Ranking Table
PWR	Pressurized Water Reactor
SA	Severe Accident
SFR	Sodium Fast Reactor
SPX	Super PheniX
VHTR	Very High Temperature Reactor

12. References

ALEMBERTI, CARLSSON, MALAMBU, ORDEN, STRUWE, AGOSTINI, MONTI, (to be published in 2011), European lead fast reactor – ELSY. Nuclear engineering and design (electronic version available)

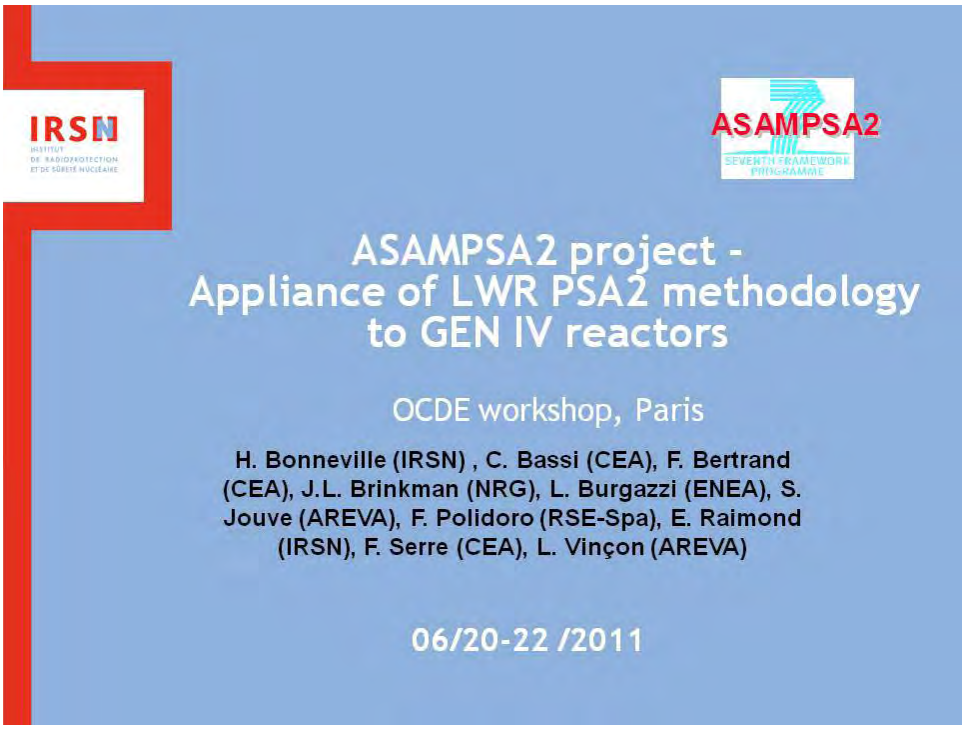
DUMAZ, ALLEGRE, BASSI, CADIOU, CONTI, GARNIER, MALO, TOSELLO, (2006), Gas-cooled fast reactors – status of CEA preliminary design studies, Nuclear engineering and design 237

EVERLINE, (1986), Probabilistic Risk Assessment of the Modular HTGR plant, issued by General Atomics for the DOE. Reference HTGR-86-011.

FASSBENDER & KRÖGER. Results of a German probabilistic risk assessment study for the HTR-1160 concept. Available on the AIEA website

GAUTHIER, BRINKMANN, COPSEY, LECOMTE, (2006), ANTARES : the HTR/VHTR project at Framatome ANP. Nuclear engineering and design 236.

GRS-51. Risikoorientierte Analyse zum SNR-300. Publication from GRS, Oktober 1982. ISBN 3-923875-00-2



PART 1 - Information on ASAMPSA2 project

PART 2 - Treatment of Gen IV reactors

PART 1 - The ASAMPSA2 project:

- *ASAMPSA2 stands for "Advanced Safety Assessment Methodology: level 2 PSA"*
- Project in the frame of the 7th European Framework Program (FP).
- FP = funding programmes created by the European Union in order to support and encourage research in the European Research Area.
- Goal of the project : developing best practice guidelines for the performance of Level 2 PSA for PWR and BWR

IRSN

The ASAMPSA2 project:

- Specific concerns of the project were L2PSA methodology harmonization at EU level and methodology for uncertainty evaluation in a Level-2 PSA
- 22 partners
- Kick-off meeting in 2008
- Work was initiated with the writing and the sending of a questionnaire to end-users in Europe to clarify and crystallize their views about the performance of Level 2 PSAs
- Conclusion discussed during an open Workshop in October 2008 (Hamburg - Vattenfall)
- (e.g importance of some technical issues but also on decision-making process)
- First version of the guideline obtained at the end of November 2010.
- External review

IRSN

December 2010 : Draft guideline sent to around 150 organisations all around the world with a questionnaire (with the help of CSNI=committee on the safety of nuclear installations and SARNET=severe accident research network)

Main objectives of the survey:

a. to determine as far as possible End Users satisfaction with the guidelines,
b. to determine to what extent the initial objectives of the projects have been fulfilled
c. to identify any need for a follow-up effort

24 answers to the questionnaire were received (more or less what was expected) and pre-analyzed by PSI (Switzerland). Among which answers 11 by project partners and 13 from outside the project (India, USA, Japan, Bulgaria, Lithuania, Germany, Belgium, Italy, France, Switzerland, Slovak Republic).

Specific comments were received, especially from organizations members of SARNET

ASAMPSA2 IRSN

- Thorough analysis of the survey performed by PSI.
- Three indicators have been defined and chapters scored according to these indicators.
- 2011, 7-9 March - Helsinki meeting, opened to non-participants of the project, to discuss the improvments to be done to the draft report (when possible within a short time)
- An improved version of the report is foreseen for next September although, as a consequency to Fukushima accident, work has rather been delayed since.
- Follows-up of the project still to be discussed

ASAMPSA2 IRSN

- **Draft report is composed of 3 volumes (huge volumes 1 & 2 devoted to LWR and thiner volume 3 to GEN IV reactors)**
- **Chapter division in volumes 1 & 2 according to:**
  - physical phenomena (ex : one chapter for core degradation, one for in-vessel steam-explosion etc.),
  - more specific PSA2 questions as: how to make the interface between L1 and L2 PSA, how to take into account the human factor etc.

- **PART 2 - A small part (only 6 organizations, ENEA, NRG, RSE, CEA, AREVA, IRSN and with reduced time) of the project dedicated to GEN IV reactors with two goals:**
  - To determine how far the L2PSA methodology guidelines are relevant for GenIV concepts
  - To provide a basis for new models development or extension to describe the GenIV reactors specific "mechanisms"

OUTLINE of the work performed

- **Review of the Main features of GEN IV Reactors**
  - Design Features of 4 different GEN IV Reactors
  - Degradation Mechanism and damage criteria
  - Passive safety systems
  - Calculation tools and uncertainties
  - Treatment of Hazards
- **Existing Tools for Accident Analyses**
- **Screening of the compliance with L2PSA guidelines for LWRs**
  - Compliance with LWR phenomena and systems for L2PSA
  - L2PSA Structure
  - Human reliability assessment
  - Role and extend of expert judgment
- **Conclusion and Prospect**

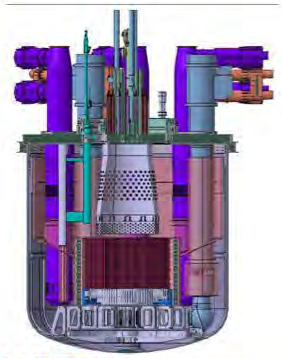
ASAMPSA2 IRSN

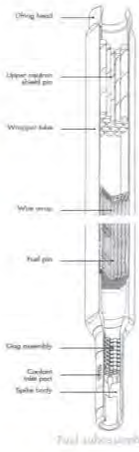
Four representative GEN IV concepts selected (choice based on data availability for project members):

- **Gas-cooled Fast Reactor (GFR)**
  - GFR project as designed end of 2007
    Developed by CEA
- **Lead -cooled Fast reactor (LFR)**
  - ELSY reactor
    Developed in the framework of the EU FP6
- **Sodium Fast Reactor (SFR)**
  - European Fast Reactor (EFR)
    Developed in the framework of a European collaboration 1988-1998
- **Very High Temperature Reactor (VHTR)**
  - ANTARES
    Commercial project designed by AREVA

ASAMPSA2 IRSN

Review of the main features of the EFR (SFR)

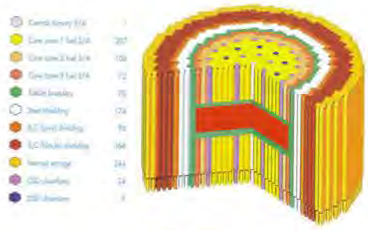




EFR: 3600 MWth

1. Fast neutron spectrum + closed fuel cycle for efficient conversion of U
2. Coolant: sodium, Tsc= 400 to 550°C
3. Pin-type core with high core power density and low coolant volume fraction
4. Pool-type reactor concept
5. Indirect Rankine thermodynamic cycle (Na filled intermediate cooling circuit and a steam-water at tertiary)

➔ thermal efficiency around 35%



Core layout

ASAMPSA2

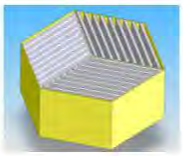
IRSN

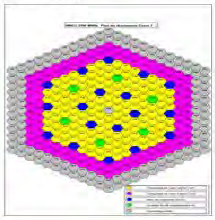
Review of the main features of the GFR

GFR: 2400 MWth

1. Fast neutron spectrum + closed fuel cycle for efficient conversion of U + management of Minor Actinides (up to 5% of MAs)
2. Coolant: helium (at 70 bar), Tsc=850°C
3. Plate-type core of (U,Pu,MAs)C + SiC coating (closing plates)
4. Combined thermodynamic cycle (indirect Brayton-cycle in the secondary circuit and indirect Rankine cycle in tertiary)

➔ thermal efficiency (45-50%).





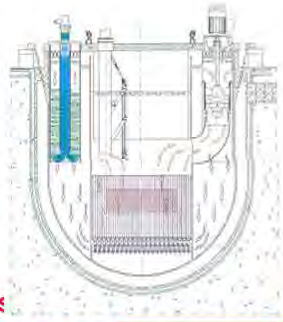
IRSN

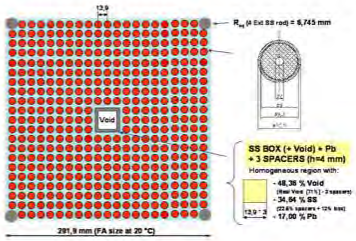
Review of the main features of ELSY (LFR)

LFR (ELSY 1500 MWth)

1. Fast neutron spectrum + closed fuel cycle for efficient conversion of U
2. Coolant: Lead (and not LB eutectics), Tsc=480°C,
3. Pool-type reactor concept and supercritical water at secondary side (240 bars, 450°C)

➔ thermal efficiency above 40%.





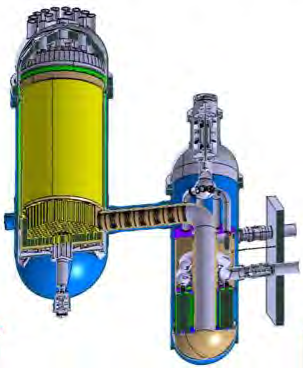
IRSN

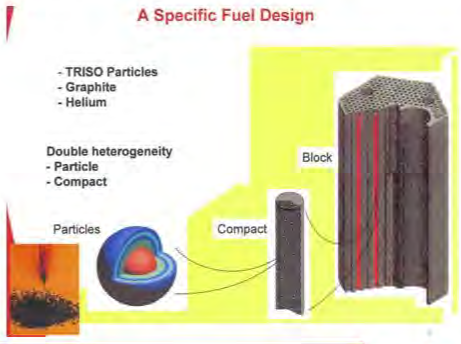
Review of the main features of ANTARES (VHTR)

ANTARES: 600MWth

1. thermal neutron spectrum (graphite as a moderator)
2. Coolant: helium, Tsc>900°C.
3. full passive decay heat removal
4. Prismatic bloc type core (UO2 fuel, TRISO coated particles).
5. Indirect Brayton cycle (i.e. gas turbine in the secondary circuit)

➔ thermal efficiency (45-50%).





IRSN

Main features of the coolant circuits (1/3)

	SFR (EFR)	GFR (CEA design)	LFR (ELSY)	VHTR (ANTARES)
Primary				
Nature of coolant	Sodium	Helium	Lead	Helium
Mass or volume of the fluid	~2500 m^3	8000 kg	$6.3*10^6$ kg	
Inertia (fluid+structure)	5 MJ/K			
Operating pressure (MPa)	0.1 (cover gas pressure)	7.0	0.1	6.0
Core inlet temperature (°C)	395	400	400	400
Mean core outlet temperature (°C)	545	850	480	850
Hottest core outlet temperature (°C)	570	900	500	

Main features of the coolant circuits (2/3)

	SFR (EFR)	GFR (CEA design)	LFR (ELSY)	VHTR (ANTARES)
Secondary				
Nature of coolant	Sodium	He/N2 (80/20 %vol) *Alternative He/Ar*	Water-superheated steam	He/N2 (80/20 %vol)
Mass or volume of the fluid	6 loops x ~200 m^3 (at 180°C)	6000 kg	25000 kg	
Operating pressure (MPa)	0.1 (cover gas pressure)	6.5	18.0	5.5
maximum temperature (°C)	525	820	450	800
Tertiary circuit (if relevant)				
Nature of coolant	Water	Water / steam	n/a	
Mass or volume of the fluid	n/a	n/a	n/a	
Operating pressure (MPa)	18.5	15.0	n/a	
Maximum temperature (°C)	490	535	n/a	550/250

Main features of the coolant circuits (3/3)

	SFR (EFR)	GFR (CEA design)	LFR (ELSY)	VHTR (ANTARES)
Decay Heat Removal secondary				
Nature of coolant	DRC : sodium DHRTV : water SGOSDHR : air	Water	Water	Water/air
Mass or volume of the fluid	6 loops ~15 m^3 / loop (for DRC)		3400 Kg (cold water storage)	
Operating pressure (MPa)	0.1	1.0	0.1	
DHR Ultimate heat sink	DRC : air DHRTV : water SGOSDHR : air	Water	water	Water/air
Passive / active DHR system	DRC : FC+NC DHRTV : NC SGOSDHR : FC	Forced Convection + NC in He / pressurized water	NC	

ASAMPSA2 IRSN

Next stage = Focussing on degradation phenomena

→Description of main degradation phenomena

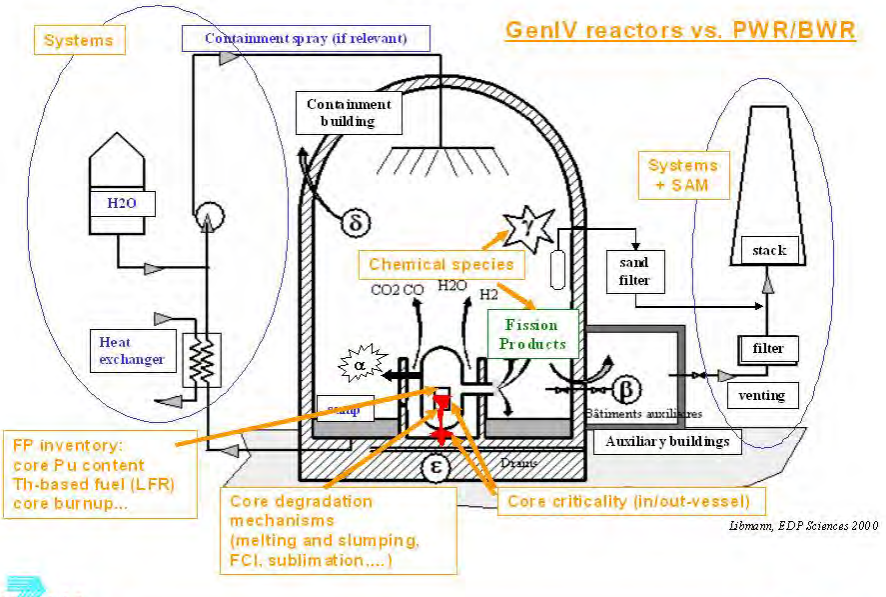
→Classification of degradation phenomena

→Collection of parameters connected with degradation

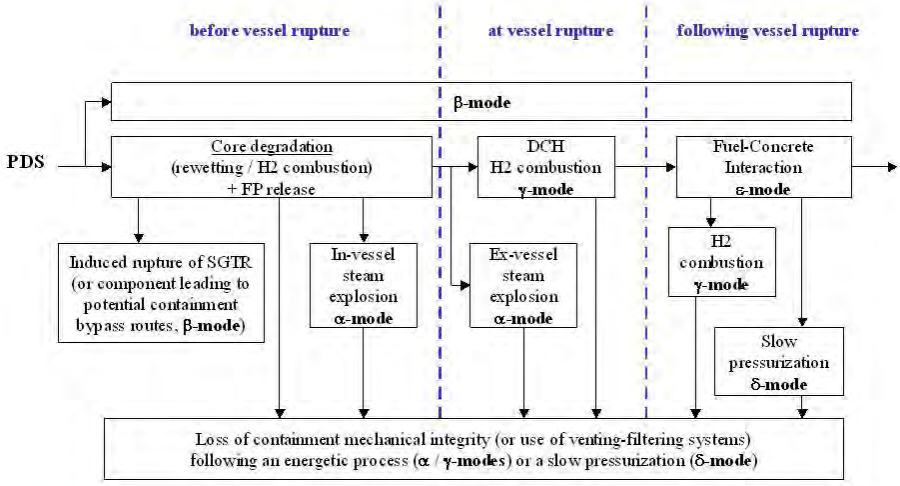
→Looking for uncertainties

ASAMPSA2 IRSN

Degradation Mechanism classification for LWR



ASAMPSA2 IRSN



ASAMPSA2 IRSN

Compliance and potential transposition of containment degradation modes

	SFR (EFR)	GFR (CEA design)	LFR (ELSY)	VHTR (ANTARES)
α-mode	Mechanical energy release in case of CDA, recriticality in case of core degradation, FCI	Energy release due to recriticality in case of core degradation	Steam explosion due to Steam Generator Tube Rupture	Dust explosion (or δ-mode ?)
β-mode	IHX, DHX tube rupture Secondary containment failure	Similar to LWRs, IS-LOCA (IHX, DHX tube rupture) combined with the containment isolation failure, HSS failure	Steam Generator Tube Rupture, Containment Isolation failure	Identical to LWRs because of the thermal loading of the IHX (failure of the isolation valves)
γ-mode	Na fire	H2 / CO emission (following steam ingress in the "carbide" core)	H2, CO/CO2 emission (following MCCI)	H2 / CO emission (following steam ingress in the graphite moderated core)
δ-mode	Na vaporization (in case of LDHR)	H2 of CO slow deflagration, failure of the guard vessel → pressurization of the Containment	Over pressurization in containment building	Dust explosion (or α-mode ?)
ε-mode	Corium / Concrete Interactions	FCI	MCCI	Not relevant

ASAMPSA2 IRSN

Collection of key parameters related to core degradation mechanisms for each concepts

- **Material inventories**
- **Material interaction at high temperature**
  - Core material behavior
  - Fuel coolant interaction
  - Interaction of core material with foreign fluids
- **Interaction between the primary fluids and others fluids**
  - SFR: Na interaction with water or air
  - LFR: No hazard
  - GFR and VHTR: not relevant
- **Key parameters for core disruptive accident**
- **Core criticality concerns**
  - Control rod(s) withdrawal
  - Coolant voiding
- **VHTR case (no gas change, low FP releases, …)**

ASAMPSA2 IRSN

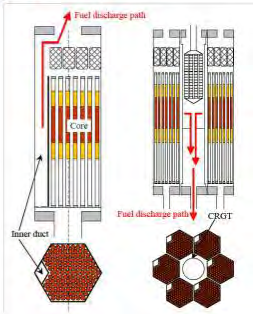
Identified needs of knowledge

- Sodium Fast Reactor (SFR)
  - Large efforts (codes, exp.) in the past and continuing
  - For CDA secondary phase, shortcomings identified
- Gas-cooled Fast Reactor (GFR)
  - Substantial lack of experiments and analysis tools
- Lead -cooled Fast reactor (LFR)
  - Known Limitations of the analysis tools: large uncertainties
- Very High Temperature Reactor (VHTR)
  - PIRT performed in US and available

ASAMPSA2 IRSN

Specific provisions for prevention and mitigation of SA

- Supplementary shutdown system
  - SFR: passive system
  - GFR: as for SFR redundant monitoring system (CR withdrawal)
  - LFR: 3 independent diverse systems
- In-core corium spreading system
  - SFR: Faidus, CRGT systems
  - LFR: Reduced risk (large pin pitch)
- Core catcher
  - EFR: in-vessel core catcher
  - GFR: ex-vessel ceramic core catcher
- Specific Containment safety features
  - SFR: liner above the roof to prevent Na-Concrete interaction
  - GFR: Vented and filtered containment + pressure relief system
  - LFR: provisions against SGTR (steam explosion)
  - VHTR: primary coolant clean-up system + RCCS (heat sink)



ASAMPSA2 IRSN

Important parameters for L2PSA source term evaluation

1. Inventory of radioactive materials in the fissile region (at EOL)
2. In-vessel radionuclide release and transport mechanisms
3. Retention and deposition of fission products inside RCS;
4. Chemical species (e.g. organic or non-organic iodine…)
   a. Iodine and caesium chemistry (Affinity of these isotopes with coolants involved);
   b. Chemistry of other isotopes (Te, Sr…): knowledge regarding phenomenological trends in presence of helium, lead or sodium;
5. Activation and corrosion products;
6. Ex-vessel radionuclide release and transport (related to containment type)
7. Aerosols behaviour inside the containment;
   a. Deposition and re-suspension of aerosols mechanisms;
   b. Effect of energetic phenomena on in-containment fission product behaviour;
   c. Activation and corrosion products of concrete surrounding the core vessel (if any) and air of its cooling system;
8. Radionuclide release outside the containment (i.e. Source Term);
9. Tritium;
10. Potential for FPs scrubbing;
11. Additional barriers or structures (e.g. close containment for GFR is not considered as confinement barrier but could lead to a potential of FPs retention)

ASAMPSA2 IRSN

Treatment of hazards

1. Internal missile,
2. Jet effects
3. Pipe whip
4. Leakage/LOCA
5. Internal flooding
6. Dropped loads
7. Internal fire
8. Asphyxiate and toxic gas release (dust)
9. Gas/chemical explosion
10. Hot and cold gas release
11. Sound, vibrations
12. Graphite dust explosion
13. Aircraft impact
14. Vehicular impact
15. Sabotage
16. Transport, industrial activities (fire, explosions, missiles, toxic & asphyxiant gases, corrosive gases)
17. Electromagnetic interference (EMI).

ASAMPSA2 IRSN

Treatment of hazards: case of V-HTR

Hazard	Risk as compared to LWR
Internal missile Jet effects Pipe whip Leakage/LOCA Internal flooding	Less
Dropped loads Internal fire Asphyxiate and toxic gas release (dust) Gas/chemical explosion	Same
Hot and cold gas release Sound, vibrations	Higher
Core / fuel chemical reactions Graphite dust explosion	Higher, HTR specific hazard
Aircraft impact Vehicular impact Sabotage Transport, industrial activities (fire, explosions, missiles, toxic & asphyxiant gases, corrosive gases) Interference with water intake and Ultimate Heat Sink EMC	Same

ASAMPSA2 IRSN

Specifics related to shutdown or refuelling states

- SFR: manufacture or loading errors: detected by instrumentation
- GFR: handling under pressure for fuel cooling
- VHTR with pebble bed: continuous refuelling

Existing L2PSA for Gen IV

- Sodium Fast Reactor (SFR)
  - SNR-300
  - US PRISM
  - JSFR
- Gas-cooled Fast Reactor (GFR): no
- Lead -cooled Fast reactor (LFR):No
- Very High Temperature Reactor (V-HTR))
  - HTGR of General Atomics
  - HTR-1160 (Germany)
  - MHTGR (US)
  - PBMR (South Africa)

ASAMPSA2 IRSN

List of codes given for describing:

1. Core damage progression (initiating phase, transition phase, core disruption for FRs; slow core heat-up for VHTR)
2. Failure modes of the RCS (dynamic thermal-mechanical calculations and tools / assessment of conditional probabilities regarding the missile emission potentially challenging the containment integrity)
3. Failure modes of the containment (dynamic thermal-mechanical calculations and tool)
4. MCCI
5. Source term assessment (FPs release from the core, transportation & deposition in RCS, in retention tanks and transfer to the environment).

ASAMPSA2 IRSN

Compliance with LWR phenomena and systems (1=HC-5=LC)

Sections	*Subsections*	*Items*	SFR	GFR	LFR	V-HTR
Quantification of physical phenomena and containment loading	Definition and calculation of representative thermal-hydraulics sequences for each PDS		5	5		3
	In-vessel core degradation	a - Core degradation	5	4	3	5
		b - Induced-RCS rupture including induced-SGTR	5	3	4	5
		c - Hydrogen production	5	5	5	3
		d - Restoration of core-cooling	5	5	4	5
		e - Vessel cooling from outside	5	5	3	5
		d - Consequences of in-vessel water injection (coolability, hydrogen production, RCS pressurization ...)	5	5	5	5
		e - Containment atmosphere composition (recombiners/igniter effect) and containment pressurization	5	5	5	3
		f - Containment venting	2	2	1	3
		g - Hydrogen distribution/combustion	5			4
		h - Corium criticality	5	5	5	4
		i - In-vessel steam explosi on and consequences (leak in the RCS, vessel rupture, containment rupture)	3	5	5	4
		j - Vessel rupture (delay, break size ...)	3	3	3	5
	Vessel rupture phase	a - Direct Containment Heating, including H2 combustion and vessel uplift	5	5	2	5
		b - Ex-vessel steam explosion	5	5	2	5
		c - Corium criticality	5	5	2	5
	Ex-vessel phase (MCCI)	a - Corium coolability	3	3	2	5
		b - Basemat lateral and axial erosion	5	1	1	5
		c - Impact of water injection	5	5	2	5
		d - Production of steam and incondensable gases	4	5	2	5
		e - H2/CO combustion	5	3	1	3
		f - Evolution of containment atmosphere composition and long term pressurization	2	2	1	3
		g - Containment venting	2	2	1	3
		i - pool scrubbing		5		5
		h - Melt propagation into ducts and channels	5			5
Containment performance (tightness)	Initial containment performance (pre-existing leakage)		1	1	1	
	Failure of the isolation system		1	1	1	
	Evaluation of containment performance in severe accident conditions	a - Quasi- static loading / dynamic loading – Structural response, structural analyses, fragility curve (leak or	4	1	1	
		b - Specific issues : example the impact of a steam explosion in the vessel pit on the overall structure	5		2	
		c - drywell/supression pool performance			5	
	Containment penetrations performance (tightness) in severe accident conditions		2	2	1	
	Identification of specific containment bypass ways (example: case of existing pipes in the plant foundations, cavity door failure for VVER)		2		1	
Systems behaviour in severe accident conditions	Sump recirculation, CHRS, Spray system		5	5	5	5
	RCS safety valves		3	2	5	3
	Steam Generator		5	5	1	3
	Instrumentation		5	3	1	2
	Pedestall cavity flooding systems		5	5	5	5
	H2 recombiners/igniters		5		2	5
	Core catcher		3	3	5	5
	Reliability of passive systems		1	1	1	2
Source term assessment	Definition of release categories	a – identification of key parameters for source term assessment	2	2	1	3
		b – example of release categories		1	1	2
		c - screening frequency		1	1	2
	Group of fission products		3	1	1	2
	Source term assessment by integral codes		2	2	1	2
	Source term assessment by dedicated (fast-running) source term models				1	2
	Radiological consequences		1	1	1	2

ASAMPSA2 IRSN

Level 2 PSA Structure

- **Common adopted approach for L2 (performed after L1PSA)**
  - Definition of the initial conditions by binning of L1PSA end states into Plant Damage States (PDS);
  - Development, construction and quantification of event trees: Containment Event Trees (CET, i.e. small event trees) or Accident Progression Event Trees (APET, i.e. large event trees);
  - Definition of source term categories or release categories;
  - Binning of containment states related to specific containment failure modes
- **L1-L2 interface parameters**
  - The 2nd barrier integrity (e.g. intact RCS vs. LOCA) Primary pressure during core meltdown;
  - The core power (i.e. time after IE) at core damage onset;
  - The status of safety systems linked to the RCS;
  - The availability of power supplies (external, internal, AC and DC);
  - The integrity of the containment (intact/failed through isolation failure, bypass through heat exchangers or IS-LOCA);
  - The availability of containment protection systems (if any).

ASAMPSA2 IRSN

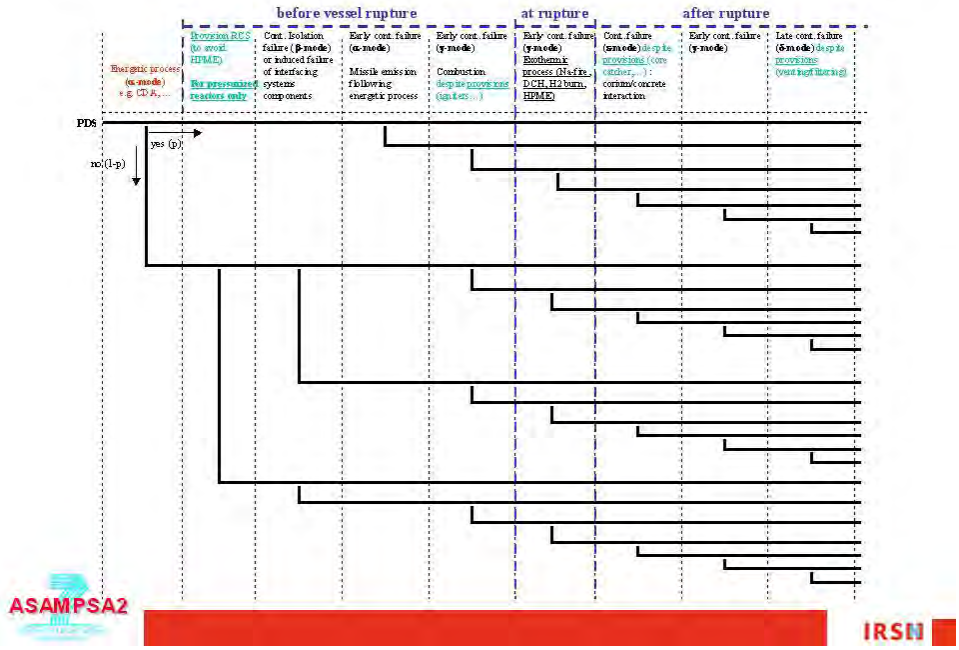
Level 2 PSA Structure: APEC/CET

- GEN IV arising questions
  - The general structure of APET/CET assuming that time phases (i.e. before reactor vessel failure, at failure, and after) could be consistent if the vessel rupture "notion" (i.e. bottom head rupture in LWRs) is extended to the loss of integrity of the second barrier (e.g. cross-duct rupture for GFR and VHTR, rupture of the roof in SFR and LFR); then no major difference regarding time phases is expected.
  - The most important phenomena that should be considered for APET/CET building.
  - Mission time of system and definition of the reactor final state.
  - Common Cause Failures (containment penetrations and isolating devices).
  - Use of cut-off frequency (if any), compliance with the cut-off frequency of PWR/BWR.
  - Extend of feedback regarding the Generation IV reactors (data, level 2 PSA technical feedback…).

  Tentative ET for GEN IV reactors
  - SFR: small event tree (only the action of isolation of containment, the reliability of the corium coolability, and the criticity risk $\neq$ LWRs will be modelled)
  - LFR: No CDA; SGTR may lead to α (steam explosion), γ (H2) and ε (MCCI) modes
  - VHTR: example of event tree for the typical accident (loss of He flow) already available

ASAMPSA2 IRSN

Generic Event Tree related to containment degradation modes



Screening compliance (continued)

- **Human reliability asssessment**
  - For GEN IV no mitigation measures and procedures defined
- **Quantification of physical phenomena and uncertainties**
  - Sources of uncertainties:
    - **Parameters (data) uncertainties;**
    - **Model uncertainties**
    - **Model Completeness**
- **Passive safety systems**
  - Passive system used in a greater extend than with LWRs
  - Failure assessment of passive system is complex (will a natural circulation establish or not ? etc.)
- **Calculation tools and uncertainties**
- **Role and extend of expert judgment**
  - More important / LWRs due to limited experience

Compliance level with GenII/III L2PSA model building (from 1 to 5 : 1 = potentially highly compliant, 5 = not compliant)

Sections	Subsections	Items	SFR	GFR	LFR	V-HTR
L1-L2 PSA interface				2	1	
Accident Progression Event Tree (APET)			5	2	1	
Release Categories and result presentation			2	2	1	
L1-L2 interface			1	1	1	
Human Factors		Examples of human actions (from severe accident management guide, support of crisis organization, systems recovery ...)	3	3	2	3
		Methods for the human factor quantification	4	3	1	3
APET-CET			2	2	1	3
List of plant data that should be available for the L2 PSA			4	5	1	
Severe accidents codes			5	5	1	
Event trees codes			1	1	1	1

Conclusions (1/3)

- **GEN IV technology roadmap:**
  - "the design detail must allow use of simplified Probabilistic Risk Assessment (PRA) to identify design basis accidents and transients as well as the highly hypothetical sequences. The detail should be sufficient to identify and rank phenomena of importance to transient response and to specify experimental information required to validate transient models". In addition, it was recalled that "Generation IV nuclear energy systems will eliminate the need for offsite emergency response"
- **Issues to be addressed (end-users requirements)**
  - the determination of LERF (Large Early Release Frequency/LRF;
  - the identification of main containment failure modes and the related assessment of releases;
  - the plant vulnerabilities insights in Accident Progression and assessment of containment performance;
  - the insights to plant specific risk reduction option;
  - and finally, the insights to Severe Accident Management Guidelines (SAMG)

ASAMPSA2 IRSN

Conclusions (2/3)

- **L2PSA may be performed at the early stage of design will give insights on:**
  - The identification of major containment failure modes and on how severe accident progress;
  - A rough estimation of the quantities of released radioactive material to the environment for different accident sequences;
  - The identification of particular important phenomena and processes, and especially those who are of importance for containment performance (i.e. the last barrier in order to avoid massive and long-term population displacement following an accident);
  - A useful help for the prioritization of R&D activities
- **Main differences of GEN IV reactors compared to LWRs**
  - Neutron Fast spectrum: Core Disruptive Accidents
  - Pu and Minor Actinide Inventories
  - Fire concerns (Na, graphite): have an impact on FP and chemical releases

ASAMPSA2 IRSN

Conclusions (3/3) and perspectives

- **Too Early to perform study of compliance of LWR L2PSA guidelines to Gen IV reactors:**
  - GEN IV reactor still under design
  - No Emergency Operating Procedures (EOP) and Severe Accident Management Guidelines
  - Needs of probabilistics models
- **but**
  - Core damage prevention can be done (by design)

And later EOP will be defined to mitigate the consequences of severe accidents

ASAMPSA2 IRSN

Thank you for your attention

Thanks to the ASAMPSA2 project partners and specially to F. Serre (CEA) for his help preparing this presentation.

ASAMPSA2 IRSN

Reliability analysis of 2400 MWth gas-cooled fast reactor natural circulation decay heat removal system

M. Marquès[1], C. Bassi[1] and F. Bentivoglio[2]
[1] CEA, DEN, SESI, F-13108 Saint-Paul-lez-Durance, France, michel.marques@cea.fr
[2] CEA, DEN, SSTH, F-38054 Grenoble, France, fabrice.bentivoglio@cea.fr

Abstract

In support to a PSA performed at the design level on the 2400 MWth Gas-cooled Fast Reactor, the functional reliability of the decay heat removal system working in natural circulation has been estimated in two transient situations corresponding to an "aggravated" Loss of Flow Accident (LOFA) and a Loss of Coolant Accident (LOCA). The reliability analysis was based on the RMPS methodology. Reliability and global sensitivity analyses use uncertainty propagation by Monte Carlo techniques. The results obtained on the reliability of the DHR system and on the most important input parameters are very different from one scenario to the other showing the necessity for the PSA to perform specific reliability analysis of the passive system for each considered scenario. The analysis shows that the DHR system working in natural circulation is a very reliable system in case of LOFA situations even when only one DHR loop is available. On the other hand, its reliability has to be improved in LOCA situations. This analysis shows the way to make this improvement in specifying the main uncertainties, which could to be reduced.

Keywords: Gas-cooled fast reactor, passive system, natural circulation, reliability

.

1. Introduction

Probability Safety Assessment (PSA) of nuclear power plants has demonstrated its efficiency in decision-making process. The interest of a PSA on a reactor equipped with safety passive systems is in analysing if these systems improve reactor safety and if yes, in determining the design limits and operating conditions to be respected. But the treatment in PSA of safety passive systems, specially those implementing moving working fluid (category B passive systems), is a difficult task because in addition to the mechanical failures of its components (hardware failure), the failure of the system in achieving its intended design function, referred as functional failure (Burgazzi 2002) has to be considered. The difficulty in the evaluation of this type of failure risk lies in the great number of parameters that must be taken into account, in their associated uncertainties and in the limitations of physical modelling. A PSA has been developed by CEA (Bassi 2010, Balmain 2011) to support the design of the 2400 MWth Gas-cooled Fast Reactor (GFR). We present in this paper the functional reliability analysis carried out for the passive decay heat removal system (DHR) of the GFR, in support to this PSA. The reliability of the DHR system has been studied in two accidental situations. For these two situations, we have considered that all the active features cannot operate and that the only way is completely passive using natural circulation. The thermal-hydraulic calculations have been performed with the CATHARE2 code (Messié 2007, Bentivoglio 2007). Various failure criteria, different for each scenario, have been considered. The reliability analysis is based on the RMPS methodology (Marquès 2005). Reliability and global sensitivity analyses use uncertainty propagation by Monte Carlo techniques. The function of DHR system is described in Section 2; the two scenarios are presented in Section 3, the failure criteria in Section 4 and CATHARE modeling in Section 5; identification and quantification of uncertainties and their propagation are described respectively in Section 6 and 7; estimations of failure probabilities for each scenario is presented in Section 8; global sensitivity analysis is described in Section 9 and conclusion is given in Section 10.

2. DHR system description and function

The DHR system (Figure 1a) consists of 1) three dedicated DHR loops: the choice of three loops (3x100% redundancy) is made in assuming that one could be lost due to the accident initiating event (break for example) and that another one must be supposed unavailable (single failure criterion); 2) a metallic guard containment enclosing the primary system (referred as close containment), not pressurized in normal operation, having a free volume such as the fast primary helium expansion gives an equilibrium pressure of 1.0 MPa, in the first part of the transient (few hours). Each dedicated DHR loop (Figure 1b), designed to work in forced circulation with blowers or in natural circulation (NC), is composed of 1) a primary loop (cross-duct connected to the core vessel), with a driving height of 10 meters between core and DHX mid-plan; 2) a secondary circuit filled with pressurized water at 1.0 MPa (driving height of 5 meters for natural circulation DHR); 3) a ternary pool, initially at 50°C, whose volume is determined to handle one day heat extraction (after this time delay, additional measures are foreseen to fill up the pool).

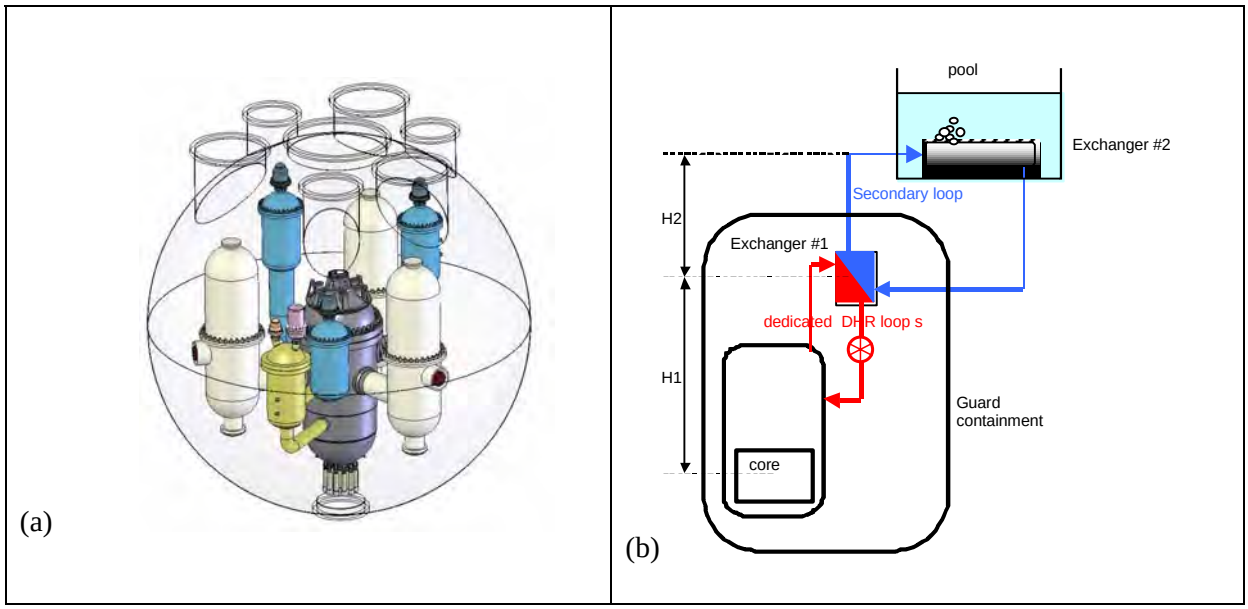
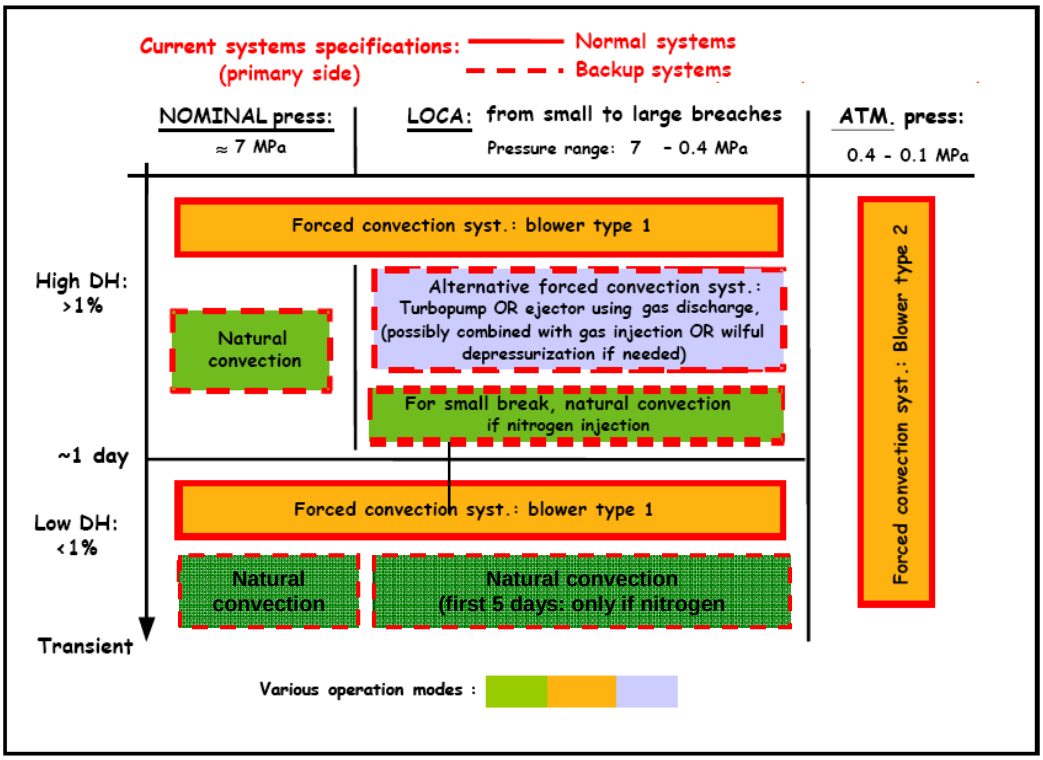


Figure 1: a) view of the primary circuit (DHR loops in blue) and the close containment. b) scheme of a DHR loop.

The design specifications of the DHR system have been proposed (Malo 2007) according to a strategy presented in the figure 2: the selected combination of systems is shown, considering the two main accidental situations families with maintenance of the primary pressure near to the nominal pressure (LOFA, etc.) and with a backup pressure resulting from a LOCA. In addition, the situation related to a primary pressure reaching 0.1 MPa (corresponding to a combination of LOCA and a leak of the close containment) has been addressed. According to this strategy, the Natural Circulation (NC) of gas, through the DHR system is foreseen: 1) for pressurized situations (i.e. with intact helium pressure boundary), 2) for depressurized situations (i.e. with non-intact helium pressure boundary) with the supply of the dedicated nitrogen-filled tanks discharge. For the later, owing to the poor NC capability of gaseous coolant, a back-up pressure level is provided thanks to the close-containment.



- **Figure 2. Schematic of the first reference DHR strategy based on mixed natural and forced convection systems.**

3. Scenarios selected for NCDHR reliability evaluation

Two transient scenarios are selected to be representative of the situations of interest regarding the natural circulation DHR process for the GFR:

1) A Station Black-Out (SBO) initiating event, i.e.: loss Of Station service Power (LOSP) cumulated with all Emergency Diesel Generators failure to start; with only one DHR loop available. This "aggravated" LOFA transient is considered as an envelope case of the pressurized situations despite its very low occurrence frequency.

2) A 3 inches diameter LOCA initiating event (maximum bounding size of Small-Break LOCA), located on the cold part of a main cross-duct, representative of depressurized situations; with a total loss of forced circulation DHR means (DHR blowers fail to start by example), with two DHR loops available and with nitrogen injection from the N_2-filled tanks in order to ensure a sufficient back-up pressure level (primary circuit linked to the close containment).

The sequences of events corresponding to the two scenarios are depicted in Figure 3. For the first scenario, scram is performed at initiating event; for the second scenario, scram is performed when the close containment pressure becomes higher than 130% of its nominal value (it is the way selected to detect the leak due to the 3 inches breach). For both scenarios, the main blowers are stopped at scram; then there is a phase of reduced velocity of the blowers, which continue to run on their inertia. When the helium mass flow rate at core inlet becomes less than 3% of nominal one a sequence starts with the isolation of the main loops and the connection of the DHR circuits. In the second transient, the nitrogen injection from the three accumulators starts when the lower plenum pressure becomes lower than 1 MPa (initial pressure is close to 7 MPa).

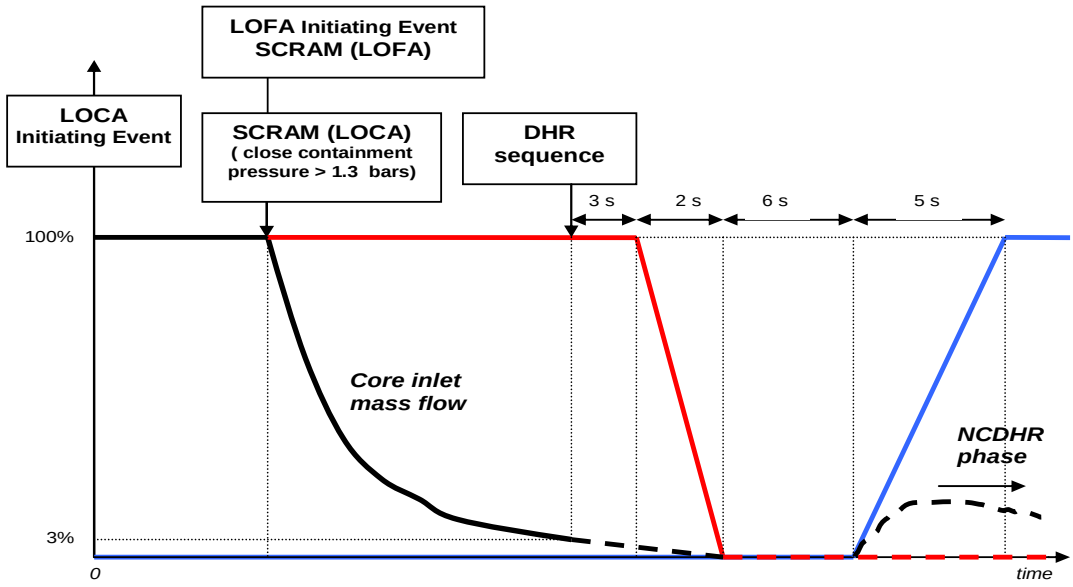


Figure 3: Transient event sequences defined for LOFA and LOCA scenarios.

4. Failure criteria

The two scenarios belong to category 4 situations (frequency ranging from 10^{-6} to 10^{-4}) for which the preliminary acceptance criteria are given in Table 1. These maximal temperatures and pressure have been defined to insure a margin up to the physical integrity of the components considered (clad, core upper structures, DHR loop structures and close containment).

Criterion	LOFA transient	LOCA transient
DHR loop structural integrity Maximum temperature of DHR structural material (stainless steel)	850 °C	850 °C
Coolability and core integrity Maximum clad (SiC coating) temperature	1600°C	1600 °C
Core upper structures integrity Maximum temperature of gas at core outlet (hot channel outlet)	1250°C	1250 °C
Nitriding and exothermic reactions Maximum clad temperature	-	1000 °C
Close containment integrity Maximum pressure in the close containment	-	1.4 MPa

Table 1: Failure criteria for transients 1 and 2

5. Modelling

The calculations have been performed with the CATHARE2 code. In addition to the circuits represented in the figure 4, a large free volume used to describe the spherical close containment and three nitrogen accumulators (540 m3, 7.5 MPa) have been modeled in the second scenario. The

transient calculations has been performed over 7100s for transient 1 and over 21600s (6 hours) for transient 2.

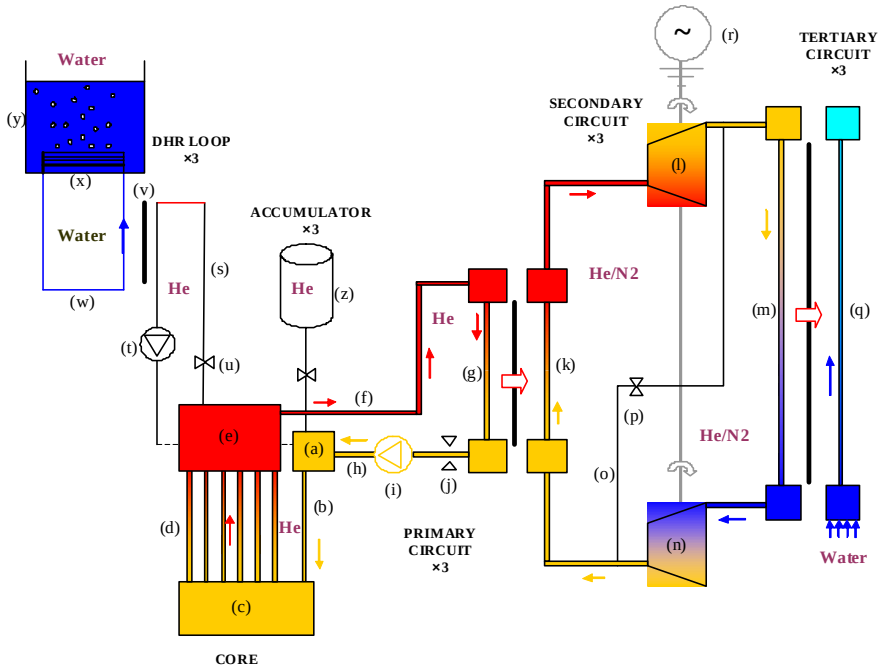


Figure 4: Schematic drawing of the GFR CATHARE modelling. (a) Volcold, (b) Downcomer, (c) Lowerplenum, (d) Core, (e) Upperplenum, (f) Hotduct, (g) IHX primary side, (h) Colduct, (i) primary blower, (j) primary isolating valve, (i) accumulators, (k) IHX secondary side, (l) Turbine, (m) GV gas side, (n) Compressor, (o) Bypass line, (p) Bypass valve, (q) GV water side, (r) generator, (s) DHR primary loop, (t) DHR blower, (u) DHR isolating valve, (v) DHR primary heat exchanger, (w) DHR secondary loop, (x) DHR secondary heat exchanger, (y) DHR water pool, (z) Helium accumulators.

5.1 Reference results on scenario 1 (LOFA)

The reference calculation, with nominal values of the input parameters, has shown that only one DHR loop working in natural circulation fulfills perfectly its mission. A stable flow-rate of about 30 kg/s is quickly (in less than 100 s) established in the DHR loop and is maintained up to the end of the transient during the natural circulation phase. During two hours (time considered in the study) from the beginning of the transient, the heat removal is sufficient and all failure criteria are respected, with values staying well below the safety limits. A maximum of clad temperature (criterion 2) equal to 1054°C is obtained at 195s, after the sequence involving isolation of the main loops and connection of the DHR circuits (Figure 5a). The maximum of gas temperature (criterion 3) is equal to 1034°C.

5.2 Reference results on scenario 2 (LOCA)

The reference calculation, with nominal values of the input parameters, has shown that two DHR loops working in natural circulation fulfill their mission with the help of nitrogen injection from accumulators. After nitrogen injection, a flow-rate of at least 50 kg/s is maintained up to the end of the transient during the natural circulation phase. During six hour from the beginning of the transient, the heat removal is sufficient and all failure criteria are respected, with values staying below the safety limits: a Peak Clad Temperature (PCT) (criterion 2) equal to 1404°C at first peak is obtained at 624s and a second peak (criterion 4) equal to 840°C is observed at 6206s after nitrogen injection (Figure 5b), the maximum of gas temperature (criterion 3) is equal to 1241°C; however the margin is only 9°C for this third criterion.

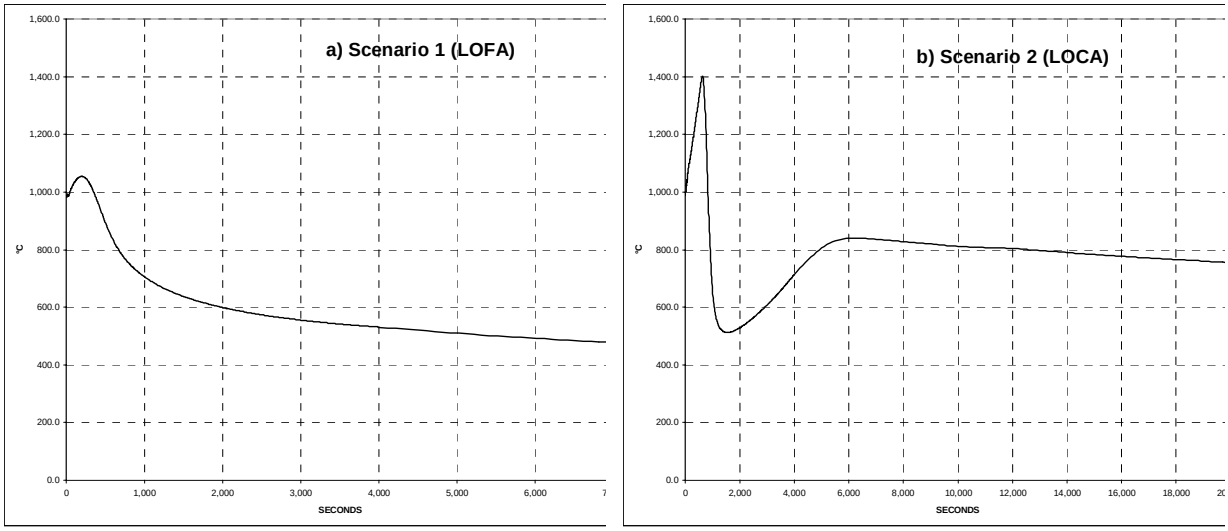


Figure 5: Clad temperatures in the central channel of the core

6. Identification and quantification of uncertainies

In order to identify the main sources of uncertainties in the estimation of the quantities associated with the failure criteria, sensitivity analyses have been performed for a number of input parameters in the CATHARE2 calculations. Classical *OAT (One-at-A-Time)* analysis, which varies one factor from the nominal condition, the others being kept at theirs nominal values, has been used for this sensitivity analysis.

6.1 Scenario 1 (LOFA)

Among the 24 parameters studied (Table 2), very few have a significant influence on the transient, in the area investigated. The major effect is produced by the additional singular pressure drop coefficient of 674 (estimated by CFD analysis), which simulates the stopped DHR blower. In this case, the increase of clad and helium maximal temperatures in the core reaches 600°C over the reference case and the third criteria (maximal temperature of gas) is greatly exceeded (by 400°C). The primary blower inertia has a noticeable effect on the transient sequence and on the whole system parameters. Initial power, delay between primary valves closure and DHR valves opening and wall inertia are others parameters of influence. All remaining parameters have a very limited impact on the transient. Especially uncertainties on materials properties play a very limited role. For the next reliability analysis phase, the ten most relevant uncertain input parameters have been selected (in bold in Table 2); these selected parameters are supposed to follow uniform distributions. The singular pressure drop due to the stopped blower will not be taken into account, considering that a by-pass will be installed and that, in this case, the uncertainty on this parameter will not have a significant effect; in the PSA analysis, however the reliability of this by-pass will have to be considered.

6.2 Scenario 2 (LOCA)

The effects of 27 input parameters on the four responses of interest (1st PCT, 2nd PCT, maximum temperature of gas at core outlet and maximum pressure in the close containment) have been studied independently. Table 3 gives the list of these 27 parameters with their range of variation. In all the *OAT* cases, the clad temperature criteria are satisfied, but the criterion on the gas maximal temperature is exceeded several time and the criterion on the close containment maximal pressure one time. Table 4 presents the OAT cases of the parameters giving exceedance of the failure criteria; these parameters have been chosen for the reliability analysis and they have been modeled by normal distributions. Note that the effects of some parameters (i.e. pressure for accumulator discharge, helium-clad heat transfer coefficient…) on the first and on the second peak of clad temperature are contradictory, generally because an early nitrogen injection limits the first peak but is unfavorable for the second, the nitrogen

accumulators being empty earlier. This gives a glimpse of the difficulties in the design of the reactor in finding an optimum for these parameters.

N°	Parameter	Selected N°	Reference	Min value	Max value
1	Secondary DHR loop pressure (MPa)		1	0.7	1.3
2	**Plate-type core laminar pressure drop coefficient**	**1**	1	0.85	1.15
3	Singular pressure drop coef. for DHR stopped blower		1	-	674
4	Natural leakage from primary circuits to containment (kg/s)		0	-	0.02
5	Singular pressure drop coefficients for core channels		K	K*0.9	-
6	**Singular pressure drop coefficient at DHR IHX inlet**	**2**	1	-	10
7	**Singular pressure drop coefficient at DHR IHX outlet**	**3**	1	-	10
8	DHR pool temperature (°C)		50	42.5	57.5
9	**Helium-clad heat transfer multiplicative factor**	**4**	1	0.95	1.05
10	**Multiplicative factor for all wall thermal inertia**	**5**	1	0.85	1.15
11	**Corrective factor for HT in DHR IHX**	**6**	1	0.9	1.1
12	Corrective factor for HT in DHR pool		1	0.5	1.5
13	Delay between main loop closure and DHR loop opening		6	-	26
14	Core flow rate threshold for primary valve closure		3% Q_{nom}	2.5% Q_{nom}	3.5% Q_{nom}
15	**Core nominal power**	**7**	Pnom	0.98 Pnom	1.02 Pnom
16	**Core residual power**	**8**	Pres	0.9 Pres	1.1 Pres
17	**Primary blowers inertia**	**9**	Iref	0.75 Iref	1.25 Iref
18	**Main circuit pressure (MPa)**	**10**	P_{main}	0.8 P_{main}	1.2 Pmain
19	Heat exchange coef. for DHR cross-duct insulation (W/m/K)		0.6	0.1	10
20	Homogenized fuel specific heat capacity		$\rho.Cp_{FUEL}$ = f(T)	-10%	+10%
21	Homogenized fuel thermal conductivity		λ_{FUEL} = f(T)	-10%	+10%
22	Helium specific heat (J/kg/K)		5193	-10%	+10%
23	Helium thermal conductivity		λ_{HE} = f(T)	-10%	+10%
24	Helium dynamic viscosity		μ_{HE} = f(T)	-10%	+10%

Table 2: Parameters studied for scenario 1 (LOFA)

N°	Parameter	Selected N°	Reference	Min value	Max value
1	Core total pressure drop		1	-15 %	+15%
2	Inlet k-factor in DHR primary loop		1	0	2
3	Outlet k-factor in DHR primary loop		1	0	2
4	**Helium clad heat transfer coefficient**	**1**	K	-25%	+25%
5	Multiplication factor for thermal inertia for all walls		1	-15 %	+15%
6	**Corrective factor for heat transfer in DHR IHX**	**2**		-25%	+25%
7	**Core nominal power**	**3**	Pnom	-2%	+2%
8	**Core residual power**	**4**	Pres	-10%	+10%
9	**Primary blower inertia**	**5**		-25%	+25%
10	Main circuit pressure (MPa)			-0.2	0.2
11	**SCRAM actuation ($P_{containment}$ in bar)**	**6**	1.3	1	2
12	**Accumulators discharge (Primary pressure in bar)**	**7**	10	8	12
13	Delay between main loop isolation and DHR conection (s)		6	4	10
14	Gas mixture viscosity		Wilke law	-5%	+ 5%
15	**Gas mixture conductivity**	**8**	Mason & Saxena law	- 10%	+ 10%
16	**Gas mixture heat capacity**	**9**		-5%	+5%
17	Close containment leakages (kg/s)		$2\ 10^{-4}$	-	+10%
18	**Close containment free volume (m^3)**	**10**	11620	-10%	+10%
19	Close cont. heat exchange with the outside ($w/m^2/K$)		15	-10%	+10%
20	Close containment outside temperature (°C)		20	10	30
21	Close containment initial temperature		50	30	70
22	Volume of heat structures in close containment (m^3)		1574	-10%	+10%
23	Closed containment initial pressure (bar)		1	-10%	+10%
24	Accumulators initial pressure (bar)		75	70	80
25	Accumulators initial temperature (°C)		50	30	70
26	Discharge line singular pressure drop		15	-50%	+50%
27	Break size (inches)		3	-10%	+10%

Table 3 : Parameters studied for scenario 2 (LOCA)

7. Propagation of uncertainties through thermal hydraulic models

For each scenario, Latin Hypercube Sampling (LHS) has been performed using the 10 respective input parameters with their corresponding distributions. 1000 samples of the input parameters were simulated for the first scenario and 100 samples for the second and for each sample a thermal-hydraulic calculation was performed with the CATHARE2 code. For the scenario 1, response surfaces were calculated: the process carried out by the thermal-hydraulic code is approximated by a simple mathematical function in the region of interest. First order linear response surfaces are constructed for all the three quantities of interest; they are given by:

$$\mathbf{Y = \beta_0 + \sum_{i=1}^{p} \beta_i X_i} \quad \mathbf{(1)}$$

with Y the response and X_i the input parameters. The quality of the fitness of the assumed model, in comparison with the actual code response, is given by the coefficient of determination R^2.

N°	Parameter	Modification	1st PCT (°C)	2nd PCT (°C)	He max T (°C) at core outlet	Close containment max P (bars)
Failure criteria			**1600**	**1000**	**1250**	**14.000**
Reference case			1404.4	842.2	1243.3	13.332
1	**Helium clad heat transfer coefficient**	- 25 %	1377.9	851.2	1219.6	13.330
		+ 25 %	1417.7	836.9	**1253.0**	13.331
2	**Corrective factor for heat transfer in DHR IHX**	- 25 %	1428.3	926.9	**1263.8**	13.514
		+ 25 %	1385.3	792.8	1226.1	13.215
3	**Core nominal power**	- 2 %	1378.7	825.9	1222.7	13.325
		+ 2 %	1426.5	858.8	**1260.8**	13.338
4	**Core residual power**	- 10 %	1327.7	761.0	1184.1	13.287
		+ 10 %	1472.3	921.8	**1292.4**	13.371
5	**Primary blower inertia**	- 25 %	1457.6	844.1	**1284.9**	13.312
		+ 25 %	1359.3	840.6	1206.4	13.351
6	**SCRAM actuation ($P_{containment}$)**	- 0.03 MPa	1386.1	842.2	1227.0	13.320
		+ 0.07 MPa	1452.7	842.6	**1282.8**	13.350
7	**Accumulators discharge (Primary pressure)**	- 0.2 MPa	1460.7	839.9	**1292.5**	13.337
		+ 0.2 MPa	1356.1	844.3	1195.7	13.328
8	**Gas mixture conductivity**	- 10 %	1416.6	859.1	**1253.0**	13.418
		+ 10 %	1392.7	828.2	1232.8	13.261
9	**Gas mixture heat capacity**	- 5 %	1429.4	871.0	**1269.4**	13.396
		+ 5 %	1377.4	816.1	1215.7	13.281
10	**Close containment free volume**	- 10 %	1400.5	799.4	1239.5	**14.367**
		+ 10 %	1406.1	885.2	1244.5	12.450

Table 4 : Parameters of scenario 2 (LOCA) giving exceedance (in bold) of the failure criteria

8. Failure probabilities

8.1 Scenario 1 (LOFA)

None of the cases among the 1000 simulations met the failure criteria: maximum clad temperature never exceeds 1600°C and maximum gas temperature at core outlet never exceeds 1250°C. The estimate of the probability of failure should be $p_f = m/N$, where m is the number of code runs which met the failure criterion and N = total number of code runs but in this case, p_f takes the value zero since no code run provides an output observable within the failure domain. This result illustrates a limitation of Monte Carlo simulation: the complexity of the physical problem to solve involves large computational time on each run and enables only a limited number of simulation, which are not enough for achieving a proper estimation of failure probability. Wilks' formula for one sided tolerance interval can be used for calculating a conservative upper bound γ of the actual probability of failure p_f : $1 - (1-\gamma)^N \geq \beta$, where β expresses the "confidence" that p_f will be lower or equal than γ. Considering β = 0.95 and N = 1000, it is obtained γ = 0.003. This constitutes however a very high upper bound for the failure probability, according to the margins that we obtain on the two failure criteria.

Reliability analysis using the regression model

These reliability analysis concerns the failure criterion on the maximum helium temperature at core outlet for which we have the less margin. Considering the linear relation between the maximum helium temperature and the input parameters (R^2 = 0.994), we will use this linear model instead of the CATHARE2 code to study the effect of changing the range of the input parameters uncertainties on the failure probability. The regression model is the following:

Max Helium T = 1022.6 + V_1 * 3.0972 + V_2 * 0.5621 + V_4 * 58.772 + V_5 * -203.18 + V_6 * -40.26 + V_7 * 738.8 + V_8 * 259 + V_9 * -287.14 + V_{10} * -21.541 (V_i the input parameters with the subscript *i=1 to 10* corresponding to column *Selected N°* in Table 3)

Performing various numbers of simulations (up to 10^7) with this linear model and keeping the initial probabilistic model, the maximal value obtained is 67°C below the failure criteria. We have performed several modifications of the initial probabilistic model in order to test the influence of these changes on the failure probability. Table 5 shows the various modifications in the probabilistic model and the corresponding failure probabilities and maximal helium temperatures. We obtain in this way rough estimations of the failure probability of the DHR system in case of transient 1 occurrence. Even in doubling the range of variation of the most important variables (blower inertia or wall thermal inertia), the failure probability obtained keeps very small. The same is observed in increasing the ranges of variation of all the input parameters by 50%. In order to obtain a relatively significant failure probability (~10^{-4}) , it is necessary to double the range of variation of the two most important variables simultaneously or to increase the ranges of all the parameters by 70%. In the PSA, the functional failure probability of the natural circulation DHR in pressurized situations has been upper-bounded by 5×10^{-6} and this result is implemented as basic event in the PSA model (Bassi 2008, Bassi 2010). However studies should be sustained to evaluate the pressure drop caused by the stopped blower and to assess the need to bypass it in situations of natural circulation.

Modification in the initial probabilistic model	**Failure probability *Pf***	**COV of *Pf***	**Max Helium T (°C)**
V9 (blower inertia) : [-50% , 50%]	7.2 10^{-7}	0.12	1256
V5 (wall thermal inertia) : [-30% , 30%]	*No failure case*	-	1209
V9 (blower inertia) : [-50% , 50%] and V5 (wall thermal inertia) : [-30% , 30%]	2.71 10^{-4}	0.06	1277
Uncertainty range of all variables * 1.1	*No failure case*	-	1197
Uncertainty range of all variables * 1.2	*No failure case*	-	1212
Uncertainty range of all variables * 1.3	*No failure case*	-	1229
Uncertainty range of all variables * 1.4	*No failure case*	-	1247
Uncertainty range of all variables * 1.5	3.5 10^{-6}	0.17	1263
Uncertainty range of all variables * 1.6	5.7 10^{-5}	0.13	1276
Uncertainty range of all variables * 1.7	3.2 10^{-4}	0.06	1292

Table 5: Effect of modifications of the probabilistic model on the failure probability

8.2 Scenario 2 (LOCA)

For each simulation performed, the natural circulation DHR system is considered failed if at least one of the four failure criteria is exceeded, i.e.:

$T_{max\_clad\_1st\_peak}$ > 1600°C or $T_{max\_clad\_2nd\_peak}$ > 1000°C or T_{max_gas} > 1250°C or $P_{close\_containment}$ > 1.4 MPa.

With the 100 simulations, we obtain an estimate of the failure probability $\overline{P_f}$ = 0.49 with an acceptable accuracy (variation coefficient $cov(\overline{P_f})$ = 0.10). To date, this estimation should be retained for this scenario in the PSA. However, this result shows also the necessity to improve the reliability of the natural circulation DHR. Tracks of improvement should be to increase the nitrogen volume, to drain successively the three accumulators or to review the design of the close containment.

Failure probability with regards to each criterion considered independently

In this estimation, the four responses of interest have been modeled by normal distributions (hypothesis not rejected by goodness-of-fit tests), with averages and standard deviations obtained on the 100 simulations. The failure probabilities (Table 6) are then estimated by: $P_f = P(Y \geq S) = 1 - P(Y$

$< S) = 1 - F_Y(S)$, with: Y, one of the responses, S, the associated failure criterion and F_Y, the cumulative function of Y (normal distribution). Note that here the failure probability for each response is evaluated independently of the others and the sum of these four probabilities exceeds slightly the total failure probability of the system calculated previously ($\overline{P_f}$ = 0.49), because in some simulations, two failure criteria may have been exceeded at the same time. These results enable us to conclude that the most often exceeded failure criterion is the gas temperature at core outlet (1250 °C). Figure 6 shows the scatter in the 100 curves of evolution of this gas temperature and on the peak of temperature. The second failure criterion, for which attention should be paid, is the pressure in the close containment. The criteria on the clad temperatures have very low probabilities compared to the two mentioned above.

Responses of interest	P_f
Maximum clad temperature (1st peak)	$2{,}46.\ 10^{-4}$
Maximum clad temperature (2nd peak)	$3{,}61.\ 10^{-4}$
Maximum temperature of gas at core outlet	0,456
Maximum pressure in the close containment	0,092

Table 6: Failure probabilities with regards to each criterion

9. Global sensitivity analysis

The objective of this analysis is to evaluate the importance of each input uncertain parameter in contributing to the overall uncertainty of each response of interest. A global sensitivity analysis has been carried out by the way of standard regression coefficients. Considering that the response Y is a linear function of the random input variables X_i, the standardized regression coefficients (SRC) are obtained from the regression model (1). They quantify the effect of varying each input variable away from its average by a fixed fraction of its variance. They are given by:

$$\mathbf{SRC(Y, X_i) = \beta_i \sqrt{\frac{Var(X_i)}{Var(Y)}}}$$

The sign of the SR coefficients indicates if the response increases (+) or decreases (-) when the variable increases. The sum of the SRC^2 is equal to the coefficient of determination R^2.

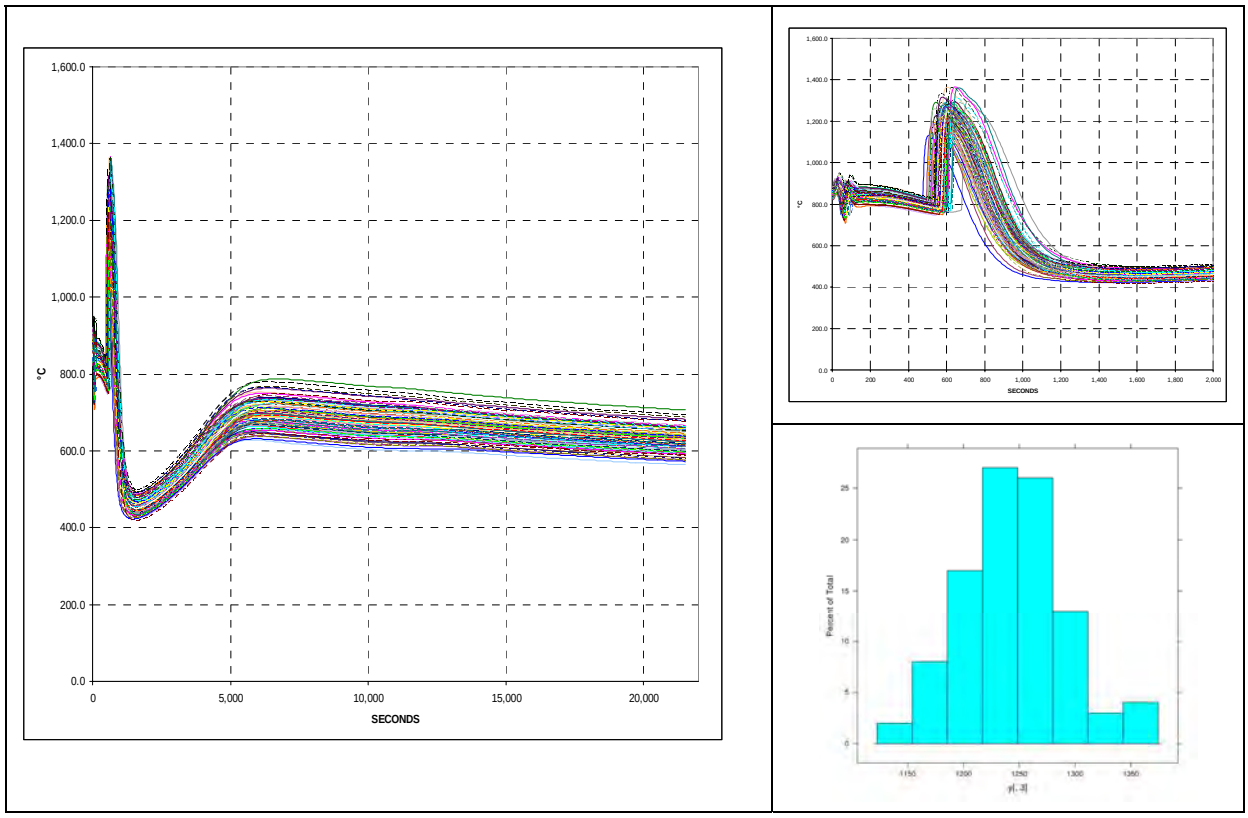


Figure 5: LOCA scenario - 100 curves of evolution of gas temperature at core outlet (left), zoom on peak of temperature (right upper) and histogram of distribution of the peak (right lower)

9.1 Scenario 1 (LOFA)

For the three responses of interest (maximum fuel, clad and helium temperatures), the hypothesis of a linear relation between the output and the input parameters is valid, because the values of the R^2 are close to 1 in each case and so we can use the *SR* coefficients as sensitivity indices. The results obtained on the *SR* coefficients for the three temperatures are logically very close as the three temperatures are correlated. Table 6 gives for example the *SR* coefficients obtained for the maximum clad temperature. The most influential parameters on this temperature are the primary blower inertia, the wall thermal inertia and the core residual power. They explain together about 90% of the uncertainty of the clad temperature. The most important parameter is the primary blower inertia which explains itself about 69% of the temperature uncertainty.

9.2 Scenario 2 (LOCA)

For the four responses of interest (maximum clad and gas temperatures at first and second peak, maximum helium temperature and close containment pressure), the hypothesis of a linear relation between the output and the input parameters is valid and *SR* coefficients are used as sensitivity indices. *SR* coefficients for the two temperatures (clad and helium) at first peak are very close because these two temperatures are correlated. The most influential parameters (Table 7) are the core residual power, the lower plenum pressure for accumulator discharge and the primary blower inertia. For the maximum clad temperature at second peak (Table 8), the most influential parameters are the residual power and the close containment free volume.

Rank	Input parameter	*SRC*	SRC^2
1	Primary blower inertia	-0.829	0.687
2	Wall thermal inertia	-0.328	0.107
3	Core residual power	0.300	0.090
4	Core nominal power	0.193	0.037
5	Heat transfer in DHR IHX	-0.116	0.014
6	Helium clad heat transfer	0.114	0.013
7	Main circuit pressure	-0.054	0.003
8	Inlet k-factor in DHR primary loop	0.013	1.7 e-04
9	Core total pressure drop	0.008	6.8 e-05
10	Outlet k-factor in DHR primary loop	-0.008	5.9 e-05

Table 6: Standardized regression coefficient for maximum clad temperature (LOFA)

Rank	Input parameter	*SRC*	SRC^2
1	Residual power	0.658	0.433
2	Lower-plenum pressure for accu. discharge	-0.495	0.245
3	Primary blower inertia	-0.480	0.230
4	Gas mixture heat capacity	-0.255	0.065
5	Nominal power	0.226	0.051

Table 7: Standardized regression coefficients for maximal clad temperature at first peak (LOCA)

Rank	Input parameter	*SRC*	SRC^2
1	Residual power	0.864	0.747
2	Close containment free volume	0.454	0.207
3	Gas mixture heat capacity	- 0.301	0.091

Table 8: Standardized regression coefficients for maximal clad temperature at second peak (LOCA)

10. Conclusions

In support to a PSA performed at the design level on the 2400 MWth GFR, the functional reliability of the DHR system working in natural circulation has been estimated in two transient situations corresponding to an “aggravated” LOFA and to a LOCA. The reliability analysis was based on the RMPS methodology. The failure probability of the DHR system in case of LOFA transient is very small, considering realistic uncertainties for the input parameters and even in increasing greatly their ranges of variation. The DHR system working in natural circulation appears a very reliable system for this type of LOFA accident and even when only one DHR loop is available. In the PSA, the functional failure probability of the natural circulation DHR in pressurized situations has been upper-bounded by 5×10^{-6}. For the second transient, the reliability analysis of the natural circulation DHR system shows a high conditional probability of failure essentially due to the risk of exceeding the criterion associated to the gas temperature at core outlet. Following the global sensitivity analysis, this risk should be limited by increasing the reference values of two parameters: the lower plenum pressure for accumulator discharge (this parameter has been set to 14 bars in the reference design) and the blower inertia, and by limiting their uncertainties.

11. Acknowledgments

This work has been partly carried out within the framework of the collaborative action “Performance Assessment of Passive Gaseous Provisions” (PGAP) of the IAEA INPRO project. The authors acknowledge the insights gained through the fruitful discussions with the PGAP members and with Mr Hussam Khartabil, INPRO responsible officer.

12. References

BALMAIN M. et al.(2011), A level 1 PSA as a support to the CEA 2400 MWth Gas-cooled Fast Reactor, In Proc: PSA2011 conference, Wilmington, USA.

BASSI C. et al. (2008), Reliability assessment of 2400MWth gas-cooled fast reactor natural circulation decay heat removal in pressurized situations. Science and Technology of Nuclear Installations, Special issue “Natural Circulation in Nuclear Reactor Systems.

BASSI C. et al. (2010), Level 1 probabilistic safety assessment to support the design of the CEA 2400MWth gas-cooled fast reactor, Nuclear Engineering and design, 240, pp 3758-3780.

BURGAZZI L. (2002), Reliability evaluation of passive systems through functional reliability assessment, Nuclear Technology, 144, pp.145-150.

BENTIVOGLIO F. et al. (2007), CATHARE simulation of a depressurization transient for the 2400MW Gas Fast Reactor concept, In proc: ICAPP’07 Conference, Nice, France.

MALO J.Y. et al. (2007), The DHR systems of the GFR, preliminary design and thermal-hydraulics studies, Proceedings of ICAPP’07, Nice, France.

MARQUÈS M. et al. (2005), Methodology for the reliability evaluation of a passive system and its integration in a Probabilistic Safety Assessment, Nuclear Engineering and Design, 235, Issue 24, pp. 2612-2631.

MESSIÉ A. et al. (2007), The CATHARE simulation of non depressurized transients for the 2400 MWth gas fast reactor concept”, In proc: ICAPP’07 Conference, Nice, France.

RELIABILITY ANALYSIS OF 2400 MWTH GAS-COOLED FAST REACTOR NATURAL CIRCULATION DECAY HEAT REMOVAL SYSTEM

M. Marquès, C. Bassi & F. Bentivoglio
michel.marques@cea.fr
CEA, DEN, SESI, Cadarache, F-13108 Saint-Paul-lez-Durance, France

INTRODUCTION

- The treatment in PSA of safety passive systems (specially category B passive systems implementing moving working fluid) is a difficult task because in addition to the mechanical failures of its components (**hardware failure**), the failure of the system in achieving its intended design function, referred as **functional failure** [Burgazzi] has to be considered.
- The difficulty in the evaluation of the functional failure risk lies in the great number of parameters that must be taken into account, in their associated uncertainties and in the limitations of physical modelling.
- A **PSA has been developed by CEA** [Bassi, Balmain] **to support the design of the 2400 MWth Gas-cooled Fast Reactor** (GFR).
- We present here the functional reliability analysis carried out for the **passive decay heat removal system (DHR) of the GFR**, in support to this PSA.
- The **reliability** of the DHR system has been studied **in two accidental situations**.
  - For these two situations, we have considered that all the active features cannot operate and that the only way is completely passive using **natural circulation**.
  - The reliability analysis is based on the **RMPS methodology** [European Project].
  - **Reliability and global sensitivity** analyses use uncertainty propagation by **Monte Carlo** techniques.

OUTLINE

- Introduction
- DHR system description
- DHR system function
- Scenarios selected for natural circulation reliability evaluation
- Failure criteria
- Modeling
- Identification and quantification of uncertainties
- Propagation of uncertainties through Thermal-Hydraulic code
- Failure probabilities evaluation
- Global sensitivity analysis
- Conclusion

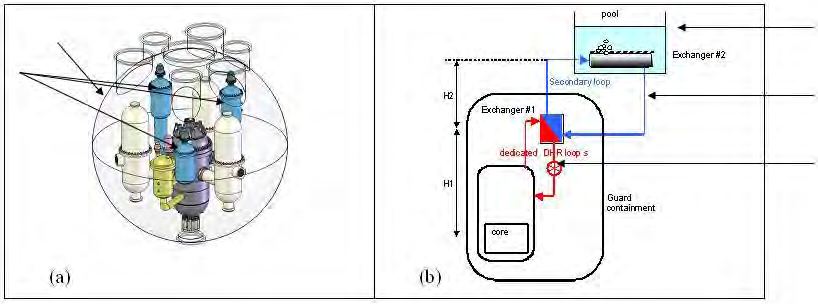
DHR SYSTEM DESCRIPTION

The DHR system (a) consists:

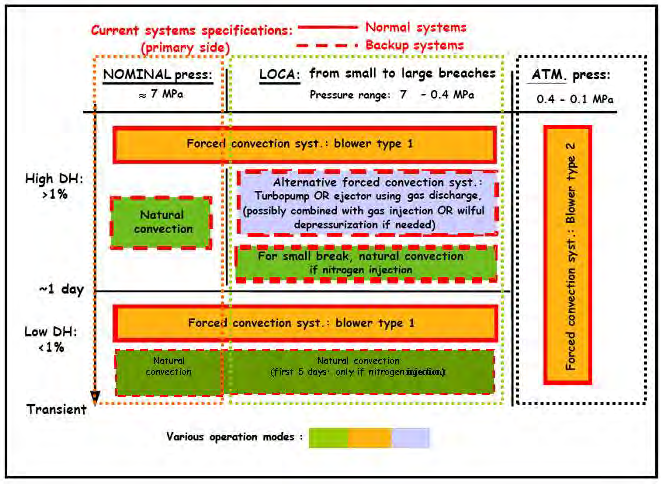
1. 3 dedicated DHR loops (3 x 100% redundancy)
2. a metallic guard containment enclosing the primary system (close containment),

Each dedicated DHR loop (b) is composed

1. a primary loop (in **F**orced **C**irculation with blower, or **N**atural **C**irculation)
2. a secondary circuit filled with pressurized water (**N**atural **C**irculation)
3. a ternary pool, initially at 50°C,



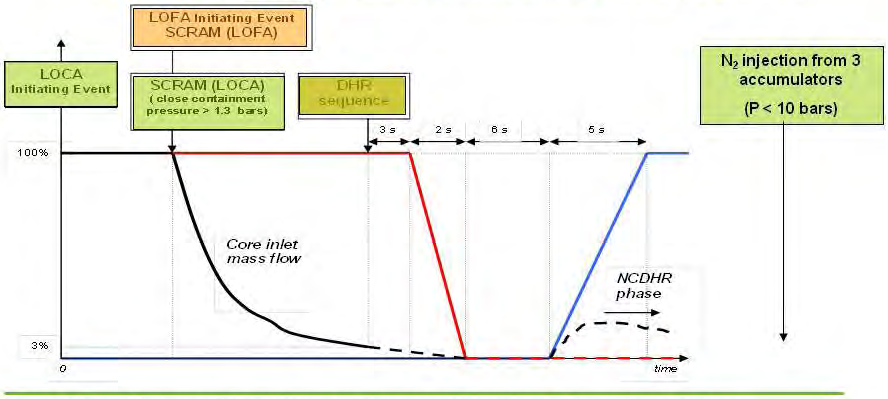
DHR STARTEGY WITH NATURAL/FORCED CIRCULATION



SCENARIOS FOR NCDHR RELIABILITY EVALUATION

1. **Station Black-Out (SBO) initiating event:** Loss Of Station service Power [illegible] failure to start 1 DHR loop available
2. **3 inches diameter LOCA initiating event** located on the cold part of a main cross-duct, representative of depressurized situations, with a total loss of forced circulation DHR means: 2 DHR loops available.

Two transient scenarios are selected to be representative of the situations of interest regarding the natural circulation DHR process for the GFR

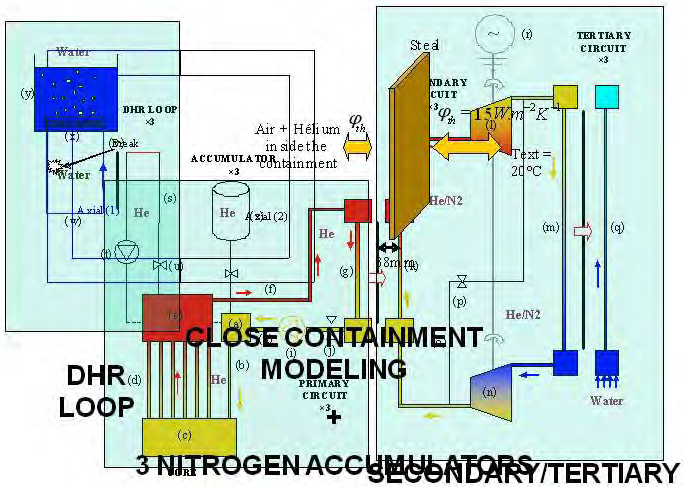


FAILURE CRITERIA

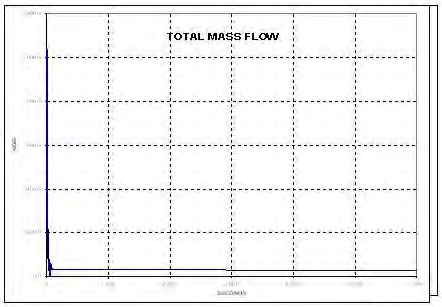
Preliminary acceptance criteria for Category IV scenarios (frequency ranging from 10^{-6} to 10^{-4})

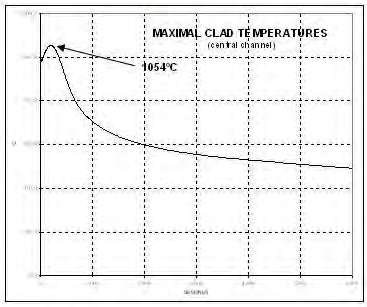
CRITERION	LOFA	LOCA
DHR LOOP STRUCTURAL INTEGRITY (MAX T OF DHR STRUCTURAL MATERIAL)	850°C	850°C
COOLABILITY & CORE INTEGRITY (MAX CLAD T)	1600°C	1600°C
CORE UPPER STRUCTURES INTEGRITY (MAX GAS T AT CORE OUTLET)	1250°C	1250°C
NITRIDING & EXOTHERMIC REACTIONS (MAX CLAD T)	-	1000°C
CLOSE CONTAINMENT INTEGRITY (MAX P IN CLOSE CONTAINMENT)	-	1.4 MPa

MODELING WITH CATHARE 2 CODE



REFERENCE RESULTS (LOFA)





- a stable flow-rate of ~30 kg/s is quickly (less than 100 s) established in the DHR loop
- and maintained up to the end of the transient during the natural circulation phase

- all failure criteria are respected, with values staying well below the safety limits:

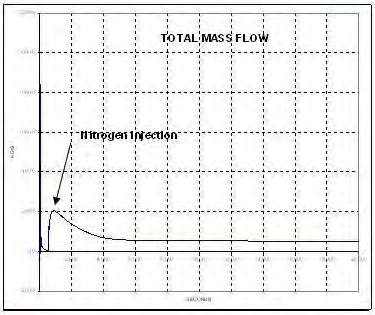
T_{MAX_CLAD} = 1054°C << 1600°C

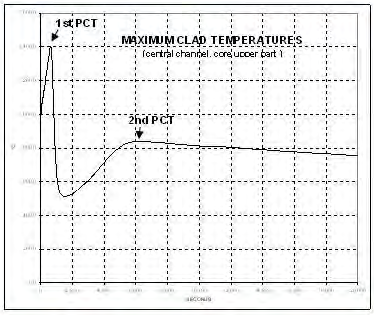
T_{MAX_GAS} = 1034°C << 1250°C

$T_{MAX\_DHR\_STRUCTURES}$ < 850°C

On the reference calculation, with nominal values of the input parameters, the heat removal is sufficient and only one DHR loop working in natural circulation fulfils perfectly its mission

REFERENCE RESULTS (LOCA)





- after nitrogen injection a flow-rate of at least 50 kg/s is established in the DHR loops
- and maintained up to the end of the transient during the natural circulation phase

- all failure criteria are respected:

1st T_{MAX_CLAD} = 1404°C << 1600°C

2nd T_{MAX_CLAD} = 840°C << 1000°C

T_{MAX_GAS} = 1241°C < 1250°C

$T_{MAX\_DHR\_STRUCTURES}$ < 850°C

On the reference calculation, with nominal values of the input parameters, the heat removal is sufficient and two DHR loops working in natural circulation fulfils their mission with the help of nitrogen injection from accumulators. But the margin is only 9°C on third criteria (core upper structures integrity)

UNCERTAINTIES IN LOFA SCENARIO

Selected for reliability anaysis

N°	Parameter	Selected N°	Reference	Min value	Max value
1	Secondary DHR loop pressure (MPa)		1	0.7	1.3
2	**Plate-type core laminar pressure drop coefficient**	1	1	0.85	1.15
3	Singular pressure drop coef. for DHR stopped blower		1	-	674
4	Natural leakage from primary circuits to containment (kg/s)		0	-	0.02
5	Singular pressure drop coefficients for core channels		K	K*0.9	-
6	**Singular pressure drop coefficient at DHR IHX inlet**	2	1	-	10
7	**Singular pressure drop coefficient at DHR IHX outlet**	3	1	-	10
8	DHR pool temperature (°C)		50	42.5	57.5
9	**Helium-clad heat transfer multiplicative factor**	4	1	0.95	1.05
10	**Multiplicative factor for all wall thermal inertia**	5	1	0.85	1.15
11	**Corrective factor for HT in DHR IHX**	6	1	0.9	1.1
12	Corrective factor for HT in DHR pool		1	0.5	1.5
13	Delay between main loop closure and DHR loop opening		6	-	26
14	Core flow rate threshold for primary valve closure		3% Q_{nom}	2.5% Q_{nom}	3.5% Q_{nom}
15	**Core nominal power**	7	Pnom	0.98 Pnom	1.02 Pnom
16	**Core residual power**	8	Pres	0.9 Pres	1.1 Pres
17	**Primary blowers inertia**	9	Iref	0.75 Iref	1.25 Iref
18	**Main circuit pressure (MPa)**	10	P_{main}	0.8 P_{main}	1.2 Pmain
19	Heat exchange coef. for DHR cross-duct insulation (W/m/K)		0.6	0.1	10
20	Homogenized fuel specific heat capacity		$\rho.Cp_{FUEL} = f(T)$	-10%	+10%
21	Homogenized fuel thermal conductivity		$\lambda_{FUEL} = f(T)$	-10%	+10%
22	Helium specific heat (J/kg/K)		5193	-10%	+10%
23	Helium thermal conductivity		$\lambda_{HE} = f(T)$	-10%	+10%
24	Helium dynamic viscosity		$\mu_{HE} = f(T)$	-10%	+10%

UNCERTAINTIES IN LOCA SCENARIO

Selected for reliability anaysis

N°	Parameter	Selected N°	Reference	Min value	Max value
1	Core total pressure drop		1	-15 %	+15%
2	Inlet k-factor in DHR primary loop		1	0	2
3	Outlet k-factor in DHR primary loop		1	0	2
4	**Helium clad heat transfer coefficient**	1	K	-25%	+25%
5	Multiplication factor for thermal inertia for all walls		1	-15 %	+15%
6	**Corrective factor for heat transfer in DHR IHX**	2		-25%	+25%
7	**Core nominal power**	3	Pnom	-2%	+2%
8	**Core residual power**	4	Pres	-10%	+10%
9	**Primary blower inertia**	5		-25%	+25%
10	Main circuit pressure (MPa)			-0.2	0.2
11	**SCRAM actuation ($P_{containment}$ in bar)**	6	1.3	1	2
12	**Accumulators discharge (Primary pressure in bar)**	7	10	8	12
13	Delay between main loop isolation and DHR conection (s)		6	4	10
14	Gas mixture viscosity		Wilke law	-5%	+ 5%
15	**Gas mixture conductivity**	8	Mason & Saxena law	- 10%	+ 10%
16	**Gas mixture heat capacity**	9		-5%	+5%
17	Close containment leakages (kg/s)		$2\ 10^{-4}$	-	+10%
18	**Close containment free volume (m^3)**	10	11620	-10%	+10%
19	Close cont. heat exchange with the outside ($w/m^2/K$)		15	-10%	+10%
20	Close containment outside temperature (°C)		20	10	30
21	Close containment initial temperature		50	30	70
22	Volume of heat structures in close containment (m^3)		1574	-10%	+10%
23	Closed containment initial pressure (bar)		1	-10%	+10%
24	Accumulators initial pressure (bar)		75	70	80
25	Accumulators initial temperature (°C)		50	30	70
26	Discharge line singular pressure drop		15	-50%	+50%
27	Break size (inches)		3	-10%	+10%

OAT SENSITIVITY ANALYSIS (LOCA)

N°	Parameter	Modification	1st PCT (°C)	2nd PCT (°C)	He max T (°C) at core outlet	Close containment max P (bars)
	Failure criteria		1600	1000	1250	14.000
	Reference case		1404.4	842.2	1243.3	13.332
1	Helium clad heat transfer coefficient	- 25 %	1377.9	851.2	1219.6	13.330
		+ 25 %	1417.7	836.9	1253.0	13.331
2	Corrective factor for heat transfer in DHR IHX	- 25 %	1428.3	926.9	1263.8	13.514
		+ 25 %	1385.3	792.8	1226.1	13.215
3	Core nominal power	- 2 %	1378.7	825.9	1222.7	13.325
		+ 2 %	1426.5	858.8	1260.8	13.338
4	Core residual power	- 10 %	1327.7	761.0	1184.1	13.287
		+ 10 %	1472.3	921.8	1292.4	13.371
5	Primary blower inertia	- 25 %	1457.6	844.1	1284.9	13.312
		+ 25 %	1359.3	840.6	1206.4	13.351
6	SCRAM actuation ($P_{containment}$)	- 0.03 MPa	1386.1	842.2	1227.0	13.320
		+ 0.07 MPa	1452.7	842.6	1282.8	13.350
7	Accumulators discharge (Primary pressure)	- 0.2 MPa	1460.7	839.9	1292.5	13.337
		+ 0.2 MPa	1356.1	844.3	1195.7	13.328
8	Gas mixture conductivity	- 10 %	1416.6	859.1	1253.0	13.418
		+ 10 %	1392.7	828.2	1233.8	13.261
9						
10						

Effects of some parameters on the first and on the second peak of clad temperature are contradictory, because an early nitrogen injection limits the first peak but is unfavorable for the second, the nitrogen accumulators being empty earlier → difficulties in the design of the reactor in finding an optimum for these parameters.

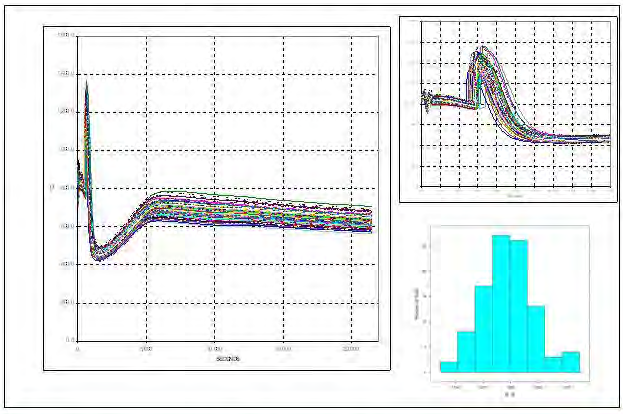
UNCERTAINTIES PROPAGATION THROUGH T-H MODEL

- **Latin Hypercube Sampling**
- **LOFA scenario**: 1000 simulations with CATHARE 2 code and use of linear response surface: $Y = \beta_0 + \sum_{i=1}^{p} \beta_i X_i$
- **LOCA scenario**: 100 simulations with CATHARE 2 code

Ex:

LOCA scenario

Gas T at core outlet



FAILURE PROBABILITIES (LOFA)

Direct simulation → No failure cases among the 1000 simulations

Conservative upper bound given by Wilks' formula:

for β (confidence level) = 0.95 & N =1000

→ $p_f \leq \gamma$ = 0.003

$$1-(1-\gamma)^N \geq \beta$$

Simulation with response surface

Performing various numbers of simulations (up to 10^7) with this linear model, the maximal value obtained is 67°C below the failure criteria

In the PSA, the functional failure probability of the natural circulation DHR in pressurized situations has been upper-bounded by 5×10^{-6} and this result is implemented as basic event in the PSA model.

However studies should be sustained to evaluate the pressure drop caused by the stopped blower and to assess the need to bypass it in situations of natural circulation.

FAILURE PROBABILITIES (LOCA)

Failure when

$$T_{max\_clad\_1st\_peak} > 1600\,℃ \textbf{ or } T_{max\_clad\_2nd\_peak} > 1000\,℃$$
$$\textbf{or } T_{max\_gas} > 1250\,℃ \textbf{ or } P_{close\_containment} > 1.4\,MPa$$

Failure probability $\overline{p_f} = 0.49$ (variation coefficient = 0.10)

To date, this estimation should be retained for this scenario in the PSA.

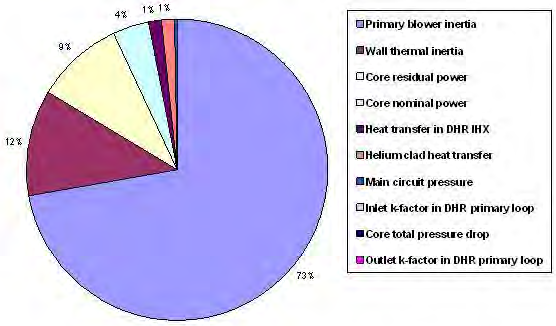
However, this result shows also the necessity to improve the reliability of the natural circulation DHR.

Tracks of improvement should be to increase the nitrogen volume, to drain successively the three accumulators or to review the design of the close containment.

GLOBAL SENSITIVITY ANALYSIS (LOFA case)

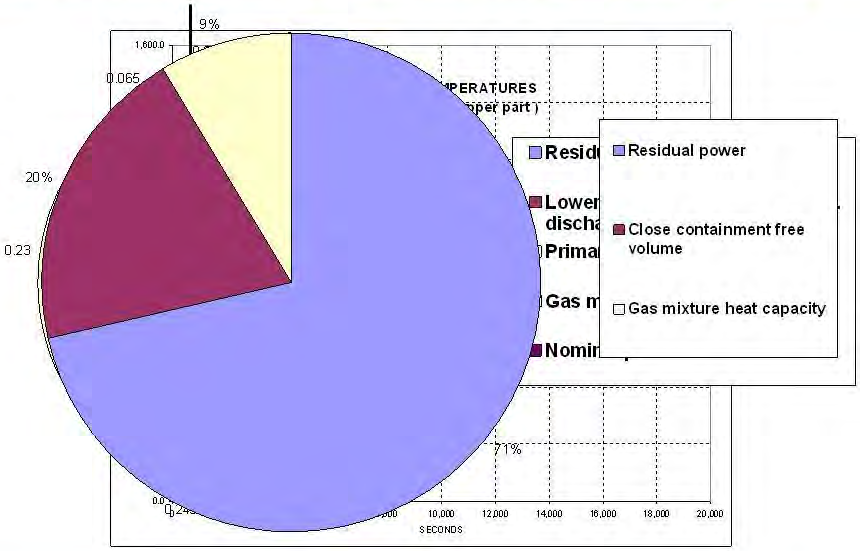
Objective: evaluate the importance of each input uncertain parameter in contributing to the overall uncertainty of each response of interest.

Standard Regression Coefficients : $SRC(Y, X_i) = \beta_i \sqrt{\frac{Var(X_i)}{Var(Y)}}$



SRC ON RESPONSE : MAXIMAL CLAD TEMPERATURE

GLOBAL SENSITIVITY ANALYSIS (LOCA case)



CONCLUSIONS

- In support to a PSA performed at the design level on the 2400 MWth GFR, the functional reliability of the DHR system working in natural circulation has been estimated in two transient situations corresponding to an "aggravated" LOFA and to a LOCA.
- The failure probability of the DHR system in case of LOFA transient is very small, considering realistic uncertainties for the input parameters and even in increasing greatly their ranges of variation. The DHR system working in natural circulation appears a very reliable system for this type of LOFA accident and even when only one DHR loop is available.
- For the LOCA transient, the reliability analysis of the natural circulation DHR system shows a high conditional probability of failure essentially due to the risk of exceeding the criterion associated to the core upper structures integrity. Following the global sensitivity analysis, this risk should be limited by increasing the reference values of two parameters: the primary pressure for accumulator discharge and the blower inertia, and by limiting their uncertainties.

Probabilistic Safety Assessment Activities in India for New and Advanced Reactors

Rajee Guptan[1], S.G. Ghagde[1], ,P.V. Varde[2], Gopika Vinod[2], J. Arul[3], R. B. Solanki[4], R. Nama[1]
1. Nuclear Power Corporation of India Limited, Mumbai 400 085 (India)
2. Bhabha Atomic Research Centre, Mumbai 400 085 (India)
3. Indira Gandhi Centre of Atomic Research, Kalpakkam, (India)
4. Atomic Energy Regulatory Board, Mumbai 400 085 (India)
Email: grajee@npcil.co.in

Abstract

In India, Level 1 PSA activities to a large extent focus on the PHWR type of designs since late eighties. The PSA of Twin (comprises of unit 1 and 2) BWRs at Tarapur Atomic Power Station (TAPS) has also been carried out and the insight gained on this PSA was used in support of ageing studies. However, currently there exists Level 1 PSA studies for new reactors which include 1000 MWe VVER type PWRs and up-rated 540 MWe PHWRs.

Apart from this, the design work of 300 MWe Advanced Heavy Water Reactor and 700 MWe PHWR is at the advanced stages. While the PSA activities for AHWRs for all the three stages has been completed the Level 1 PSA for 700 MWe PHWR is in progress.

This paper discusses, in brief, the salient features of the Level 1 PSA for New and Advanced reactors in India. The features of Level 1 PSA for new reactors are being discussed through a case study of 540 MWe twin unit (comprises of Unit 3 and 4) PHWRs at TAPS. The major feature of PSA of advanced reactors is also discussed through the specific issues that were encountered during PSA modeling of AHWR and 700 MWe PHWR.

Keywords - PSA, CDF, RIDM

1. Introduction

This paper discusses, in brief, the salient features of the Level 1 PSA for new reactors and extensive use of PSA/RA studies for finalizing the design aspects of Advanced reactors, in India. The features of Level 1 PSA for new reactors are being discussed through a case study of 540 MWe twin unit (comprises of Unit 3 and 4) PHWRs at TAPS. The major feature of application of PSA in advanced reactors is also discussed through the specific issues that were encountered in the design stage of AHWR and 700 MWe PHWR

A comprehensive Level-1 PSA for internal events has been conducted for Tarapur Atomic Power Station -3&4 a Pressurized Heavy Water Reactor comprises of two units of 540 MWe each. The reactor uses Heavy water moderator and pressurized heavy water coolant, natural uranium fuel and horizontal pressure tubes.

Latest methodologies and approaches recommended by IAEA/NUREG guidelines were adopted for conducting this PSA. The study has been done for internal initiating events during full power operation considering reactor core as the main source of radioactivity. The study was performed using RISK SPECTRUM software which is one of the state of the art software being used in many countries.

2. Objective

The major objective of TAPS-3&4 Level-1 PSA was to provide an understanding of the possible plant vulnerabilities to core damage arising from hardware, human or procedural deficiencies[7]. The anticipated uses of the study include the following:

1. Presenting an integrated picture of the safety of the 540 MWe PHWR which encompasses-design, operational practices, component reliability, dependencies and human reliability.

2. Identifying predominant contributors to possible severe core damage in terms of component failures and human actions. Attention then can be devoted to ensuring high reliability of the

components and human actions through appropriate design and O&M practices (includingsurveillance testing, ISI, permissible outage period, operator training, procedures etc.)

3. Identifying any weak-links or imbalances affecting the safety of the plant with reference to components/human actions, which could be improved.

4. Evaluating Core Damage Frequency in terms of relative importance of contributors, so as to make comparative assessments.

3. Approach

A comprehensive list of initiating events was prepared under two broad categories.

- LOCA initiators
- Transient initiators

Using (i) engineering evaluation of plant (ii) operational experience (iii) reference to lists available in literature for PHWRs (iv) List of IEs for deterministic safety analysis of Indian PHWRs (including AERB draft safety guide SG-D5). This comprehensive list was screened out on the basis of similar event progression and subsequently the initiating events (IE) were grouped based on the demands they place on safety functions, frontline systems and support systems. After grouping the IEs, nine LOCA initiating events and thirty transient initiators were analysed.

The front-line systems required for the performance of each safety function viz. reactor shutdown, decay heat removal and long term reactivity control were identified and the support systems required for functioning of these front line systems were identified. A dependence table of frontline systems and support systems was prepared. Thus, all hardware/ functional dependencies among front line systems were identified, recognising that sometimes they depend on the same support systems.
Event trees were used for event sequence modelling. Small event tree large fault tree approach was used in this analysis. Event Trees with front line systems as headings were developed based on knowledge of plant responses. For this purpose, Safety Reports and Emergency Operating Procedures were extensively referred. For each event tree heading suitable boundary conditions were incorporated wherever necessary to reflect the effect of the conditions imposed by the initiating events on the mitigating action and any other conditions that develop during the event progression. Event sequences were expressed in terms of initiating events and failures of mitigating systems, in various combinations.

Associated with some of the end states in the event trees is a certain level of core damage resulting from the postulated failure modes. There are several possible degrees of core damage, the severity depending on the extent of fuel damage and on the magnitude of the resulting radioactivity releases from the core. Radioactive releases without core damage are also of concern. For the present analysis entire spectrum of fuel damage accident sequences has been considered.

The fault tree method was used for reliability analysis of all front line systems and support systems. The general techniques of constructing and quantifying fault trees as per NUREG 0492 were used. Consistent and standardised event coding, representation of human errors and dependent failures were adopted. Generally, systems were modelled with limit of resolution established at the last component. All possible failure modes that may contribute to system unavailability including individual component failure modes, outages for testing and maintenance, human errors associated with failure to restore the equipment following testing and maintenance were considered in system analysis.

Common Cause Failures were accounted systematically. All functional dependencies were explicitly modelled in fault trees. For accounting for all other dependencies arising out of common design, manufacture, operation & maintenance and environment, common cause component groups were introduced in the FTs which were subsequently quantified using parametric models. Initial screening analysis was carried out using beta factor model and alpha factor model was subsequently used for those common cause component groups identified as dominant in screening analysis. For detailed common cause failure analysis, the generic alpha factors from NUREG/CR-5801 were used.

A judicious mix of generic and plant specific data was used, where appropriate the plant specific data were combined with generic data, using Bayesian technique.

Initiating events were classified into two groups for frequency quantification. For frequent and moderately frequent events the initiating event frequencies were quantified using outage reports of our Operating Stations since their commercial operation. For plant specific events like grid failures only TAPS-3&4 data was used. For rare events and less frequent events, international literature on CANDU reactors were made use of with reasonable judgements. Zero Occurrences for Transient Group of Initiators Chi-squared Approximation was used. Zero Occurrences for Transient Group of Initiators detailed fault trees are developed.

Uncertainty analysis was carried out using Monte-Carlo simulations. Error factors were either taken directly from the generic data sources or estimated using expert judgement and other available PSAs.

Human Reliability Analysis was performed to quantify Human Error Probability (HEP). Three types of human errors were considered.

- Pre initiators/latent human actions – Actions that cause equipment or systems to be unavailable when required post-fault due to errors that occurred pre-fault.
- Initiators that either by themselves or in combination with equipment failures lead to IEs.
- Post initiators/dynamic human actions – Actions occurring post fault.

Initiators are generally implicit in the quantification of IEs and contribute as a part to their total frequency. For the other two types of human actions i.e. latent and dynamic, IAEA TECDOC 592 and NUREG CR 1278 were followed for quantification of HEP. Both these human errors are incorporated in the fault tree models. Latent errors are quantified using screening values and refining them appropriately by use of various performance shaping factors. Human Cognitive Reliability model was used for quantifying the dynamic actions giving due credit to performance shaping factors.

Influence on operator action due to the types of cognitive processing i.e. rule based, skill based and knowledge based was also considered.

Computer code RISK SPECTRUM was used for qualitative and quantitative analysis of this PSA. The individual accident sequences of all event trees were quantified by integrating the fault tree models of all front line systems along with support systems, associated with each event tree with suitable boundary conditions. Consequence quantification analysis for each type of fuel damage category was carried out to obtain the frequency of the fuel damage category by generating Minimal Cutsets (the list of component failures) which contribute to each category of fuel damage. Uncertainty analysis was performed for each fuel damage category to estimate the range of the uncertainty associated with each category. Importance and sensitivity analyses were also carried out parallelly for basic events to identify the importance of the individual cutsets.

The engineering functions in NPCIL are governed by ISO 9001. By virtue of this, the Quality Assurance aspects of Level-1 PSA were covered by the Engineering Directorate procedures applicable for design analysis. Frontline/support system reliability analyses carried out by engineers in PSA Section were independently reviewed by adequately qualified and experienced engineers in respective design groups. RSA PROC-1 prepared by the PSA Section establishes the guidelines for various tasks in Reliability Analysis in line with IAEA guidelines, which are meticulously followed. Likewise, the event trees were got cross-checked from independent experts in NPCIL. For operational aspects, including inputs for human error probabilities, experts with operations background were consulted. The use of a verified computer code, namely RISK SPECTRUM ensures the correct processing of the inputs and quantification. Besides outputs of minimal cutsets were critically checked against physical understanding of expected outcomes.

For the 700MWe type of advanced reactors Reliability studies were extensively used for ECCS Design finalisation. Two train systems with series parallel combinations located in diametrically opposite ends of containments were designed which was first of its kind in PHWR type of reactors. Staggered testing was recommended for the first time to designers by bringing out the comparison among staggered and non staggered testing with quantitative results of system reliability analysis. A design modification was also suggested in containment isolation system based on RA/ PSA results[6].

4. Reliability Assessment of Advanced NPP

Advanced / innovative nuclear power plants employ passive systems to achieve substantial simplification and improved safety, in order to reduce active component malfunctions and human errors. It has to be ensured that the passive systems are really more reliable compared to the active systems to carry out their safety function under the prevailing conditions. A passive system may fail due to the deviation from expected behavior of parameters representing physical phenomena mainly related to thermal hydraulic, different boundary/ initial conditions in addition to the mechanical failure of (passive/active) component of the system. In AHWR, passive systems are employed to remove heat from the fuel rods during normal operation by natural circulation (main heat transport system), during LOCA (high pressure and low pressure emergency core cooling system), during accident situations where heat removal by conventional means by condenser is affected (Isolation condenser), reactor shutdown under certain situations even when wired shutdown systems fail to operate and the reactor pressure is high (passive shutdown system) and in removing heat from the containment. Studies on Passive system reliability, software reliability and uncertainty analysis are in progress.

Level-1, 2 and 3 PSA studies were carried out for a proposed advanced reactor [5]. In addition to the evaluation of LERF, it is essential to ensure that the probability of receiving dose above prescribed regulatory limit is very small. This necessitates the evaluation of the consequences in the public domain. It is all the more essential if a reactor is located near to population centre. Consequences were evaluated for postulated (i) 200% Inlet Header Break with failure of both the wired shutdown system and (ii) Main Steam Line Break (MSLB) outside the containment with failure of both the wired shutdown system for AHWR. The source term for these two cases were analysed as a part of Level-2 studies. As a part of Level-3 study, the dispersion of the radionuclides in the atmosphere and the doses to the public has been evaluated by PC-COSYMA. The predicted very low frequency of exceedence values of low dose (thyroid and bone marrow) are indicative of the defense in depth employed in AHWR.

5. Conclusion & recommendation

The results of the PSA indicate that a fairly high level of redundancies exists in TAPS-3&4 design. This is evidenced through the final CDF numbers, as well as from the predominant common cause failures observed in the core damage sequences. With the present database on component reliabilities (generic) and the identified vulnerabilities to core damage, the calculated mean frequency of severe accidents in the range of 1E-5 – 1E-6 per reactor per year. Out of this, mean frequency of severe accident beyond design basis, involving loss of core structural integrity is 2.03×10^{-6}. The later is more appropriate when comparing with CDF in LWR's. This compares favourably with IAEA recommended reference mean frequencies of 1×10^{-5} per reactor per year for new plants, no single event sequence has a predominant contribution to the severe accident frequency. The well spread-out distribution is indicative of a balanced design with respect to strengths against severe accidents.

Special emphasis should be given in training and licensing programmes of operators for creating awareness about the consequences of rare events requiring specific operator actions like Blind LOCA.

Recommendations :

1. It is recommended that staggered testing philosophy should be adopted especially for Emergency Core Cooling System, to reduce the probability of common cause failure among the motorized valves
2. It is recommended that the PSA be reviewed with a periodicity of say, five years in the light of any changes in reliability databases (generic & plant specific), new knowledge or insights on core damage phenomenology, or additional failure modes or vulnerabilities identified through operating experience.
3. It is also recommended to emphasize the importance of Small Break LOCA in general and their consequences in the licensing process of the plant operators.

References

Procedure for analysis of Common Cause Failures in Probabilistics Safety Analysis, NUREG/CR-5801

IAEA TECDOC 592 “Case study on the use of PSA methods : Human Reliability Analysis”.

Swain Handbook – HRA Hand Book of Human Reliability Analysis with an emphasis on Nuclear power Plant Application – A.D. Swain, H.E. Guttonan NUREG/CR-1278 F

Procedures for conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level-1), IAEA Safety Series 50-P-4.

‘Probabilistic Safety Assessment of AHWR’, V.Gopika, B. Chatterjee, V.Verma, I. Tangamani, M. Hari Prasad, V.V.S. Sanyasi Rao, H.G. Lele, A.K. Ghosh, International Conference on Peaceful Uses of Atomic Energy 2009, September 29 – October 2, 2009, Vigyan Bhavan, New Delhi

‘Evaluation in 700 MWe PHWR ECCS Design’ Ranjan Kumar, A.K. Vijaya, K.K. De, Rajee Guptan, Suma Nair and A.K. Chakrabarti, International Conference on Advancesin Performance and Safety of Complex System, January 5-7, 2008, NUB, Mumbai.

‘Plant Specific Risk Informed Decsision Making – A vision for Indian PHWR’, Rajee Guptan, Nalini Mohan, S.G.G hadge, S.S. Bajaj, International Conference on Reliability, Safety and Hazard, December 12-14, 2005, Mumbai.

Probabilistic Safety Assessment Activities in India for New and Advanced Reactors

Rajee Guptan
Head PSA Section
NPCIL INDIA

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

PRESENTATION OUTLINE

i) Objective

ii) Major Elements of TAPS-3&4 Level-1 PSA

- Scope
- Initiating Event
- Quality Assurance Programme
- Event Tree Development
- Features of Fault Tree
- Data for Analysis
- Human Reliability Analysis

iii) Results & Insights

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

OBJECTIVES

- Presenting an integrated picture of the safety of the 540MWe PHWR which encompasses Design, Operational Practices, Component Reliability, Dependencies and Human Reliability.
- Identifying predominant contributors to possible severe core damage in terms of component failures and human actions.
- Identifying any weak-links or imbalances affecting the safety of the plant with reference to components/human actions, which could be improved.

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

OBJECTIVES (Contd.)

- Evaluating Core Damage Frequency in terms of relative importance of contributors, so as to make comparative assessments.
- To provide an assessment of reliabilities of systems having bearing on reactor safety.
- To provide a template for `living' PSA model to assess the effect of any design and procedural changes, and to provide a tool for plant configuration management.

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

SCOPE

The main parameters that characterizes the scope of this PSA are:

- Source of radioactivity is the reactor core.
- Operational state of the reactor considered is full power operation.
- Type of Initiating Events (IE) – Internal IEs.
- Four broad categories of core damage states.
- Issues like Uncertainty and Sensitivity Analysis, Human Action Reliability and Dependence Analysis etc. were given special attention

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

INITIATING EVENTS

Initiating Events (IE) were identified under two broad categories:

- LOCA Initiators
- Transient Initiators

An Initial List of IEs was prepared by:

A) Engineering Evaluation of Plant
B) Operational Experience of Indian PHWRs
C) Reference to lists available in Literature for PHWRs
D) List of IES from Deterministic Safety Analysis of Indian PHWRs

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

INITIATING EVENTS (Contd..)

Thus, fourteen LOCA Initiators and thirty-five transient Initiators were identified.

Subsequently, the IEs were grouped based on the demands they place on safety functions, frontline systems and support systems. after grouping the IEs, nine LOCA initiators and thirty transient initiators were analysed.

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

QUALITY ASSURANCE PROGRAMME

As part of the QA programme, RSA PROC was issued by PSA Section to standardize the following:

- ❑Standardization of Procedure for System Modelling through Fault Tree Methods
- ❑Standard Formats for Documenting the System Modelling Reports
- ❑Standard Coding of Component

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

QUALITY ASSURANCE PROGRAMME (Contd.)

- Standard Component Failure Data
- Standard Reference Documents for Event Sequence Modelling
- Review By Designers and Plant Operators

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

EVENT TREE DEVELOPMENT

- An Approach to Event Sequence Modelling.
- Modelling the Plant Responses to Each Group of IEs.
- Small Event Tree and Large Fault Tree Approach.

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

FEATURES OF FAULT TREE

- Immediate Cause Concept
- Separate Dependence Table for Frontline and Support Systems
- Detailed Instrumentation Logic Development
- Unavailability of System for Different Modes for Some Systems.

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

DATA USED IN THE ANALYSIS

- Standard Table for Reliability Parameters (for Numerical Value)
- Standard Values for Repair Time
- Standard Basic Events (Relay Contact / Relay, Pump / Pump Motor)
- Pipe Failure Rate (Based on Number of Sections/Length)
- Common Cause Component Group (CCCG)
- Human Error Probability (HEP)

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

HUMAN RELIABILITY ANALYSIS

- Pre and Post Initiator Human Actions considered in the Analysis i.e. Latent and Dynamic Human Errors
- Human Cognitive Reliability Model (Ref IAEA Tec Doc 592) used for Quantification of the Dynamic Human Errors
- Eight Significant Dynamic Human Errors Modeled in the Study

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

OBSERVATIONS / RESULTS

Calculated Mean Frequency Of Severe Accidents: 2.03×10^{-6} per Reactor per Year.

- Systems High on the Importance List:
  - Emergency Core Cooling System
  - Class-III Power Supply System
  - Fire Water System
  - Service Water System
  - Active Process Water System
  - Non-Active Process Water System
- The results of this PSA indicate that a fairly high level of redundancies exist in TAPS-3&4 Design

This is evident through the final CDF numbers, as well as from the pre-dominant common cause failures observed in the core damage sequences.

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

RECOMMENDATIONS

- Special emphasis should be given in training and licensing programmes of operators for creating awareness about the consequences of rare events requiring specific operator actions.
- Components like Check Valves, restricting orifices, etc. may be regularly monitored.
- By adopting staggered testing for ECCS MVs, the calculated mean frequency of severe accident reduces by 30%

Hence, it is recommended that staggered testing philosophy should be adopted especially for Emergency Core Cooling System, to reduce the probability of common cause failure among the motorised valves.

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

700 MWE NEW PHWR
RELIABILITY ANALYSIS OF ECCS

Improvement in ECCS Reliability due to

-Two high pressure groups

-Two groups in recirculation paths

-Each capable to perform the desired function with internal redundancy

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

700 MWE NEW PHWR
RELIABILITY ANALYSIS OF ECCS (Contd..)

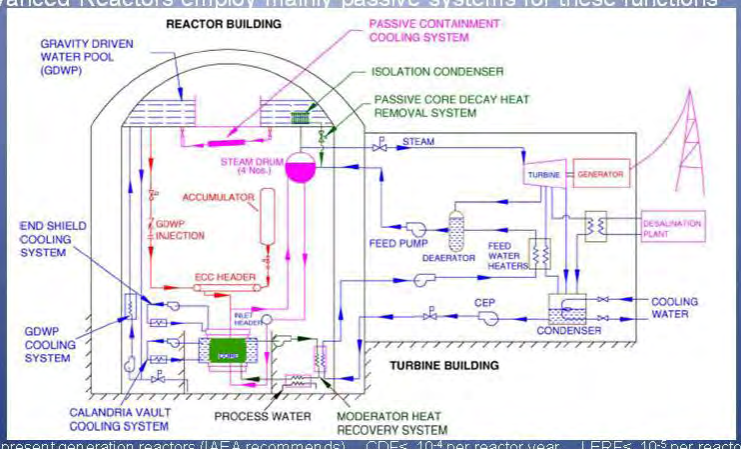
- **Testing**

  Staggered testing of redundant components will help in reducing unavailability due to common cause failures.

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

ADVANCED HEAVY WATER REACTOR

- Present generation reactors employ active systems for reactor shut down, core cooling and containment isolation,
- Advanced Reactors employ mainly passive systems for these functions



for present generation reactors (IAEA recommends) CDF≤ 10^{-4} per reactor year LERF≤ 10^{-5} per reactor year

Desired values for Advanced reactors CDF≤ 10^{-6} per reactor year LERF≤ 10^{-7} per reactor year

Ref: 'Probabilistic Safety Assessment of AHWR', V.Gopika, B. Chatterjee, V.Verma, I. Tangamani, M. Hari Prasad, V.V.S. Sanyasi Rao, H.G. Lele, A.K. Ghosh, International Conference on Peaceful Uses of Atomic Energy 2009, September 29 – October 2, 2009, Vigyan Bhavan, New Delhi

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

SALIENT FEATURES

Level 1 Studies

(i) Selection of initiating events
(ii) Event Sequence Analysis (Physics, Fuel and Thermal hydraulic Analysis)
(iii) Event Tree / Fault Tree Analysis of Process and Safety Systems
(iv) Metric is Core Damage Frequency (CDF)

Plant damage state categorization, based on thermal hydraulics studies.
(1) Core Damage State: peak clad temperature (PCT) > 1473 K
(2) Core Degradation State: 1073 K <PCT< 1473 K.
(3) Deviation from Safe State: 673 K<PCT<1073 K, (fuel failure criteria)
(4) Success State: PCT<673 K.

Passive System Reliability Analysis

- Natural circulation failure in AHWR can be identified by
  - rise in clad surface temperature above 4000C, or/and
  - occurrence of CHF by flow induced instability
- Fault trees are drawn for these deviations, considering them as virtual components
- Thermal hydraulic analysis has been done to generate the failure surface, keeping the criterion as clad temperature exceeding 400°C.
- the frequency of accident scenario involving natural circulation failure and reactor trip has been found to be 8.2e-9/yr using this method

The frequency of **Core Damage Frequency is ~5.32e-8/yr and Core Degradation is 2.56E-7/yr.**

Low CDF is attributed to (i) deployment of passive systems (ii) large water inventory (iii) lower power density (iv) –ve void coefficient

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

Thank You

Workshop on PSA for New and Advanced Reactors, June 20-24 OECD Conference Center

Applying Risk Insights in USNRC Reviews of Integral Pressurized Water Reactor Designs

M.A.Caruso, T. Hilsmeier, T. A. Kevern
U.S. Nuclear Regulatory Commission, Office of New Reactors, Washington DC, 20555,
mark.caruso@nrc.gov

Abstract

In its Staff Requirements Memorandum (SRM) on COMGBJ-10-0004/COMGEA-10-0001, "Use of Risk Insights to Enhance Safety Focus of Small Modular Reactor Reviews," dated August 31, 2010 (ML102510405), the U.S. Nuclear Regulatory Commission (NRC) directed the NRC staff to more fully integrate the use of risk insights into pre-application activities and the review of small modular reactor (SMR) applications with near-term focus on integral pressurized water reactor (iPWR) designs. The Commission's objective is to align the review focus and resources with the risk-significant systems, structures, and components (SSCs) and other aspects of the design, that contribute most to safety in order to enhance the efficiency of the review process while still enabling a decision of reasonable assurance of the design's safety. The staff was directed to develop a design-specific, risk-informed review plan for each SMR to address pre-application and application review activities. The NRC staff submitted a response to the Commission which describes its approach for (1) using risk insights, consistent with current regulatory requirements, to assign SSCs to one of a limited set of graded categories, and (2) adjusting the scope and depth of current review plans--where possible--consistent with regulatory requirements and consistent with the applicable graded category. Because the staff's review constitutes an independent audit of the application, the staff may emphasize or de-emphasize particular aspects of its review guidance (i.e., Standard Review Plan), as appropriate and consistent with regulatory requirements, for the application being reviewed. The staff may propose justifications for not performing certain sections of the reviews called for by the applicable review plan. Examples of acceptable variations in the scope of a review can include reduced emphasis on SSC attributes such as reliability, availability, or functional performance when the SSC will be in the scope of a program that specifically address the attribute (e.g., reliability assurance program, start-up testing program), or revision or elimination of acceptance criteria or review procedures that are not applicable to iPWRs due to design features that are fundamentally different from large light water reactor designs in operation or being licensed. The primary focus of this paper will be the process to determine which risk insights will be defined and applied in the grading process as well as the progress to date in applying the process to pre-application activities for iPWR designs.

Keywords reactor, PSA, iPWR, risk

1. Introduction

In its Staff Requirements Memorandum (SRM) on COMGBJ-10-0004/COMGEA-10-0001 (USNRC 2010), the U.S. Nuclear Regulatory Commission (NRC) directed the NRC staff to more fully integrate the use of risk insights into pre-application activities and the review of small modular reactor (SMR) applications with near-term focus on integral pressurized water reactor (iPWR) designs. The Commission's objective is to align the review focus and resources with the risk-significant systems, structures, and components (SSCs) and other aspects of the design, that contribute most to safety in order to enhance the efficiency of the review process while still enabling a decision of reasonable assurance of the design's safety. The staff was directed to develop a design-specific, risk-informed review plan for each SMR to address pre-application and application review activities. In response, the staff proposed a framework for review of iPWR designs (USNRC 2011) that addresses the objectives put forth in the SRM.

The proposed iPWR review framework is consistent with current regulatory requirements and Commission policy statements and builds on the staff's current application review process. The framework is more risk-informed in that it provides a graded approach for the review of SSCs with the most detailed, in-depth review (analogous to the current review process) conducted for SSCs determined to be both safety-related and risk-significant, and progressively less detailed reviews applied through those SSCs determined to be nonsafety-related or not risk-significant.

This paper briefly discusses the categorization process and discusses in detail how applicable risk information is developed and used to inform the categorization of review activities for iPWRs. However, this paper does not discuss how review plans for the various categories will be structured. This is a complex topic in its own right and is discussed in the NRC staff's response to the SRM on COMGBJ-10-0004/COMGEA-10-0001 documented in SECY-11-0024. The reader should consult that reference for more information.

2. Discussion

2.1 Categorization of Review Activities

Before discussing how appropriate risk information is developed and used to inform the categorization of review activities, it is important to understand the categorization process. Figure 1 shows the process of categorizing iPWR review activities. Four specific categories are shown. This set of categories is similar to other sets of categories that have been used for risk categorization applications in the U.S., most notably, the categories defined in Title 10, Code of Federal Regulations, § 50.69, "Risk Categorization and Treatment of Structures, Systems and Components for Nuclear Power Reactors." The categories identified for the staff's iPWR review framework distinguish between whether or not the NRC criteria for categorizing SSCs or related activities as safety-related have been satisfied and whether or not a threshold for risk significance has been exceeded.

The process begins by selecting a review activity and its associated acceptance criterion from the Standard Review Plan (SRP) and considering whether or not it applies to a non-SSC topic, e.g., programmatic, procedural or organizational. If so, it is removed from the categorization process because the framework does not include grading the review of these activities. The next consideration is whether or not the subject of the review activity is safety-related[1] or not. Following this, the staff considers whether the subject of the review activity is risk-significant or not. Reviews of issues considered both safety-related and risk-significant (category A1 in Figure 1) are performed using existing practice and are not modified in any way.

[1] Safety-related structures, systems, and components mean those structures, systems, and components that are relied on to remain functional during and following design basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable to the guidelines in Title 10, CFR, § 52.47(a)(2) or § 52.79(a)(1), as applicable.

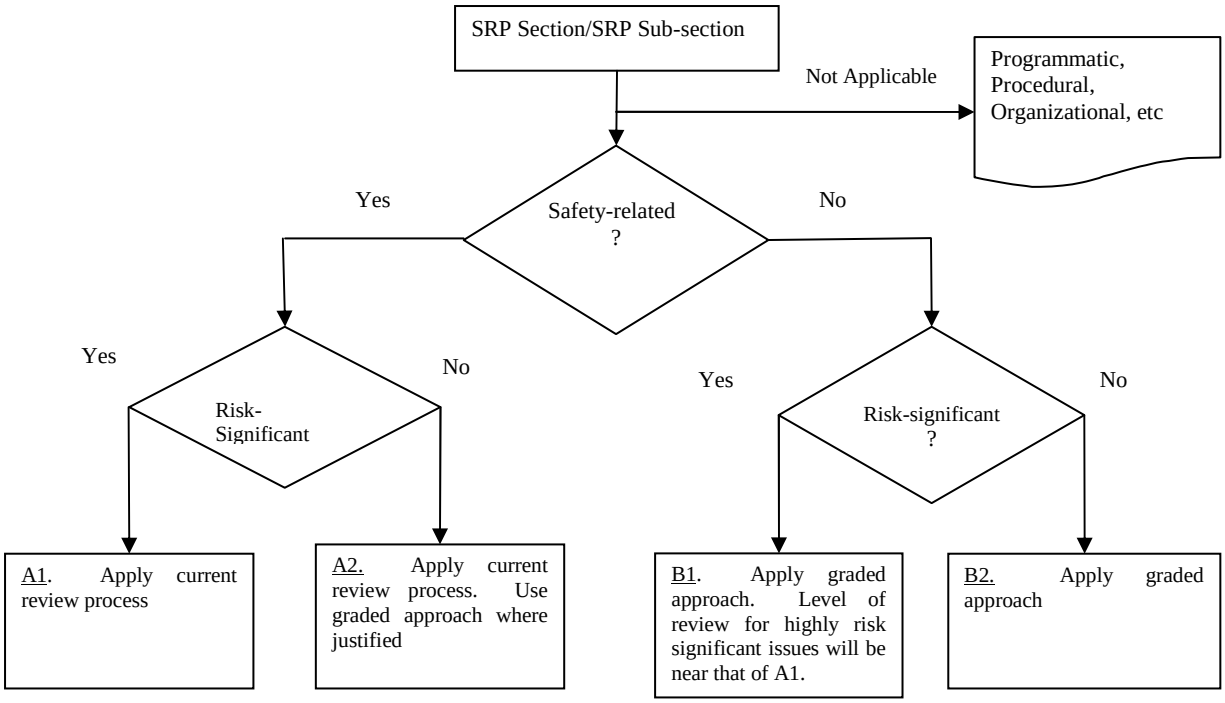


Figure 1. Process for Categorizing Review Activities

Review items in category A2 will receive a review adequate to provide reasonable assurance that whatever role they play in ensuring (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable to the guidelines in Title 10, CFR, § 52.47(a)(2) or § 52.79(a)(1), as applicable, will be performed successfully. Review items in category B1will be further classified as either highly risk-significant or risk-significant. Those that are highly risk-significant will receive a detailed review comparable with the reviews given to items in the A1 category. The remaining items in category B1will be processed in accordance with the criteria in the framework for choosing to do a less detailed review. In most cases no review will be necessary for items in category B2. However, in some cases some review may be necessary if there is a potential for impacting the health or safety of the public (e.g., potable water systems).

2.2 Determining Risk-Significance of Systems, Structures and Components

This process of determining risk-significance of SSCs consists of the following four basic steps which are discussed below.

(1) Assembly of Design/Plant-Specific Information
(2) Identification of Plant Systems and System Functions
(3) Risk Significance Determinations for Systems Functions
(4) Update Risk Significance Determinations

Like all risk-informed processes, determining the risk significance of SSCs to facilitate the risk-informed review of iPWR applications relies on an integration of information from both risk analyses and deterministic sources, such as design and licensing information. The first step in the process is to collect and examine this information. The key sources of information include:

- Information from design/plant-specific risk assessments and severe accident evaluations that cover the full spectrum of potential events and the range of plant operating modes, such as:

  - Importance measures;
  - Risk insights and key assumptions from full power and low-power/shutdown risk assessments;
  - SSCs associated with important operator actions or initiating events that are significant contributors to risk.
- The list of SSCs included in the reliability assurance program (RAP) and bases for inclusion.
- The list of nonsafety SSCs that meet criteria for regulatory treatment of nonsafety systems (RTNSS) and the bases for inclusion.
- Technical Specifications

The challenge for the NRC staff in this step is that in order to prepare review guidance that will be available when an iPWR application is submitted, the determination of risk-significance and categorization processes must be carried out before the information described above has been formally submitted to the NRC by the applicant. Indeed, the facility design is evolving and the design PRA is a work in progress during this pre-application period. To address this challenge, the NRC staff is performing pre-application audits of the design PRAs under development by likely applicants for design certification that have issued letters of intent and engaged the NRC in pre-application activities. The fundamental purpose of these audits is to gather pre-application information from the pre-applicant's probabilistic risk assessment (PRA) of their iPWR design for purposes of:

1. Assessing the extent to which the PRA is aligned with the NRC guidance and expectations for a PRA suitable for supporting design certification, and;

2. Identifying risk-insights regarding the iPWR design that the NRC staff may use to allocate its review effort for a future application for design certification in a manner consistent with the safety significance of the various design features.

The NRC has completed one such audit. During this audit the NRC gathered a significant amount of design information and risk insights useful for making some coarse preliminary qualitative assessments of risk-significance.

In the second step of the process, plant systems and associated functions addressed in SRP acceptance criteria are identified. The risk-significance and safety significance (safety-related or not) of these systems or system functions will be used to categorize the SRP acceptance criteria. From the perspective of efficient reviews of iPWR applications, it is preferable to prioritize the reviews commensurate with the risk significance of system functions rather than the risk significance of the systems themselves. This is because different SRP acceptance criteria and review activities may address different functions performed by the same system and the risk significance of different functions of the same system can be very different. For example, the ability of the condenser vacuum system to pull a vacuum in the condenser is a design function that is important to power production but not especially important to safety. However, a complete failure of the condenser vacuum system can cause a plant scram and transient and the potential for this type of event should be minimized from a risk perspective. Another example is the blowdown valves on steam generators. The safety function is to close on a containment isolation signal. The valves are placed in the open position to maintain water chemistry which is a nonsafety function. If the available information does not support risk significance determinations for system functions, then the reviews will be prioritized commensurate with the risk significance of the systems themselves.
The plant systems and system functions are identified from the following sources:

(a) design/plant-specific risk assessments and severe accident evaluations;
(b) the list of risk-significant SSCs included in the RAP, which may contain SSCs that are outside the scope of the risk assessments and severe accident evaluations and were determined to be risk-

significant by other methods (e.g., defense-in-depth, deterministic, and expert panel);
(c) nonsafety systems that meet the criteria for RTNSS.

In step three, the risk significance is determined for each identified system function or system, if available risk information does not support risk significance determinations for system functions. The NRC will use the following approach to determine risk significance:

(1) System functions that are included in RAP or RTNSS are considered risk-significant. System functions that are not included in RAP and are not included in RTNSS are low risk-significant candidates. Nonsafety system functions whose unavailability leads to focused PRA results that reach or exceed NRC safety goals are considered highly risk-significant.

(2) The risk significance of low risk-significant candidates will be confirmed during the NRC's review of the RAP and RTNSS.

The NRC will rely heavily on information from the RAP and RTNSS assessments performed by the applicant because, as discussed in Item E of the Commission policy contained in the SRM for SECY-95-132 (USNRC 1995) and SRP Section 17.4 (USNRC 2007), the application should describe an acceptable methodology for evaluating, identifying, and prioritizing SSCs according to their degree of risk significance, using a combination of probabilistic, deterministic, or other methods of analysis. The staff expects the methodology to include the use of information obtained from the following sources:

Risk evaluations that cover the full spectrum of potential events and the range of plant operating modes considered in DCD Tier 2, Chapter 19.0, which includes the use of non-PRA evaluations (e.g., Seismic Margins Analysis) when PRAs have not been performed;

Industry operating experience and relevant component failure databases;

Expert panels.

The roles and responsibilities of expert panels are also described in the application, since they play an important part in reviewing the information associated with risk-significance determinations and could compensate for the limitations of the PRA.

The RTNSS assessment uses sensitivity studies performed with the PRA to assess the importance of nonsafety systems with respect to core damage frequency (CDF) and larger release frequency (LRF). These studies are often referred to at focused PRA studies. In addition, the RTNSS assessment includes qualitative screening criteria for identifying nonsafety SSCs that contribute to causing risk-significant initiating events. The focused PRA studies can be used to identify those SSCs considered to be highly risk-significant.

The NRC reviews the methods used for RAP and RTNSS assessments and the results of those assessments as part of its review of the application for Design Certification or a Combined License. The information collected as part of the first step in determining risk significance is used to inform the staff's review.

Due to its reliance on the RAP and RTNSS assessments performed by the applicant, the NRC has communicated its desire to examine early results from these assessments in pre-application audits. The NRC has also acknowledged that the categorization process may need to be repeated as these assessments mature over the course of the design certification review, and that additional NRC technical review may be necessary for systems or system functions whose risk-significance determination has changed. Indeed, the design and plant-specific information used to identify the systems or system functions and associated risk significance may change during the NRC review of a new iPWR application. For example: Risk models may change as a result of findings from NRC

safety evaluations under SRP Sections 17.4, 19.0, and 19.1; or, the facility design may change as a result of resolving issues raised during the review. Any updating of the risk-significance for an SSC and associated re-categorization is considered step 4 in process we have been describing

The NRC staff is considering ways to minimize the impact of multiple review cycles on the overall schedule for an iPWR review. One such idea is to establish review schedules such that issues for which the determination of risk-significance is quite certain are reviewed early and those with a significant amount of uncertainty--because of RAP and RTNSS methods and results that are changing--are put farther back in the schedule. Another potential technique is to build time into the overall iPWR review schedule near the end to allow for updating previous reviews.

3. Summary

The NRC intends to perform a risk-informed technical review of iPWR designs. A framework for doing this has been developed that provides a graded approach for the review of SSCs with the most detailed, in-depth review (analogous to the current review process) conducted for SSCs determined to be both safety-related and risk-significant, and a progressively less detailed review applied to SSCs determined to be nonsafety-related or not risk-significant. The NRC will rely on assessments of risk-significance performed by the applicant, and its review of those assessments, for categorization of SSCs. The NRC staff has initiated a series of pre-application audits of the design PRAs under development by likely applicants for design certification to gather preliminary risk information to support early implementation of the framework prior to receipt of an application.

4. References

USNRC, (1995) “Policy and Technical Issues Associated with the Regulatory Treatment of Nonsafety Systems in Passive Plant Designs,” SECY-95-132, May 22.

USNRC, (2007) “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition”, NUREG-0800, March 3.

USNRC, (2010), “Staff Requirements – COMGBJ-10-0004/COMGEA-10-0001 – Use of Risk Insights to Enhance Safety focus of Small Modular Reactor Reviews” dated August 31.

USNRC, (2011), “Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews”, In USNRC Commission Paper SECY-11-0024, February 18.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Applying Risk Insights in USNRC Reviews of Integral Pressurized Water Reactor Designs

Mark Caruso, Todd Hilsmeier, Thomas Kevern
U.S. Nuclear Regulatory Commission
Office of New Reactors

1

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Background

- USNRC is currently engaged in pre-application activities with two Integral Pressurized Water Reactor (iPWR) design vendors and one power company.
- Applications for Design Certification expected in CY 2012 (NuScale) and late CY 2013 (mPower).
- Application for Construction Permit expected CY 2013.

2

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Background

- Commission directed the NRC staff (*ML102510405)* to more fully integrate the use of risk insights into pre-application activities and the review of small modular reactor (SMR) applications with near-term focus on iPWR designs.
- NRC staff has developed a framework for review of SMR designs that addresses the Commission's objectives. (*ML110110691, ML111320551)*
- Framework includes a graded approach for the review of SSCs based on risk significance and safety classification of SSCs.

3

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

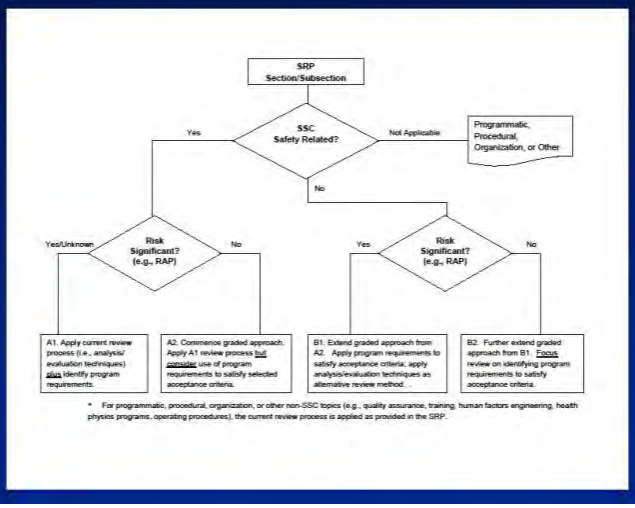
Approach

- Use risk insights to identify risk-significant SSCs and other aspects of the design that contribute most to safety
- Align review focus and resources to risk-significant SSCs and other aspects of the design that contribute most to safety to enhance the efficiency of the review process

4

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Process for Categorizing Review Activities



5

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Aligning Review Focus and Resources with Risk-Significance

- Reduce amount of licensing review where possible for less risk-significant issues
- Utilize "regulatory controls" to supplement or replace performance-oriented acceptance criteria
- Reviews against design-related acceptance criteria remain unchanged.
- Regulatory Controls include:
  - Technical Specifications
  - Availability Controls
  - Initial Test Program
  - Maintenance Rule
  - Reliability Assurance Program
  - ITAAC

6

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Determining Risk-Significance

- The process of determining risk-significance of SSCs consists of the following four basic steps:
  1. Assembly of Design/Plant-Specific Information
  2. Identification of Plant Systems and System Functions
  3. Risk Significance Determinations for Systems Functions
  4. Update Risk Significance Determinations as necessary

7

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Determining Risk-Significance
Step 1: Assembly of Design/Plant-Specific Information

- Info from design-specific PRAs
  - Importance measures
  - Risk insights and key assumptions
  - SSCs associated with important operator actions or initiating events
- List of SSCs included in the Reliability Assurance Program (RAP)
- List of nonsafety SSCs that meet criteria for regulatory treatment of nonsafety systems (RTNSS)
- Technical Specifications

8

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Determining Risk-Significance
Step 2: Identification of Plant Systems and System Functions Addressed in SRP Acceptance Criteria

- System/System function is what is being categorized
- System function preferred (can have safety and nonsafety functions in same system)
- Systems and system functions are identified from info collected in Step 2.

9

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Determining Risk-Significance
Step 3: Risk Significance Determinations for System Functions

- Approaches:
  - Use information from PRA if available (e.g., importance measures); preferred
  - Look at what is included in the RAP
  - Look at non-safety functions that will receive regulatory treatment (RTNSS)
  - Use RTNSS sensitivity studies (focused PRA) to find high risk-significant nonsafety functions

10

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Determining Risk-Significance
Step 4: Update Risk Significance Determinations

- In order to support guidance development for NRC reviews, categorization will be based on early information from an applicant's PRA.
- Applicant's PRA may change:
  - Design changes
  - Methods change
  - Errors corrected
  - Resolution of NRC review findings
- Categorization may need to be updated if the PRA changes

11

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary

- Framework for performing a risk-informed technical review of iPWR designs has been developed.
- Framework includes a graded approach for the review of SSCs based on risk significance and safety classification of SSCs.
- NRC will rely on assessments of risk-significance performed by the applicant, and its review of those assessments, for categorization of SSC related review activities.

12

Development of PSA Audit Guideline and Regulatory PSA Model for SMART

Namchul Cho[1], I.S. Kim[2], Chang-Ju Lee[1]

1 KINS, Guseoung-Dong Yuseong-gu Daejeon, Korea, 305-338, namchul.cho@kins.re.kr

2 ISSA Technology, 21318 Seneca Crossing Drive, Germantown, MD 20876, USA

Abstract

SMART is under development for dual purposes of power generation and seawater desalination in Korea. It has an integral reactor type and employs advanced design features such as a passive system. For the purpose of regulatory verification to the risk level of SMART, the insights and key issues on the PSA are identified with referring some worldwide safety guides as well as its design characteristics. Regulatory PSA model under the development for the design confirmation and its preliminary result are also described.

Keywords SMART, Regulatory PSA Model, Passive System, Reactor Risk

1. Introduction

The SMART, which stands for System-Integrated Modular Advance Reactor, with a rated thermal power of 330 MW is under development by the Korea Atomic Energy Research Institute (KAERI) for dual purposes of power generation and seawater desalination. It has advanced unique design features such as integral reactor where major components of the primary system (e.g., reactor core, pressurizer, reactor coolant pumps and steam generators) are all enclosed inside of the reactor pressure vessel, and the Passive Residual Heat Removal System (PRHRS) provides a major passive means to remove decay heat by the phenomena of natural circulation. It is noted that the safety advantage of adopting such advanced features should be confirmed through analysis or test. Therefore, it is essential to develop new probabilistic safety assessment (PSA) validation guidance to review the KAERI's PSA results, and needed to get an independent regulatory PSA model to confirm the risk outcomes provided by the KAERI's PSA model.

This paper presents the insights and key issues identified through the development of audit guideline to validate the adequacy of level 1 PSA result for SMART and preliminary evaluation results of regulatory PSA model.

2. Development of PSA Audit Guideline for SMART: Insights and Key Issues

As mentioned above, it is essential to assure technical adequacy of SMART PSA during the process of design certification since SMART employs unique design concepts. For this, the key issues due to the design characteristics of SMART are identified with referring the worldwide PSA standards and requirements for the current Pressurized Water Reactor (PWR). Finally, the audit guideline (draft) for SMART will be developed.

This section presents the insights and key issues identified through the development of audit guideline to validate the adequacy of level 1 PSA result for SMART.

2.1 Initiating Events

1) Since the maximum size of piping for the reactor coolant system in SMART is 50mm, large and medium loss of coolant accident (LOCA) by a break in the piping of the reactor coolant system can be eliminated. However, it should be confirmed whether traditional categorizing approach for LOCA size is applicable to the SMART reactor, or not.

2) SMART is a first-of-the-kind reactor and has unique design features, therefore, it is possible that some unique initiating events may occur at SMART due to its unique design features and failure of support system. And also, it is necessary to identify the new initiating events against SMART unique design features.

3) In general, initiating events identified by the use of logic structure such as master logic diagram and adopting classical list of initiating events for operational PWR are grouped considering safety functions or combinations of system response. Since safety function or system response for SMART can be different with the operational PWR, it should be reviewed that initiating events for SMART can be included in the classical initiating events group in operational PWR.

2.2 System Analysis

1) In particular, the passive system design (especially the PRHRS) poses a considerable challenge to the system reliability analysis because of its uniqueness and lack of the relevant operational experience. The worldwide PSA requirements or guideline for passive system reliability are as follows[1-2];

▪ Innovative ways to structure the search for unexpected conditions that can challenge design assumptions and passive system performance need to be developed and applied to advanced reactor.

▪ It should be checked that passive system behaviour is correctly modelled.

▪ In principle, treatment of the passive safety system in PSA is the same as that of the passive systems, such as accumulators, and of inherent passive safety features, such as natural circulation of reactor coolant when the pumps are not available. However, the reviewers should pay attention that they must, as with active systems, should identify the effectiveness by thermo-hydraulic analysis and by extensive tests.

▪ Deterministic demonstration of effectiveness needs to cover the full range of accident conditions for which they are claimed.

▪ Success performance of passive systems should be demonstrated within a set of boundary conditions which can be ensured by correct system set-up, including the correct configuration of the relevant valves.

▪ Reviewers need to check that the potential for human error is fully accounted in leaving the system in a proper condition, as well as the configuration of all necessary valves which are required to act and any active initiation signals.

▪ Given correct boundary condition and satisfactory demonstration of effectiveness, it may be regarded the system as workable.

According to above requirements, the safety advantage of adopting such advanced features should be confirmed through analysis or test. It should be also confirmed that exact fault tree analysis is performed for the PRHRS in consideration of the worldwide state-of-the-art in this area.

2) In a traditional level-1 PSA, 24 hours has typically been used as a mission time for safety systems under the assumption that once core damage is prevented for 24 hours, extensive core damage will not occur afterwards because the plant will be stabilized in a safe state. However the PRHRS in the SMART design needs to be successfully operated for 36 hours before the reactor coolant system reaches the temperature where the shutdown cooling system can be started for further removal of decay heat. Therefore, reviewers should check the impact of the assumptions (e.g., requirement for operability of PRHRS for 36 hours with subsequent decay heat removal by normal active system).

3. Development of the Regulatory PSA Model for SMART Reactor

The PSA technique has matured to the extent that can provide useful risk information to the regulatory decision-making process. Since 2009, a regulatory PSA model is under development at the Korea Institute of Nuclear Safety (KINS) focusing on internal events at power that may lead to core damage to review the design certification for SMART. In this section, the approach used in developing the regulatory PSA model for SMART, PRHRS fault tree analysis, and the preliminary result are addressed, respectively.

3.1 Approach to Develop Regulatory PSA Model for SMART

This section briefly describes the general considerations to develop regulatory PSA model for SMART.

1) Identification of Initiating Events

Initiating events that will cause a reactor trip while the SMART reactor is at power was deductively identified by use of a logic structure such as master logic diagram. The list of initiating events for Pressurized Water Reactors (PWRs) was also reviewed to identify additional initiators that are applicable to SMART. As a result, some classical initiating events such as large LOCA are eliminated considering the design characteristics of SMART and total 12 initiating events are identified.

2) Frequencies of Initiating Events

The frequencies for identified initiating events were primarily taken from NUREG/CR-6928. Since this data is based on the operating experience at PWRs, it is necessary to be adjusted for SMART reactor. For example, the frequency for a steam generator tube rupture (SGTR) at SMART was adjusted in consideration of the following unique characteristics as compared to the typical steam generators associated with the database: a) helical-coil tube bundle design of the SMART steam generators as opposed to the typical straight-tube designs, b) significant differences in thickness and length of the tubes, and in the differential pressure between the primary and secondary systems; and c) compressive forces as opposed to tensile forces resulting in a larger potential for stress corrosion cracking [3]. Some of initiating events and those frequencies for SMART is shown in Table 1.

3) Analysis of Common Cause Failures (CCFs)

Because the Alpha-factor model is event-based and as a result more straightforward in evaluating CCF events, and further, simpler in statistical treatment as compared to the Multiple Greek Letter (MGL) model, it is used in this study to quantify the potential CCFs in SMART after identifying CCF events based on the experience data in operating light-water reactors that has been recently established by the Idaho National Laboratory (INL) [4].

Table 1. Consideration on the Initiating event frequencies

IE	Frequency(/ry)	Remarks
General Transient	9.01E-01	1.2 times of NUREG/CR-6928 (Smart is a first-of-the-kind reactor)
SGTR	1.06E-03	Excluding the frequency for SCC in NUREG/CR-6928 (SMART design characteristics)
Small LOCA	5.00E-03	Including the frequency for very small LOCA and SORV

4) Analysis of Human Reliability

For identifying human error events in SMART reactor, the applicability of set of human errors that has been typically applied in PSAs for existing PWRs was reviewed. Additional human errors are also identified especially in connection with the unique SMART design and operational features. The SPAR-H methodology developed by INL under the auspices of U.S. NRC (see NUREG/CR-6883) is used for estimating human error probabilities because of several advantages such as focus on key performance shaping factors (PSFs), evaluation of the influence of each PSF on the human act with discrete scales, facilitated evaluation of dependency between multiple human error events, etc.

5) Equipment Reliability Database

The aforementioned database of NUREG/CR-6928 also contains unreliability parameters estimated for various types of equipment, and therefore, this industry-average performance data is used as a primary component database in developing the regulatory PSA model.

3.2 PRHRS Fault Tree Analysis

As mentioned above, SMART reactor employs the PRHRS to remove decay heat. In this section, we discuss our preliminary evaluation of reliability for the PRHRS using fault tree technique.

Figure 1 shows a fault tree developed in this study for unavailability of the PRHRS which consists of four independent trains with 50% of the heat removal capacity for each train. The sub-gate for components failure (i.e., PRHR1-C) models the operation of various valves needed to establish the natural circulation path along with plugging of heat exchangers and pipe rupture, while the sub-gate for natural circulation (i.e., PRHR1-N) models degraded heat transfer, loss of boundary integrity, and high concentration of non-condensable gas. Quantification of the PRHRS fault tree based on the operating data of light water reactors yields a total unavailability of 7.6 E-07, and a couple of representative minimal cutsets (i.e., the first and next dominant cutsets in terms of probability ranking) are:

▪ PRH-AOV-FO-1O (Outlet AOV of PRHRS Train 1 Fail to Open) * ACP-BAC-LP-480V2 (480V AC Bus 2 Fails)

▪ PRH-AOV-FO-2I (Inlet AOV of PRHRS Train 2 Fail to Open) * PRH-AOV-FO-3O (Outlet AOV of PRHRS Train 3 Fail to Open) * PRH-AOV-FO-4I (Inlet AOV of PRHRS Train 4 Fail to Open)

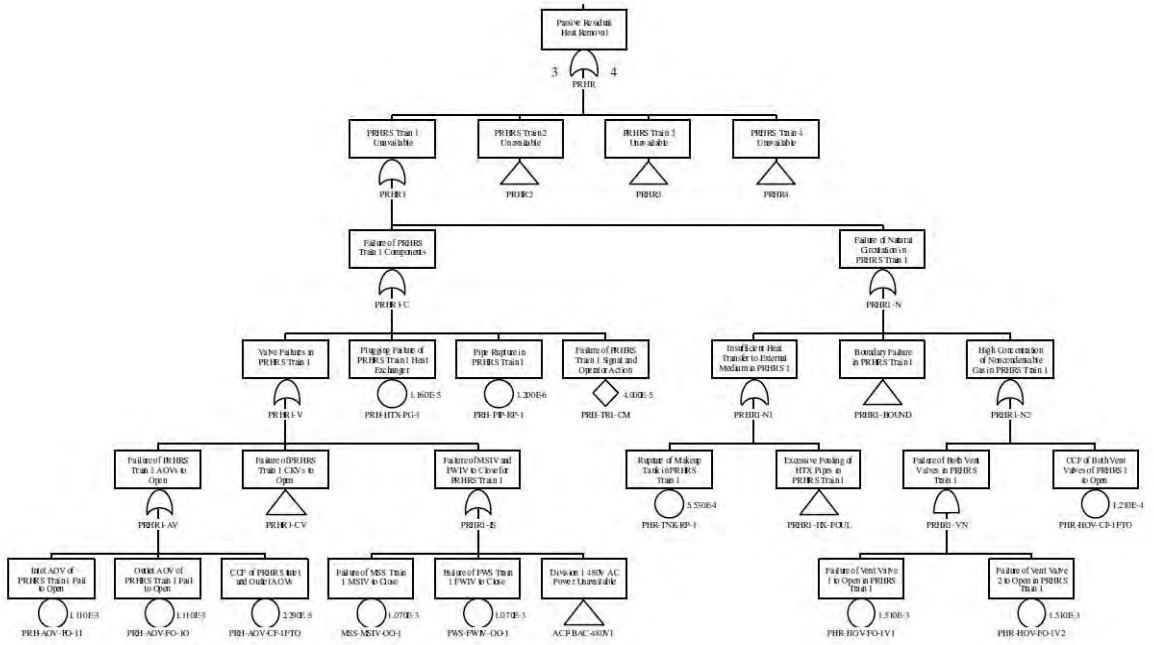


Figure 1. Fault tree for the PRHRS in the regulatory SMART PSA model

The first cutset with a probability of 1.2E-08 includes only two basic events because both train 2 and train 4 are lost by the failure of 480V AC bus 2 power which is needed to close the main steam isolation valve and the feedwater isolation valve. In this analysis, recovery actions to close these valves manually are not given credit. The second cutset with a probability of 1.4 E-09 shows that failure of each of the three PRHRS trains (i.e., train 2, 3 and 4) is caused by an active component, namely, an air-operated valve (AOV) because the flow path for the passive thermal-hydraulic function cannot be established if the AOV fails to open.

The reliability evaluation of the PRHRS yields a relatively low unavailability of 7.6E-07 primarily because of the redundancy built into the system (i.e., 2 out of 4 success criteria). However, the system unavailability may increase to some extent if the failure mechanisms for the operating passive system (e.g., breakage of natural circulation as a result of stratification, foreign material obstructions, etc.) with latent human errors potentially causing system failure or degradation are more fully accounted for. Although these failure mechanisms are not expected to cause the system unavailability markedly increased, it would have to be made sure, among others, which the PRHRS will continue to operate successfully, once initiated, under all design basis conditions.

3.3 Preliminary Results of the PSA Evaluation

A preliminary PSA model has been developed in this study using the most widely used ‘small event tree-large fault tree’ method and the approach discussed above. In this preliminary study, core damage accident scenarios identified from the event trees and fault trees of preliminary PSA model for the SMART reactor were quantified using the SAPHIRE code resulting in a total core damage frequency (CDF) of 4.88E-05 per reactor year (ry). The two most dominant initiating events were found to be loss of feedwater (LOFW) and loss of offsite power (LOOP), contributing approximately 77.9% (CDF = 3.80E-05) and 15.4% (CDF = 7.52E-06) to the total CDF, respectively (see Figure 2). In addition, the general transients scenario also make significant contribution, i.e., 3.7% of the total CDF.

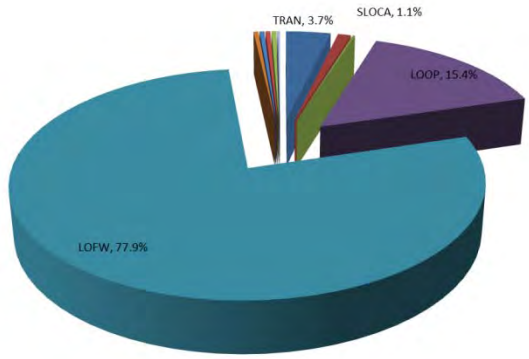


Figure 2. Preliminary importance of initiating events by the regulatory SMART PSA model

However, considerable change is expected of these risk characteristics for the SMART reactor as the PSA model becomes further refined reflecting specific design details as they become available.

Table 2. Significant accident sequences from the preliminary regulatory SMART PSA model

Dominant Scenario	Description	CDF (/ry)	%
LOFW-04	IE-LOFW*/RT*/PRHR*/PSV*/RCPSL*SDC*FAB	2.73E-05	56%
LOFW-03	IE-LOFW*/RT*/PRHR*/PSV*/RCPSL*SDC*/FAB*IRWST	1.07E-05	22%
LOOP-04	IE-LOOP*/RT*/EPS*/PRHR*/PSV*/RCPSL*SDC*FAB	4.94E-06	10%
LOOP-03	IE-LOOP*/RT*/EPS*/PRHR*/PSV*/RCPSL*SDC*/FAB*IRWST	1.94E-06	4%
TRAN-11	IE-TRAN*SGC*/PSV*/RCPSL*/PRHR*SDC*FAB	1.21E-06	2%
Total Contribution			94%

Table 2 shows the main risk significant accident sequences leading to core damage. As the event tree is shown (see Figure 3), the first dominant sequence is that the reactor successfully trips following a loss of feedwater, and the PRHRS removes decay heat for 36 hours. However, core damage occurs because the failure of shutdown cooling and also the feed and bleed operation. The second dominant sequence comes from the combination of successful reactor trip following a loss of feedwater and success of PRHRS function which removes decay heat for 36 hours. In this sequence, the plant was stable with feed and bleed cooling, but long-term cooling failed because the cooling of in-containment refueling water storage tank (IRWST) could not be properly established. The third dominant sequence is that the reactor successfully trips following a loss of offsite power, and the PRHRS removes decay heat for 36 hours. However, core damage occurs due to the same reason of the first sequence. It is note that over 94% of the total CDF is caused by failure of long-term cooling following successful

operation of the PRHRS for 36 hours, namely, failure of shutdown cooling system or feed and bleeding.

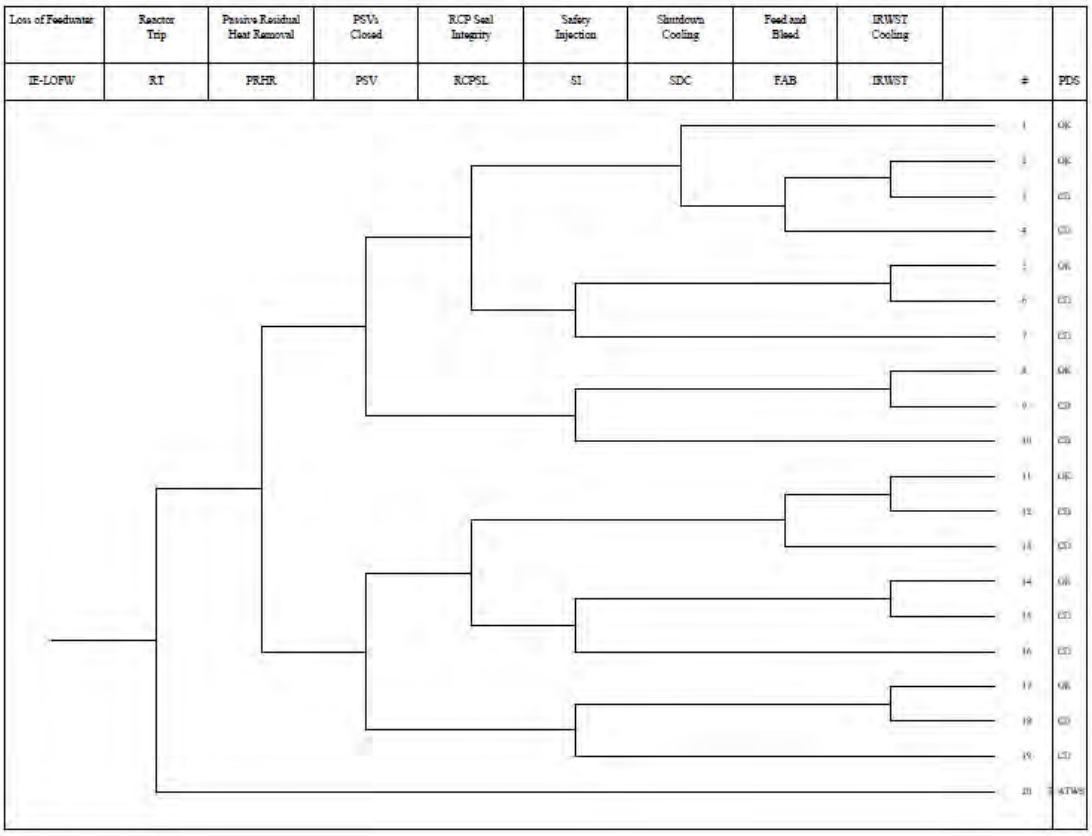


Figure 3. Event tree for the initiating event of loss of feedwater in the preliminary regulatory SMART PSA model

4. Conclusion

With referring available recent safety guides or requirements for assuring new design reactors, a lot of insights and key issues were identified for SMART reactor. Identified and currently-unresolved key issues due to SMART design characteristics are as follows:

- Applicability of classical approach for LOCA size,
- New initiating events according to the SMART unique design features,
- Grouping of initiating events considering unique design features,
- Unavailability evaluation of passive system,
- Extended mission time for the PRHRS.

It is noted that, in the design certification by the nuclear regulatory organization, special treatment or documentation may be needed in order to assure the technical adequacy for SMART PSA.

In parallel with this concern, a regulatory PSA model for internal events at power is under development and shows a first preliminary version. This paper presents key approaches to develop regulatory PSA model, to do PRHRS fault tree analysis, and to get the preliminary evaluation result. This PSA model can be utilized not only to review the level 1 PSA results obtained by licensee, but also to support various regulatory applications. We hope that it may ultimately contribute to confirm the quantitative safety level, and find – so correct some vulnerable points of current SMART design and operation concept.

In near future, these key issues and regulatory model will be managed, refined and modified by reflecting any kind of design changes for the SMART reactor since the design is being updated.

5. References

[1] U.S. Nuclear Regulatory Commission, Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, NUREG-1860, Vol. 2, December 2007
[2] Review of Probabilistic Safety Assessments by Regulatory Bodies, IAEA Safety Reports Series No. 25, IAEA, Vienna, 2002
[3] J.C. Jo and M.J. Jhung, Flow-Induced Vibration and Fretting-Wear Predictions of Steam Generator Helical Tubes, Nuclear Engineering and Design, Vol. 238, p. 890, 2008
[4] U.S. Nuclear Regulatory Commission, CCF Parameter Estimations, 2005 update, http://nrcoe.inl.gov/results/CCF/ ParamEst2005/ccfparamest.htm, January 2007

PSA for New and Advanced Reactors, June20-24, 2011

Development of PSA Audit Guideline and Regulatory PSA Model for SMART

June 20, 2011

N.C. Cho, C.J. Lee (KINS)

I.S. Kim (ISSA)

namchul.cho@kins.re.kr

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

Contents

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

1. Introduction and Objective

❑ Introduction – SMART and PRHRS

- SMART (System-Integrated Modular Advanced Reactor, 330MWt) is under development by Korea Atomic Energy Research Institute (KAERI) for dual purposes of power generation and seawater desalination
- Unique design features of SMART

  - Integral reactor where major components of the primary system, i.e., reactor core, pressurizer, reactor coolant pumps, steam generators, are all enclosed inside of the reactor pressure vessel
  - "Passive Residual Heat Removal System" (PRHRS) provides a major means to passively remove decay heat by natural circulation
- It is essential to assure technical adequacy of SMART PSA during the process of design certification since SMART employs unique design concepts

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

1. Introduction and Objective

❑ Development of PSA Audit Guideline for SMART : Insights and Key Issues

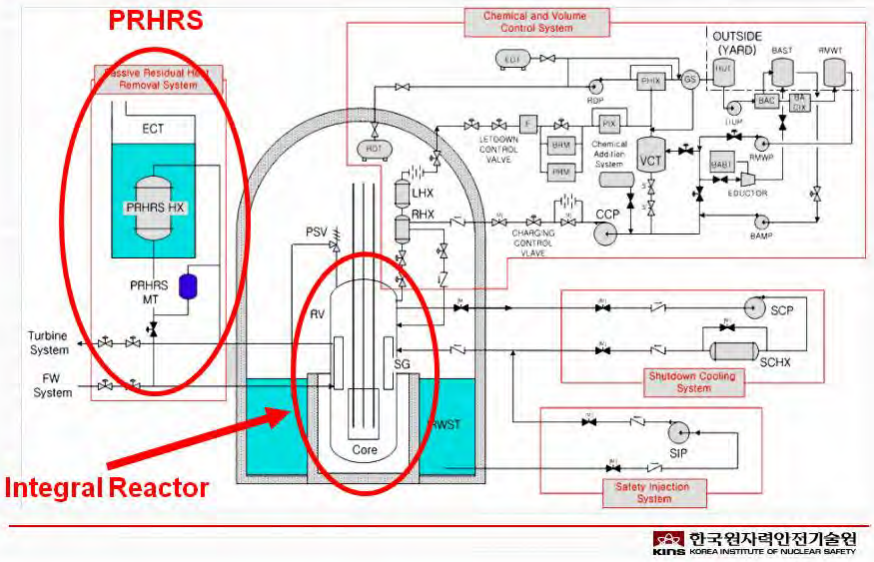
- Survey of the worldwide PSA standards and requirements for the current PWR
- Identifying the insights and key issues due to the design characteristics of SMART

❑ Development of Regulatory PSA Model for SMART

- Approach to develop regulatory PSA model for SMART
- PRHRS fault tree analysis
- Preliminary results of the regulatory PSA model evaluation

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

2. Overview of SMART Integral Reactor Plant



한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

3. Insights and Key Issues for SMART

- ❑ Initiating Events
  - ● Traditional categorizing approach for LOCA size
  - ● New initiating events against SMART unique design features
  - ● Initiating events group
- ❑ System Analysis
  - ● Treatment of the passive safety system (PRHRS)
    - Demonstrate the effectiveness by thermo-hydraulic analysis and by extensive tests
    - Check the correct system set-up including the correct configuration of the relevant valves
  - ● Mission time

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

4. Development of the Regulatory PSA model for SMART

❑ Approach to develop regulatory PSA model for SMART

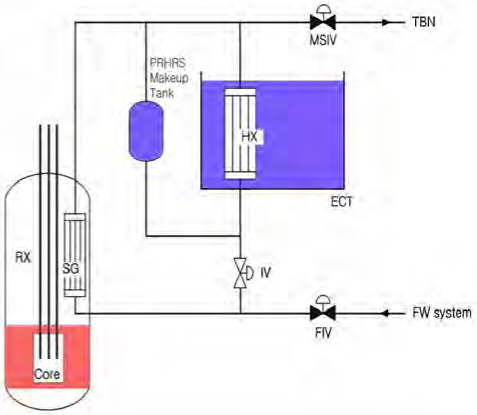
- Initiating Events
  - Master Logic Diagram + List of initiating events for PWR
  - Total 12 initiating events
- Frequencies of initiating events
  - Based on Nureg/CR-6928
  - Some initiating events are modified in consideration of unique characteristics
- Common Cause Failures
  - Alpha factor
- Analysis of Human Reliability
  - SPAR-H methodology
- Equipment reliability database
  - Based on Nureg/CR-6928

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

4. Development of the Regulatory PSA model for SMART

❑ System Description

- Four independent trains each with 50% heat removal capacity
- Piping, heat exchangers, emergency cool down tanks, makeup tanks, and PRHRS inlet/outlet valves
- MSIVs and FWIVs located in the system boundary
- Design features to maximize the natural circulation flow
  - Minimize the pressure loss in piping
  - Increase the elevation between SG and heat exchanger



한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

4. Development of the Regulatory PSA model for SMART

❑ **System Function and Operation**

- **Remove core decay heat during accident conditions**

  - From any RCS temperature during power operation down to hot shutdown condition (~323 ℃ → ~200 ℃) where Shutdown Cooling System can be initiated

- **Upon operational demand for PRHRS, the MSIVs and FWIVs should be closed and the inlet and outlet valves of the PRHRS should be opened to start the natural circulation**

- **Natural circulation path established through the tube side of the SGs between the SG and the condensation heat exchanger in Emergency Cool Down Tank (ECT) due to the density and elevation difference between the two locations**

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

5. Typical Failure Modes of Passive Systems

❑ **Natural Circulation with Active Actuation**

1. **Actuation failure (automatic and manual backup)**

   - Isolation valves or inlet/outlet valves in the system boundary fail to open or close resulting in failure to establish natural circulation loop

   - Support system (e.g., AC or DC) fails to provide motive power

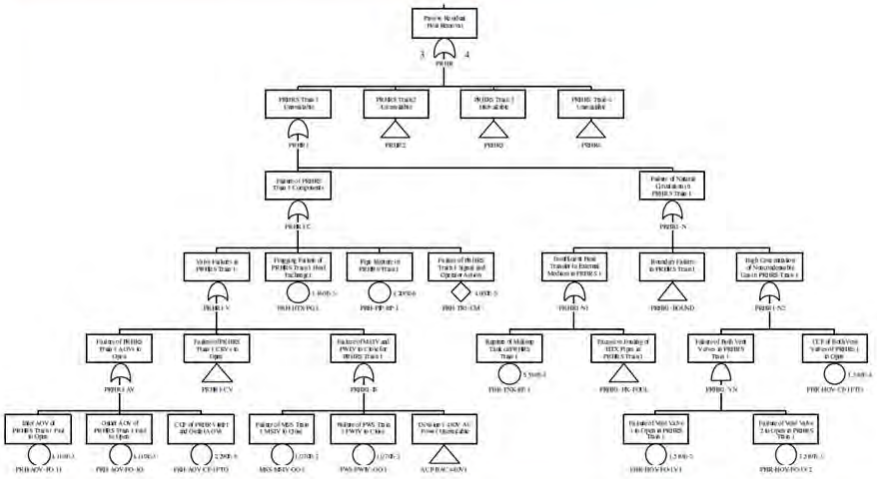
2. **Failure to continue to operate, i.e., degraded or failed natural circulation**

   - Component or boundary failure (e.g., pipe rupture, tank leakage)

   - Flow blockage or degraded heat transfer (e.g., heat exchanger plugging due to corrosion product or foreign material, excessive fouling of heat exchanger pipes, accumulation of noncondensable gases)

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

6. Fault Tree Model for PRHRS Failure



7. Preliminary Quantification Results

- **Too low PRHRS unavailability (i.e., 7.6E-7) was obtained for the baseline case**
- **Representative Minimal Cutsets for PRHRS Failure**

No.	Prob./ Freq.	Basic Event	Description	Event Prob.
1	1.20E-08	ACP-BAC-LP-480V2	480V AC Bus 2 Fails	1.04E-05
		PRH-AOV-FO-1O	Outlet AOV of PRHRS Train 1 Fail to Open	1.11E-03
9	1.10E-08	ACP-BAC-LP-480V2	480V AC Bus 2 Fails	1.04E-05
		MSS-MSIV-OO-3	Failure of MSS Train 3 MSIV to Close	1.07E-03
21	1.40E-09	PRH-AOV-FO-2I	Inlet AOV of PRHRS Train 2 Fail to Open	1.11E-03
		PRH-AOV-FO-3O	Outlet AOV of PRHRS Train 3 Fail to Open	1.11E-03
		PRH-AOV-FO-4I	Inlet AOV of PRHRS Train 4 Fail to Open	1.11E-03

8. Preliminary Results of the Regulatory PSA Model

❑ **Quantification Results**

	Base MPAS	
SMART Initiating Event	CDF (/ry)	% of Total CDF
General Transient (TRAN)	1.88E-06	3.8%
Small Loss of Coolant (SLOCA)	1.11E-05	22.5%
Steam Generator Tube Rupture (SGTR)	9.48E-08	0.2%
Loss of Offsite Power (LOOP)	7.52E-06	15.2%
Loss of Feed Water (LOFW)	2.49E-05	50.5%
Feed Water Line Break Upstream of FWIV (FWLB-U)	1.73E-06	3.5%

❑ **Current Issues**

- **Modeling of Shutdown Cooling System following operation of PRHRS**

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY

9. Concluding Remarks

❑ **Several insights and key issues have been identified with referring available recent safety guides or requirements**

❑ **Development of the preliminary regulatory PSA model**

- **The preliminary evaluation of PRHRS**
- **Quantification results from our preliminary analysis**

❑ **Considerable change is expected of these risk characteristics for the SMART reactor as the PSA model becomes further refined reflecting specific design details as they become available.**

한국원자력안전기술원 KINS KOREA INSTITUTE OF NUCLEAR SAFETY


Thank You.

Use of PSA in the Development of SMRs

Andrea Maioli, David J. Finnicum, Robert H. Lichtenstein, Stephanie Y. Harsche

WESTINGHOUSE ELECTRIC COMPANY LLC, 1000 WESTINGHOUSE DR., CRANBERRY TOWNSHIP, PA 16066, maiolia@westinghouse.com

Abstract

*Advanced reactor designs such as the **AP1000®**[2] plant made significant use of risk-information and Probabilistic Safety Assessments (PSA) to support the design phase and enhance their safety characteristics. PSA is now expected to play an even more prominent role in the design of advanced reactors of the next generation.*

*Most recently, the International Reactor Innovative and Secure (IRIS) reactor piloted a more intimate approach to PSA in the design phase, labelled Safety-by-Design™ PSA was used as an integral tool in assisting the designer in reaching an estimate Core Damage Frequency (CDF) in the range of 1.0E-08. The experience gained from the **AP1000®** plant and the IRIS is now being applied to the new Small Modular Reactor (SMR) currently under development in Westinghouse.*

The use of the risk insights obtained from present day PSA models have been helping to avoid some design problems of earlier plants. The use of the risk insights is beneficial in providing guidance in system design, plant layout, selection and design of major equipment. The review of past operational risk is factored into the design of new plants to eliminate or reduce risk in each operating state. Beyond being a mere design assisting tool for early identification of vulnerabilities, PSA is expected to have a broader impact. Leaving the familiar berths of the well known Light Water Reactor (LWR) technology, for which there are essentially historical and well rooted basis for the definition of the design and licensing basis accidents, PSA is a potential tool to assist in a new and systematic approach for the identification of such design/licensing basis. Such methodology has been conceptually defined in the ANS design standard 53.1 for high temperature gas reactors but with a technology neutral focus.

The ability of having the chance of make risk-informed considerations on a brand new design, when much more degrees of freedom are available to the designers, opens the possibility of envisioning new and bolder risk-informed applications that may require diverse consideration. The pristine example for that is probably associated with the possibility of risk-informing Emergency Planning requirements. Such risk-informed application was investigated for the IRIS design and is currently a hot topic in the ANS presidential commission on SMRs.

The new potential scenarios in which PSA is envisioned to provide support to the design of SMRs also bear challenges such as the applicability of currently used risk metrics (such as CDF) and of the standards that have been so far developed to support PSA modeling for the current fleet of operating reactors. The necessity of providing new metrics is a topic that is currently being discussed.

---

[2] AP1000 is a trademark or registered trademark in the United States of Westinghouse Electric Company LLC, its subsidiaries and/or its affiliates. This mark may also be used and/or registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

This paper reviews the potential new scenarios where PSA may be of significant support to design and operation of SMRs; it reviews Westinghouse's experience and lessons learned in this endeavour and will discuss related challenges and what the PSA community is currently developing to address them.

Keywords PSA, SMR, Design, Risk

1. Introduction

Risk-informed design through Probabilistic Safety Assessment (PSA) techniques has been playing a key role in Westinghouse approach to the development of new nuclear power plant designs. Risk insights support the design from the initial requirement definition phase to a continuous risk assessment of multiple design alternatives through both safety and reliability metrics.

As each new design builds on the lessons learned from the previous generations of nuclear plants, the use of risk information and of PSA techniques during all design phases also uses previous experience to provide a more effective and comprehensive input to the design of safer nuclear power plants.

The design of the most recent Westinghouse Small Modular Reactor (SMR) will take credit of risk-informed frameworks currently being defined for the next generation of nuclear plants and it is now using risk-informed approaches and processes initially developed during the design of the **AP1000**® plant and then further enhanced during the preliminary design of the IRIS reactor. At the same time, the SMR design is transitioning even further away from the classical Pressurized Water Reactor (PWR) characteristics; this will place the SMR design in an intermediate position in which some of the currently recognized PSA concepts will be likely challenged.

Finally, the SMR design will pursue new risk-informed applications, only available to new plants, such as risk-informed emergency planning, which will likely require new methods, new standards, and a licensing framework capable to accommodate such new concepts.

The risk-informed approach to the design of the Westinghouse SMR is a challenging new chapter of the use of PSA in the design phase of nuclear reactors.

2. Westinghouse smr preliminary design

The Westinghouse SMR (Figure 1) is a 200 MWe class, integral Pressurized Water Reactor (iPWR) with all primary components located inside the reactor vessel. Passive safety systems and proven components, based on the Westinghouse **AP1000**® plant design, are incorporated throughout to achieve the highest levels of safety and to reduce the number of components required. The passive safety systems for the SMR allow for no operator intervention required for 7 days.

The fully modular constructed Westinghouse SMR containment vessel has a height of 89 ft and an outer diameter of 32 ft. The reactor vessel has a height of 81 ft and an outer diameter of 11.5 ft. The reactor core is composed of 89 fuel assemblies from the partial-height of the 17x17 fuel assembly design used in the **AP1000**® reactor. Further based on the **AP1000**® plant design, the reactor vessel internals are modified for the smaller core and to provide support for the internal control rod drive mechanisms. Eight (8) proven, horizontally-mounted axial-flow pumps provide the driving head for the reactor coolant system while eliminating the need for pump seal injection. The recirculating, once-through, straight tube steam generator design achieves a compact physical envelope with an innovative approach to steam separation. Finally, the pressurizer is integrated into the reactor vessel head to eliminate the need for a separate component.

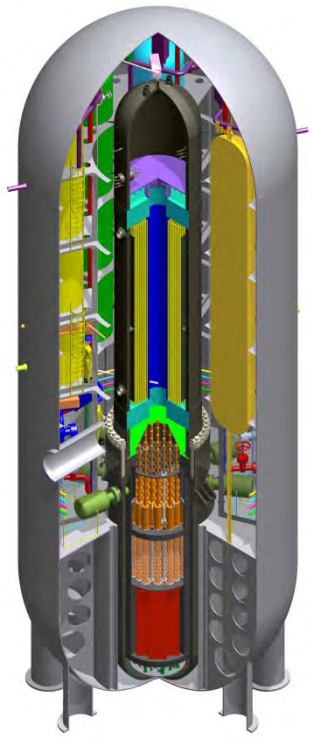


Figure 1. Westinghouse SMR Model

2.1 SMR Risk-Informed Design Framework

A Risk-informed design approach is not only a matter of initiating the PSA at the very beginning of the design phase and constantly provide risk monitoring of the design alternatives; it also and overall implies an iterative, structured and close interaction between the PSA team and the design and safety analysis team. In addition, a structured framework is required in which the risk-information can be gauged with potentially changing ultimate design goals. As a result of this structured interaction, two somehow different points of view on the design (probabilistic and deterministic) are coupled and harmonized, with a significant benefit in terms of overall plant safety.

The most complete and comprehensive risk-informed design approach is probably described in the ANS draft standard for Nuclear Safety Criteria and Safety design process for Modular Helium-Cooled Reactor Plants (ANS- draft). While still not formally approved and explicitly dedicated to the gas technology, the draft ANS standard contains a technology neutral approach to risk-informed design that is very applicable to designs such as iPWRs, for which classical design basis accidents may or may not be applicable depending on how the characteristics of each single design push them towards more innovative solutions.

The ANS 53.1 approach is based on a balanced deterministic and probabilistic interaction that starts with the definition of a set of Frequency vs. Consequences acceptance criteria and curves which are deduced from Top Level Regulatory Requirements. Such Farmer's curves are used to classify events into unacceptable and acceptable and, within this last category, differentiate between anticipated operational occurrence, design basis accident and beyond design basis accidents. The subsequent design development and safety analysis phases are in this way constraints into a well structured framework.

The ANS 53.1 draft approach aligns very well with the envisioned NRC approach for the review and licensing of iPWRs, as for example described in a recent position paper by the NRC (Magruder, 2011) that will gauge the review level of System Structures and Components (SSC) based on their safety and risk significance.

Figure 2 describes the still in draft approach to risk-informed design described in ANS 53.1.

In addition, the framework provided in the ANS draft standard allows for a consistent approach to risk-informed applications; for example the risk-informed emergency planning, which is envisioned as one potentially key aspect in the overall success of iPWR. This framework, in other words, provides discipline to the process of using risk-insights in the design phase, which will allow risk insights to play a broader role than what was possible so far.

The Westinghouse SMR risk-informed design approach will follow, as applicable, the concepts of the draft ANS 53.1 design framework.

3. Risk insights supporting design requirement definition

The Westinghouse SMR is still in its initial design phase, in which the conceptual design is proceeding in parallel with the definition of the Frequency vs. Consequences acceptance criteria, nevertheless risk-insights are being already used to influence the initial thought process, similarly to what has been done for other Westinghouse designs.

The design of the AP600 (and consequentially of the **AP1000®** plant) for example, benefited from PSA insights even before the actual design was conceived. Westinghouse investment in passive plant technology coincided with the beginning of wide spread use of PSA among the nuclear fleet, in response to Unite States Nuclear Regulatory Commission (US NRC) Generic Letter (GL) 88-20. In the requirement definition phase of the AP600, PSA insights from the existing fleet of operating reactor were reviewed with the goal of tackling directly in the design phase the common vulnerabilities of the classical PWR design which started emerging along with the results of GL 88-20 responses. The AP passive design concept stemmed, among other things, by such review of risk insights (Lutz, 2009).

Early risk insights from the existing fleet showed how reliance on either offsite or onsite ac power sources to operate pumps to provide decay heat removal from the reactor core following an initiating event resulted in loss of offsite power with failure of the onsite emergency diesel generators accounting for up to 50% of the Core Damage Frequency (CDF). Similarly, reliance on continued cooling of reactor coolant pumps (RCPs) to prevent pump seal failures that lead to rapid losses of reactor coolant system (RCS) inventory resulted in the RCS inventory loss through the RCP seals following a loss of all seal cooling being a significant contributor to core damage for station blackout events as well as fire initiated events. RCP seal failures account for up to 50% of the CDF for internal initiating events for conventional plants and a significant contribution to CDF from fire initiating events.

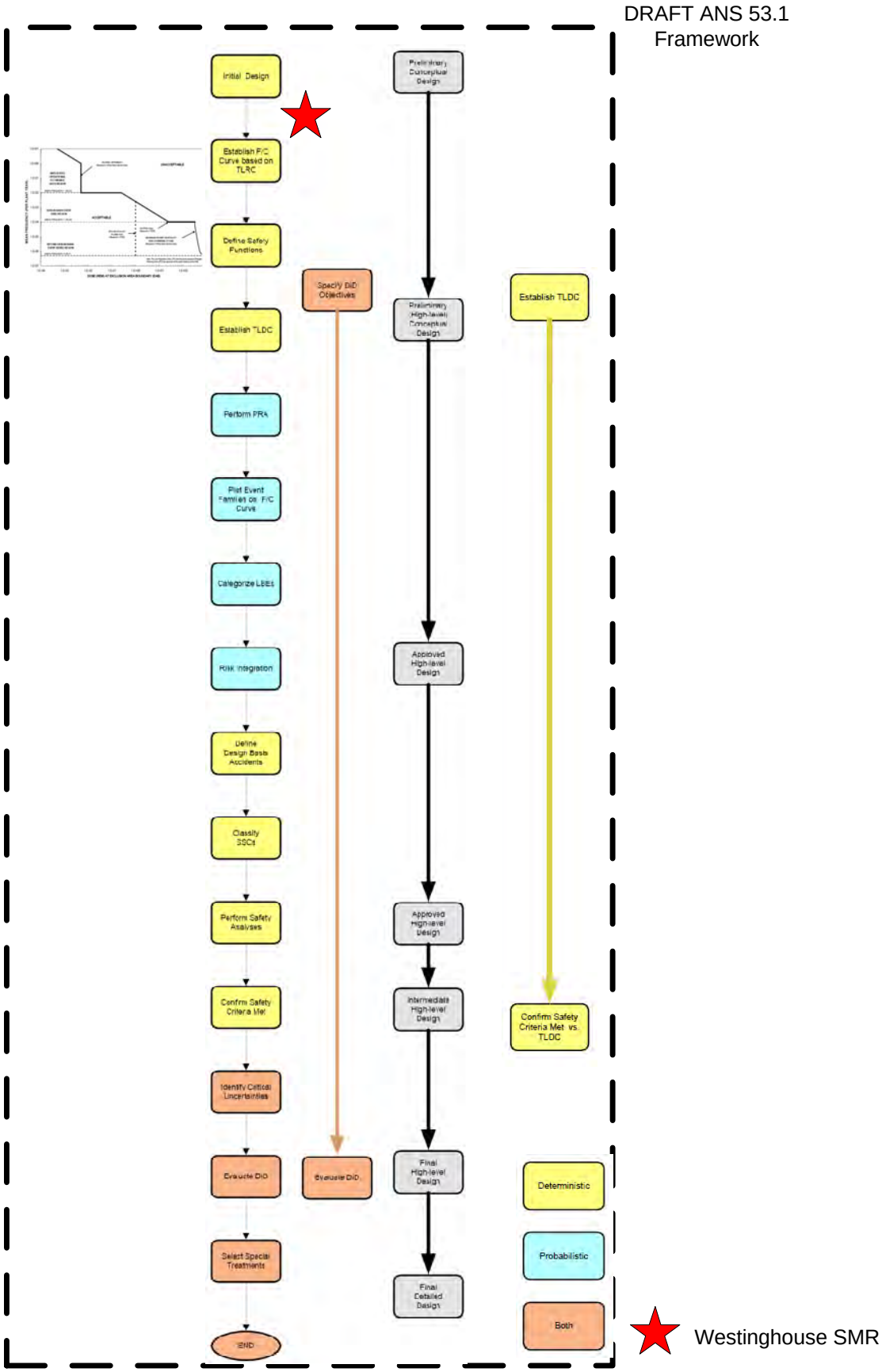


Figure 2. ANS 53.1 risk informed design framework for SMR

Reliance on pumps to provide water for long term heat removal means for example that the Emergency Core Cooling System pumps are required to operate for the duration of many loss of coolant accidents (LOCAs) to continually provide cooled water to the core. In addition, auxiliary feedwater pumps are required to operate for the duration of an event for small LOCA and non-LOCA accident conditions. Pump failures, either failure of pumps to start or failure of the pumps to complete their mission time, account for up to 50% of the CDF for some conventional plants.

Such risk insights, among others, drove AP design requirements towards passive characteristics such as:

- Minimal Reliance on Offsite Power for accident mitigation: the front-line accident mitigation for the **AP1000®** plant design is independent of AC power. Accident response does not rely on sources of pumped water for decay heat removal. There are no emergency diesel generators in the **AP1000®** plant design for accident mitigation but rather the diesel are used as a defense in depth system.
- Minimal Reliance on Pumped Decay Heat Removal: The Passive Core Cooling System is comprised of Core Makeup Tanks, Accumulators and an In-containment Refueling Water Storage Tank (IRWST) that passively provide water to the reactor core using processes that are governed by the natural laws of physics. No pumps are required for long term decay heat removal if diverse and redundant valves are opened upon automatic signals. Again pumps are provided as part of a defense in depth system which reduces overall plant risk.
- Elimination of Reactor Coolant Pump Seals as a Source of RCS Inventory Loss: The **AP1000®** plant design features reactor coolant pumps that have no seals that can fail and result in a loss of reactor coolant. As a result, accident sequences that do not result in ADS actuation do not rely on RCP seal integrity for success.

Similarly, for the current phase of the design of the Westinghouse SMR, PSA analysts are ensuring that the plant is designed for initiators that dominate the present day reactor CDF. Design provisions derived from PSA insights from the current fleet again include strategies for mitigation of loss of offsite power coincident with a failure of emergency power, for which availability of critical valves to properly align is essential even in a passive safety system design. To this end, design requirements at the system level are being derived to ensure that a fail safe approach is always adopted, this includes solutions such that critical valves be air operated rather than motor operated and potentially include local air accumulators which will ensure availability with limited requirements on emergency batteries. This approach reduces the need for a large number of batteries and the required support systems. Additionally, it potentially allow for redirection of the battery to power other critical loads for a longer time period.

At this stage of the design, a complete PSA model that can be used for estimating CDF or release frequencies metrics is still not feasible; still, PSA techniques can be used to help shape beyond design strategies that may be available or not depending on the design of the principal front-line safety systems explicitly dedicated to accident mitigation. In the design of the IRIS reactor, PSA was used in this phase through the use of simplified Event Trees. The initial lack of details related to system performance and general success criteria induced the adoption of the concept of "bellwether sequences" to sanity checks the sequence analysis. A "bellwether sequence" is a core damage sequence that reflects a key simplifying assumption. These sequences typically involve only an initiator and one system failure and the associated core damage frequency can be estimated by a preliminary hand calculation. The hand calculation of the frequency provides a quick check on the potential impact of the simplifying assumption on overall core damage frequency. If the impact is felt to be large enough to be of concern, the assumption and associated sequence are examined in more detail to determine if additional mitigation paths could be credited, additional best estimate TH analyses would be needed to revise the assumption, or the assumption is appropriate. For the

last condition, designers could then determine if the preliminary design is acceptable at the present point of the design phase.

Simplified Fault Trees can also be used to evaluate high level system alternatives and system success criteria. The simplified FTs are quantified with the only scope of having system level cutsets that can systematically provide system weak links.

4. Continuous design risk monitoring

The classical use of PSA within the design phase is centered on a continuous monitoring of the design against established classical quantitative risk metrics such as CDF and various release frequencies. To be able to enter in this phase of the PSA support to the design, a somehow complete preliminary design needs to be reached. Depending on the design stage, an extremely simplified FT modeling of support systems is used. The complete, even though simplified, PSA model allows at this point for a more comprehensive risk monitoring of the design by tracking intersystem dependencies that cannot be easily tracked in a single failure criterion approach.

Risk insights through explicit modelling of the AP600 and **AP1000®** plant design targeted for example classical high risk contributors such as common cause failure events and human action failures. The current reliance on human actions as part of the accident mitigation strategies to provide long term core cooling results in a potential decrease of CDF by over 200% for some conventional plant assuming that all human actions can be considered perfectly reliable. Reliance on redundant trains of safety systems with identical components results in common cause failure accounting for as much as 5% of the total CDF at some conventional plants.

The **AP1000®** plant design has benefited from these insights by achieving a significant reduction in Common Cause Failures (CCF) affecting the Dominant Risk Mitigation Features. The Passive Core Cooling System (PXS) uses diverse components where it has been shown to be risk significant. In addition, the ADS has four separate stages with built-in diversity. The potential for common cause failures to disable the safety systems is therefore greatly reduced or eliminated. The **AP1000®** plant design uses a digital system for the protection I&C. Such a system has a potential for CCF due to both hardware and software. The probability of such failures is reduced by extensive verification of the system. In addition, a separate diverse I&C system is designed to provide actuation functions that are risk important in the unlikely CCF of the protection I&C system.

Finally, AP600 and **AP1000®** plant aredesigned to have minimal reliance on Operator Actions. The operation of the front-line accident mitigation systems requires no operator intervention for success. Successful short term and long term core cooling is accomplished by automatic means to depressurize the RCS using the ADS and to initiate passive cooling using either recirculation between the RCS and the IRWST. While over 60 operator actions are credited in the **AP1000®** plant PRA, they involve actions to prevent an event form progressing to an accident conditions or they involve actions to mitigate an accident in which the front-line systems have failed to perform their function.

Seven major PSA quantifications have been performed on the AP600 for CDF and Large Release Frequency (LRF), while one major quantification has then been performed on the **AP1000®** plant design. During each of these quantifications, the PSA results were reviewed for potential modifications. Many design and operation changes have been made based on these PSA insights, especially during the earlier AP600 quantifications, resulting in classical safety metrics of the **AP1000®** plant design (CDF and LRF) being roughly two orders of magnitude lower than the existing fleet.

The evolution of PSA techniques and the definition, in the early 2000s, of industry standards for PSA development coincided with Westinghouse's involvement in the development of the

conceptual design of the IRIS reactor, for which lessons learned from the **AP1000®** plant design experience were used to make PSA an essential tool in the IRIS Safety-by-design philosophy. The risk-informed design approach applied for the IRIS reactor (Maioli, 2005) was therefore envisioned as a more intimate and continuous interaction between the design team and the PSA team, with a more structured feedback from the PSA to the design side. In this approach, PSA results have a more direct influence on the plant design, rather then simply following its development.

The main "drawback" of such an approach is that probabilistic studies need to be initiated at a very early stage of the design, when several required design information may only be partially or qualitatively available. This requires a more flexible approach to probabilistic analysis than used in the past and, especially, results in a relevant number of assumptions, which importance in the risk assessment is well beyond what is currently handled in a PSA for operating plants. A fundamental part of using PSA in the initial design stage was therefore the documentation and monitoring of all these assumptions for further analysis and confirmation of their actual applicability.

An IRIS PSA Assumptions Database was developed and was the primary qualitative tool used to store and document all the foreseen source of uncertainties: to each assumption added to the database, an associated degree of uncertainty was added, which was connected with the kind of design or analysis information that was still required. The database, as well as the uncertainty degree of each assumption, was continuously updated as the development of the design makes further IRIS-specific information available

While this was a continuous process, it could be divided in phases, each phase focused on one of the major assumptions categories. The IRIS internal events CDF history summarized in Fig.3 shows the iterative relationship between the PSA and the design team, which is evident in the spikes in the CDF that can be seen after the dramatic reduction of the initial values due to the first iteration, which corresponded to the system requirement definition phase. CDF changes are usually due to the PSA model being updated and refined; such refinements can bring light to some new issues to be discussed and addressed with the design team and to additional details added to the initially simplified model. The most visible change in Fig.3 is for example due to the Human Reliability Analysis (HRA) that, along with the implementation of several design modifications identified during the first PSA iteration, was one of the main areas of work during the second phase of the IRIS PSA development.

The PSA analyst supporting the design can by use of his experience add value ensuring that the expected operator actions are achievable within the required timeframe. Also the analyst can ensure that the action is one that the operator would indeed perform. This is obviously done before any plant procedures have been developed.

The importance of assumption treatment, identification, and their link with model uncertainties is now even more recognized by PSA practitioners, even for the operating fleet. The development of the Westinghouse SMR is therefore adopting a similar approach in the identification and tracking of assumptions and the associated induced model uncertainties. The new SMR PSA assumption database is going to be directly derived from current PWR Owners Group (PWROG) activities aimed at the identification of model related uncertainties.

Finally, beyond its contribution in defining the design concept and philosophy and monitoring the design evolution through risk based measures, PSA will be used to support availability/reliability programs in a fashion similar to what was done for the AP design, for which Fault Tree modeling of systems unique to the AP design supported the reliability and availability programs aimed at satisfaction of the United States Advanced Light Water Reactor Utility Requirement Document (ALWR URD) and European Utility Requirement (EUR) targets for plant availability. As result of such activities, critical equipment has been identified and ranked through the availability models

and appropriate reliability target have been consequentially set to drive the **AP1000®** plant availability well above the targets set by both the US ALWR URD and the EUR (Anderson, 2009).

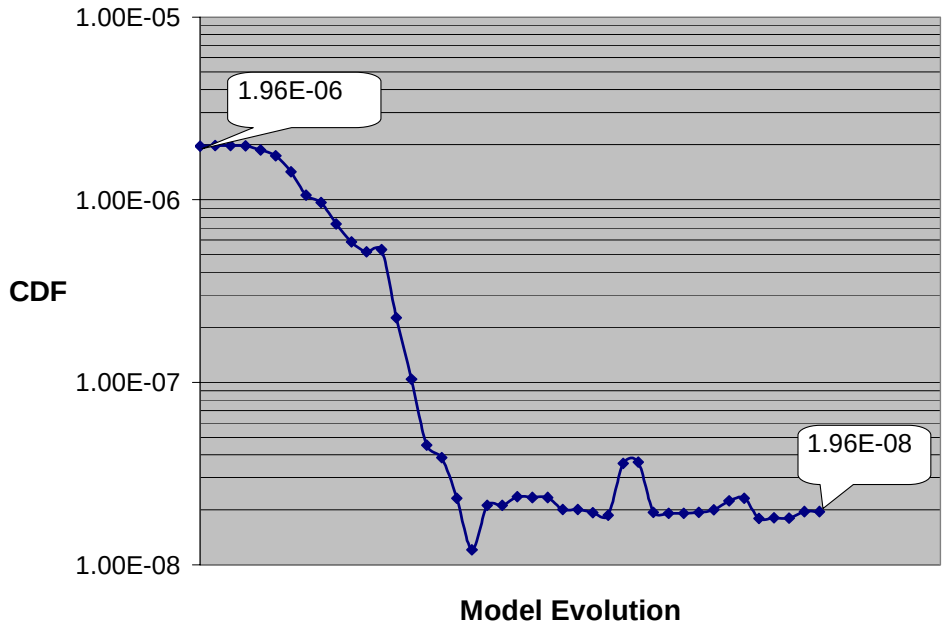


Figure 3. IRIS CDF evolution with the design

5. Challenges to use of psa in design phase

As mentioned, the main challenge in the use of PSA techniques to support the design phase of a nuclear plant is the lack of information, which exponentially increases the uncertainties associated to any quantitative risk measure that can be associated to an early design. Under this point of view, the risk-informed framework suggested in ANS 53.1, as described above, appears essential. The initial risk-based values, as provided by the PSA team in the requirement definition phase or in the initial design support, are significant only in the fact that allow for tracking what potential event is going to be a design basis accident rather than a beyond design accident and whether any design alternative initially considered becomes vulnerable to unacceptable events in the Frequency vs. Consequence curve.

With the evolution of the design, as more information comes to be available, risk metrics become more realistic but they still need to be closely watched for the associated model uncertainties. The assumption/uncertainty database is going to track design alternatives in the form of different Event Trees or different Fault Trees explicitly modeled in the PSA, which will identify the uncertainty bounds for CDF and release frequency values.

Another challenge to the use of PSA in design phase is the lack of a recognized standard against with to compare the technical adequacy of a PSA developed for a non-operating reactor, this in the view of the fact that the current ASME/ANS standard is dedicated to operating reactor and has requirements that are clearly not applicable until operation of the plant has commenced. Additionally, PSA standards already published only address Level-1 PSA (i.e., up to CDF evaluation with limited release frequency considerations) and do not address yet Level 2 (full scope release frequency assessment) or Level 3 (risk impact to population). To address this challenge, the ANS/ASME Joint Risk Management Committee which maintains PSA standard, is developing a technology neutral standard that would span from the initiating event definition to risk to the population (thus bypassing the concepts of Level 1, 2 and 3 PSA, which are tailored against the

light water technology and may not be able to accommodate different kind of designs). The technology neutral PSA standard (know as the Non-LWR PSA standard) is in its final stage of development and ready for public comments.

Finally, risk-informed applications exclusively dedicated to new design, such as risk-informed emergency planning, have been discussed for SMRs. While the technical feasibility of a risk-informed methodology has been addressed in multiple examples (see for example IAEA, 2010), there are challenges in the PSA application associated with such endeavour, such as the need for a full scope internal and external event PSA, which appears necessary. Current designs that have used PSA as support, have limited such support to internal events and have only used limited insights as far as external events (mainly seismic) are concerned (Kumagai, 2007); this has the potential to result in new design being extremely robust as far as internal events are concerned, and then being completely dominated by external events as far as the risk profile is concerned. While innovative design solutions are possible in an early design stage to cope with extreme events, the need for integrating external events considerations on a probabilistic basis at a relatively early design stage is going to be another challenge for effective and balanced use of PSA as a support of the design phase.

6. Conclusions

PSA is playing and will play a significant role in the design of the Westinghouse SMR. Lessons learned from use of risk-information in the design of the AP600 and **AP1000**® plant and of the IRIS conceptual design are being applied. In addition the experience of the PRA analyst will add insights from design and operation of present day nuclear plants.

In addition, the PSA community is gearing up with guidance such as the ANS 53.1 and the Non-LWR PSA standards, which will allow the development of new design to benefit from risk insights in an unprecedented manner. Still, significant challenges are expected on the path.

7. References

ANDERSON R.G. et. al. (2009), AP1000 Plant Availability Analysis in Accordance with the EUR, In proc: ICONE 2009, Brussels, Belgium, paper 75415

ANS Draft, 53.1, Nuclear Safety Criteria and Safety Design Process for Modular Helium-Cooled Reactor Plants

IAEA (2010), TECDOC-1657, Small Reactors without On-site Refuelling: Neutronic Characteristics, Emergency Planning and Development Scenarios.

KUMAGAI Y, et. al. (2007), PRA-Based SMA: the First Tool toward a Risk-Informed Approach to the Seismic Design of the IRIS, Journal of NUCLEAR SCIENCE and TECHNOLOGY, Vol. 44, No. 10, p. 1268–1274 (2007)

LUTZ R.J. et. al. (2009), Use of PRA in the Design of the Westinghouse AP1000 Plant, In Proc: ICONE 2009, Brussels, Belgium, paper 75408

MAGRUDER, S. (2011), Use of Risk Insights to Enhance safety Focus of Small Modular Reactor Reviews, In Proc: ICAPP 2011, Nice, France, paper 11454.

MAIOLI A. et. al. (2005), Risk-Informed Design Process of the IRIS Reactor, In proc: ANS PSA 2005, San Francisco, CA.

Use of PSA in the Development of SMRs

Andrea Maioli, David Finnicum, Robert Lichtenstein and Stephanie Harsche
Westinghouse Electric Co, LLC

OECD / NEA Workshop on
PSA for New and Advanced Reactors
June 20 – 22, 2011
Paris, France

Westinghouse

1

Background

- Probabilistic Safety Assessment (PSA) is an integral part of the design and regulatory licensing of the new and advanced reactors.
- Traditional PSA analyses are done for operating plants where equipment and procedures are well known and an operating history is available.
  - Challenges in using PSA in the design phase
  - New risk metrics, new risk-informed applications, larger scope

Westinghouse

2

Use of PRA in the design
The Westinghouse AP1000® Plant

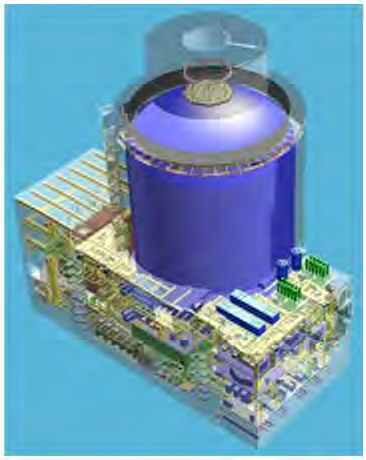
- PRA techniques have been used from the very beginning of the design phase of the AP1000® plant
- Risk-insights from PRA of existing fleet used for identifying major risk-contributors
- Risk-significant contributors have been engineered out of the design
- Design alternatives analyzed through PRA to identify impacts in CD/LRF space

Westinghouse

3

Use of PRA in the Design of AP1000® plant
Risk insights from existing PWR

- Loss of offsite power and failure of Emergency Diesel Generator account for up to 50% of CDF in some existing PWR
- Loss of Service water and Component Cooling water as IE account for 25% of CDF in some existing PWR
- RCP seal failure accounts for up to 50% of CDF in some existing PWR
- ECCS pump failure (to run or to start) following a LOCA accounts for up to 50% of CDF in some existing PWR
- Reliance on identical redundant trains: CCF can account for up to 5% of existing PWR CDF



Westinghouse

4

Use of PRA in the Design of AP1000® plant Risk beneficial design solutions

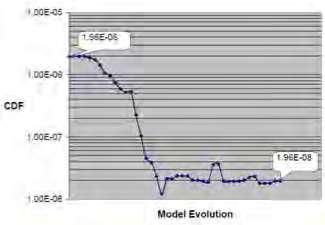
- Minimal reliance on offsite power, service and CCW for accident mitigation (passive safety systems)
- Elimination of RCP seal LOCA scenario (canned pumps)
- Minimal reliance on pumped decay heat removal
- Elimination of CCF through diverse strategies
- CCF of I&C addressed in the design
- Minimal reliance on operator action (CDF can decrease 200% in conventional plants when operator actions are assumed perfect)
- In-vessel retention reduces uncertainties in containment behavior

Westinghouse

5

Westinghouse experience in using PSA in design phase – IRIS

- IRIS employed a more extensive and participative PSA approach to the design
  - Continuous iteration PSA/design team
  - Initial CDF goal drove the design of ESF and support systems
  - Initial considerations on "beyond level 1" PSA (e.g., seismic isolation to address seismic-related risk)
  - Risk-informed emergency planning zone redefinition effort required Level-2/3 kind of considerations and risk-informed licensing considerations.

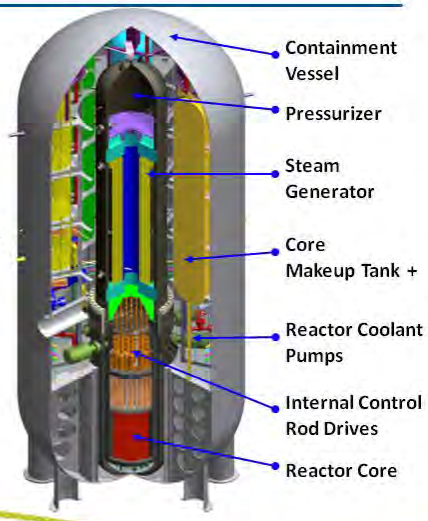


Westinghouse

6

Westinghouse SMR Basic Concepts

- 200 MWe class
- Integral PWR (iPWR)
- Classical PWR concept
- Straight-tube steam generator
  - Flow from top to bottom of tubes
  - Hot leg located in center of bundle
  - Recirculating steam generator with steam/water mixture delivered to steam drum outside containment



Westinghouse

7

Ongoing Risk-Informed Design of the SMR

- Use of Risk-insights in design goes way beyond the development of PSA at the early stage of the design phase
- A risk-informed framework needs to be developed within which the PSA and the resulting risk insights can be used in the decision making process at various stages of the design
  - Track risk objectives (driven by application and different regulatory environments)
  - Track risk profile (driven by design evolution and refinement)

Westinghouse

8

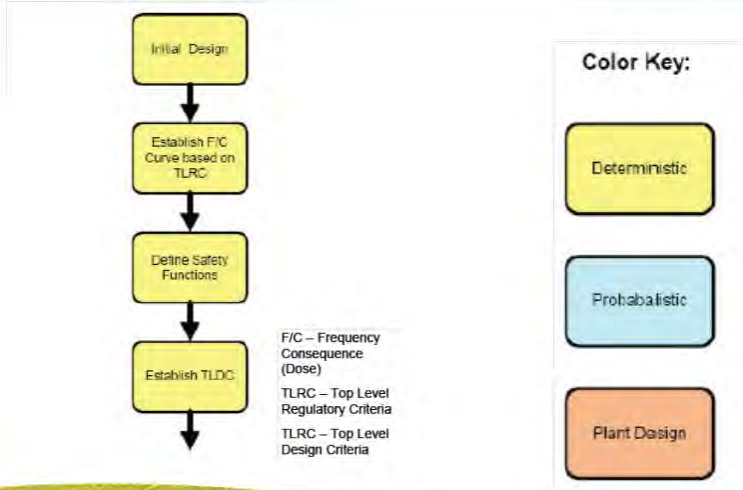
ANS 53.1 Risk informed design concept

- ANS 53.1 - Nuclear Safety Criteria and Safety Design Process for Modular Helium-Cooled Reactor Plants
  - Currently in draft form
  - Technology neutral Risk-informed design procedure
- Concept applies to the design of new advanced iPWRs that differ significantly from current (A)LWR
- Support risk-informed applications that may be beneficial for SMRs such as risk-informed emergency planning

Westinghouse

9

ANS 53.1 Deterministic phase

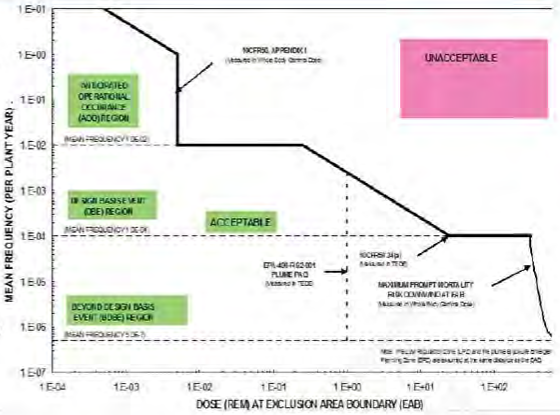


Westinghouse

10

ANS 53.1
The framework

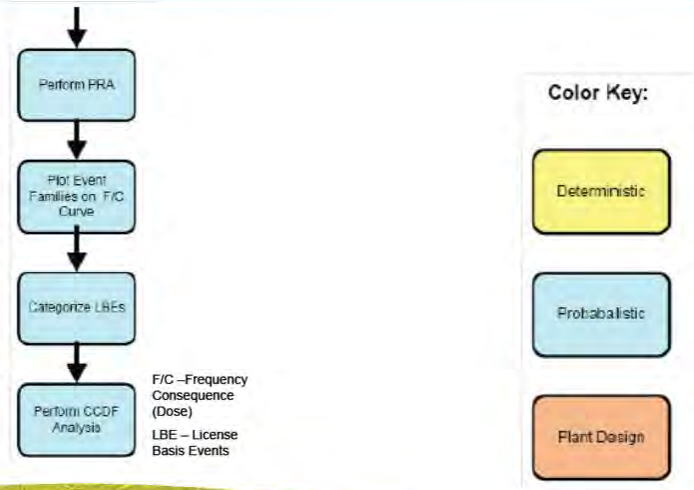
- C/f curve
- Map events during design
- Defines DBA and BDBA
- Set long-term goals for applications (emergency planning)
- Adapt to different regulatory environment
- Help respond to regulatory changes while in design



Westinghouse

11

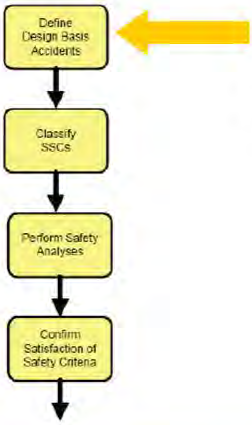
ANS 53.1
Probabilistic phase



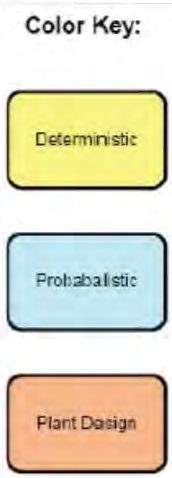
Westinghouse

12

ANS 53.1
Deterministic phase



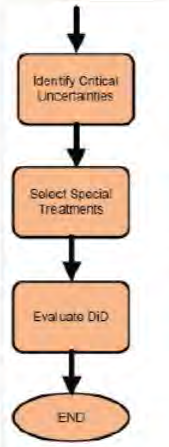
Starting point in the "classic" deterministic design approach



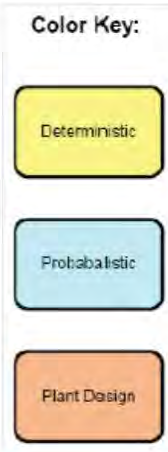
Westinghouse

13

ANS 53.1
Final phase



Special Treatments (Part B):
- Procurement Requirements
- Specifications
- Design Requirements
- Independent verification
- Inspections
- Acceptance Tests
- Surveillance Tests
- Scheduled Maintenance
- Monitoring
- Installation Testing



Westinghouse

14

Use of Risk-Insights in Design Initial Interaction with Design Team

- Conceptual plant design definition
  - The initiating events (i.e., LOCA's, Transients, SBO, etc.) are reviewed for applicability
  - The plant configuration is reviewed for equipment important to PSA based on present day plant risk insights.
  - A strict interaction plan between design and PSA teams is developed for using and developing PSA methods.
- Develop high level event trees
  - Front line systems (i.e., no support systems) are initially considered
- Fault trees for frontline systems (support system treated as black boxes with industry driven reliability data)

Westinghouse

Use of Risk-Insights in Design Current Interaction with Design Team

- Risk-insights from current plants
- Review of initiating events from current plants
- Investigation of new initiating events, specific to the plant design
- PSA engineers experience on maintenance and operability of the plant, beyond safety.

Westinghouse

Use of Risk-Insights in Design Risk Metrics

- CDF/LRF are not of interest in the initial steps of a risk-informed design
  - Extensive epistemic uncertainties due to lack of systems design
  - Area-based hazards (fires and floods) cannot be assessed till later \
  - Generic reliability data applicability to new configurations/components
  - Preliminary HRA
- Staged cutsets review on “lean” models based on the events trees developed

Westinghouse

17

Use of Risk-Insights in Design Challenges

- Maintaining coordination with design and TH team
- Ensuring that design will meet PSA requirements
- Developing success criteria with changing design
- Implementing changes to plant design to incorporate PSA insights (effective feedback to design team)

Westinghouse

18

Use of Risk-Insights in Design Other Challenges

- Epistemic uncertainty treatment
  - Explicit modeling vs. simplified parametric analysis (labor intensive)
  - Alternative system designs and alternative success criteria (at the FT and ET level)
    - Tools and modeling approach limitation: One top models not better suited for this kind of applications
  - Capability Category III analysis of model uncertainties
  - Stochastic uncertainties potentially pointless
- Mapping between assumptions and uncertainties
- Documentation (tracking) of screened out failures modes (e.g., from FMEA)

Westinghouse

19

Use of Risk-Insights in Design Tools and Methods Challenges

- Unique modeling problems due to the design
  - Impact of HRA of improved control system philosophies
  - Success Criteria codes (e.g., MAAP or MELCOR) ability to model other than classic LWR scenarios
  - New Containment/Confinements response and associated reliabilities
  - External events treatment (e.g., Seismic Margin Approach vs. Seismic PRA approach)

Westinghouse

20

Use of Risk-Insights in Licensing Challenges

- Accepted risk metrics
  - Long fuel cycles may make yearly average CDF inaccurate due to failure rate change over mission time and test intervals
  - Site risk metrics (not only for small modular reactors as Fukushima shows) vs. unit risk metrics
- PSA Standard Applicability
  - ALWR applicability of current ASME/ANS Standard (see Tuesday paper)
  - Non-LWR (technology neutral) PSA standard
- New Applications Challenges
  - Risk-Informed EPZ seems to suggest need for Level 3 PSA. How do we factor something like this in a DC/ESP licensing approach?

Westinghouse

21

Use of PSA in the Development of SMRs

Westinghouse

22

ACHIEVEMENT OF THE LEVEL 1 PSA IN SUPPORT TO THE CEA 2400 MWTH GAS-COOLED FAST REACTOR

M. BALMAIN
EDF, R&D Division, Industrial Risks Management Department
F-92140 Clamart, FRANCE
michel.balmain@edf.fr

C. BASSI, P. AZRIA
CEA, Nuclear Energy Directorate, Reactor Studies Department, Innovative Systems Service
CEA, DEN, F-13108 Saint-Paul-Lez-Durance, FRANCE
christophe.bassi@cea.fr

Abstract

Within Generation IV International Forum, the CEA has developed since 2006 a Level 1 PSA to support the design of the 2400 MWth GFR. A first period, with insights published in 2008, consisted in a model with few initiators representative of medium and high pressure situations, those used for the deterministic design of the Decay Heat Removal dedicated loops. In a second period, an iterative work reached the probabilistic targets used for generation III reactors, with prior use of normal loops, and increase of DHR reliability in high pressure conditions. The PSA team covered all the internal initiators, and supported the design of components with instrumentation and control and electrical supplies, and the shutdown operating modes of secondary, tertiary circuits, with possible re-alignment to dedicated DHR loops. Besides, the completed PSA integrated more realistic success criteria than the preliminary model and than the deterministic approach, thanks to CATHARE2 code. In case of loss of Forced Convection, the probability of success of the Natural Convection DHR was assessed by a reliability method for passive systems. The paper underlines the PSA methodology knowledge from the EdF expertise, the improvements co-developed with CEA, and the iteration design-PSA-design.

Key Words: Generation IV – PSA – Methodology - Iteration

1. Introduction

Probabilistic insights are increasingly employed for safety demonstration, at early design stages. Many risk-informed design guidance methodologies were developed to check the balance of a design or to optimize a system of a nuclear plant compared to regulatory criteria (Delanay, 2005). The CEA has developed a Level 1 Probabilistic Safety Assessment on the 2400 MWth GFR concept. From a GFR design referenced as year-2006, the first phase consisted in realizing a L1PSA that only modeled the initiators included in the deterministic design of the DHR dedicated loops (Bassi, 2008). This resulted in proposing additional systems for DHR, and increased redundancy for some components. The final L1PSA covered these new features and extended the perimeter to all initiators. The original specifications of the 2400 MWth GFR concept were driven by the objectives of Generation IV Nuclear Energy System roadmap, which led to the main features: a fast neutron core, a 3 loops helium-cooled primary circuit connected to a Brayton secondary circuit allowing for a high thermodynamic efficiency (Figure 1).

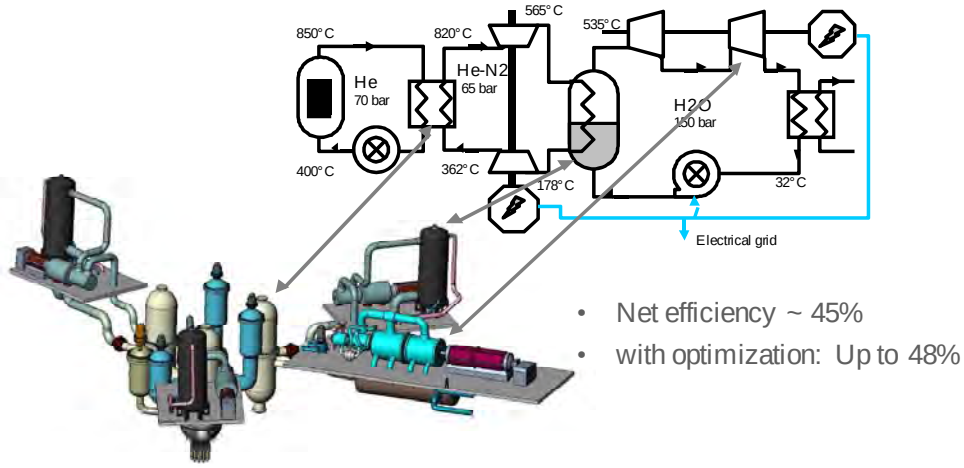


Figure 1. Layout of GFR normal loops featuring a combined Brayton cycle

Reactivity control is derived from the European Fast Reactor project and featuring: the Control & Shutdown Device (12 CSD sub-assemblies for rod group RG1, 12 CSD for RG2) and the Diverse Shutdown Device (5 DSD in RG1 and 4 in RG2). DHR cannot account on conduction or radiation due to: high core power density (100 MW/m3), reduced core thermal inertia compared to high temperature reactors, and reduced coolant thermal inertia compared to Sodium Fast Reactors (Malo, et al., 2008). As helium pressure is fundamental for NC and in pumping power for FC, a specific strategy was selected (Figure 2).

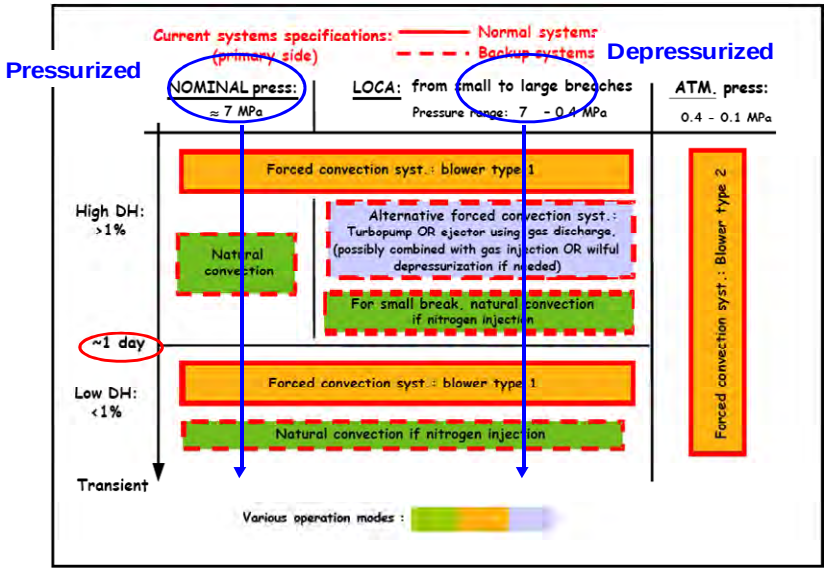


Figure 2. Medium pressure strategy for DHR (0.5 – 1 MPa)

The dedicated loops of the Reactor High Pressure system (Figure 3) allow forced and natural convection, depending on the primary pressure and the decay heat. For intact helium boundary situations and depressurized situations (LOCA), the primary side of the RHP system operates as a first line of provision in FC. If all three blowers fail, the NC becomes the second provision, in only 2 loops (for congestion reasons of the CC, and diversification for earthquakes). For both operating modes, the secondary side retains a passive functioning (NC by a pressurized water coolant, the heat sink being a water pool).

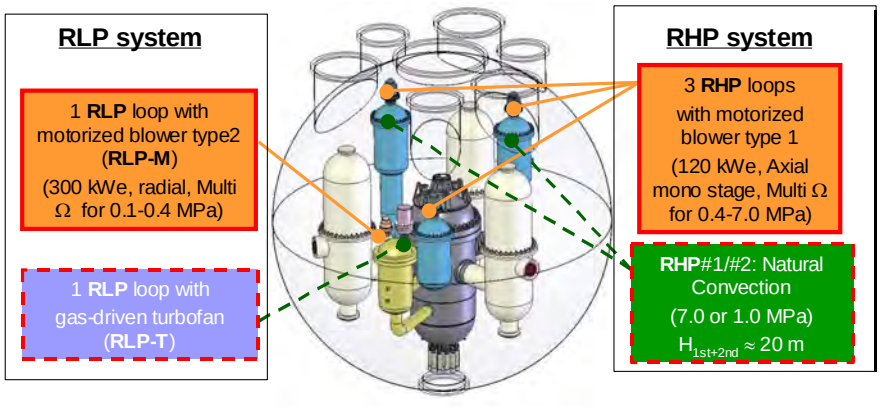


Figure 3. Layout of the DHR systems

Due to the poor thermal-hydraulic features of a gaseous coolant, a metallic Close Containment (guard vessel) is foreseen to keep a pressure allowing a reduced pumping power of RHP blowers in depressurized conditions and also an efficient NC. In normal operation this containment is inertized with nitrogen to avoid air ingress in the fissile region. In case of loss of helium towards the CC, the same strategy for RHP is applied with one difference owing to the low capability of helium coolant at low pressure: injection of nitrogen from tanks in the primary circuit to improve NC performance.

RHP blowers were designed to accommodate a large pressure range between 7.0 and 0.4 MPa, but the combined primary circuit and CC ruptures would drop the pressure below 0.4 MPa. An additional loop belonging to a so-called Reactor Low Pressure system, was designed for this situation. The primary side of this loop provides FC by a motorized blower (running between 0.4 and 0.1 MPa, whereas the secondary side is identical to the RHP ones. Finally, for diversification in case of LOCA (regarding NC uncertainties), an alternative FC mean was designed based on a gas-driven turbofan. To limit penetrations on the reactor vessel, this additional FC means shares its heat exchanger and secondary circuit with the RLP system.

The last point is related to electrically driven valves (EDVs) for isolating the 3 normal and the 4 dedicated DHR loops. At power state, the primary sides of DHR loops are isolated in order to keep a high thermodynamic efficiency and to avoid non-necessary thermo-mechanical strain on DHR heat exchangers. These 4 valves are located on the cold part of the DHR loops cross-duct, for technological constraints. If an event causes RHP blowers start-up, the gaseous features of the primary coolant require the isolation of the normal loops in order to avoid core bypass. As for the DHR loops, these 3 isolating devices are located on the cold part of the main cross-ducts.

Reactivity control is carried out by redundant shutdown devices (CSD and DSD) shared by two rod groups (RG1 and RG2). The mechanical parts of the reactivity control system, as well as scram orders were modeled for consistency of the L1PSA model. Thanks to CATHARE2 the deviation of neutronics and thermal-hydraulic parameters were calculated for each IE (Bentivoglio, 2008). A minimal reactor instrumentation was settled to lead to scram signal. On the basis of the EFR I&C system, two redundant signal processing channels were handled in the L1PSA model, starting from sensors, processing units (with a 2-out-of-3 vote) and ending at breakers for control rods groups delatching. For reliability concern, an optical cross-link between the two channels was retained.

DHR is split over two periods, from IE to 24 h, and from 24 to 168 h, during which front line systems or missions may be different (Figure 2). This choice is related to some systems 24h range, such as batteries and ternary water pools. This needed a specific treatment in the event trees building presented later on.

The GFR present specific risks, namely the need for isolation of the CC (defined as sub-function for NC in case of primary leakage) and the shunning of core by-pass (defined as the sub-function of maintaining a gas convection at core inlet):

· CC integrity. The back-up pressure for NC may be lost: by break in the CC following a SB-LOCA (conventional prob. 1E-7), or by LB-LOCA (1E-6), or by failure to isolate connected circuits (e.g. nitrogen or helium supply),

· Core by-pass pathways. As DHR is based on gas convection, the core by-pass of this light coolant is of major concern, unacceptable in two cases. Firstly after a normal loop EDV isolation failure, if a second one fails to close. Secondly after one DHR loop loss in FC, if it becomes impossible to isolate this loop.

The L1PSA is an excellent mean to account for all sources of dependencies leading to concomitant failure of missions. Besides CCFs, and common parts (as regards to FC and NC), a special attention was paid to the support systems, namely electrical supply and I&C for systems actuation and reconfiguration. The layout is inspired from French PWR of 1300 MWe (Figure 4).

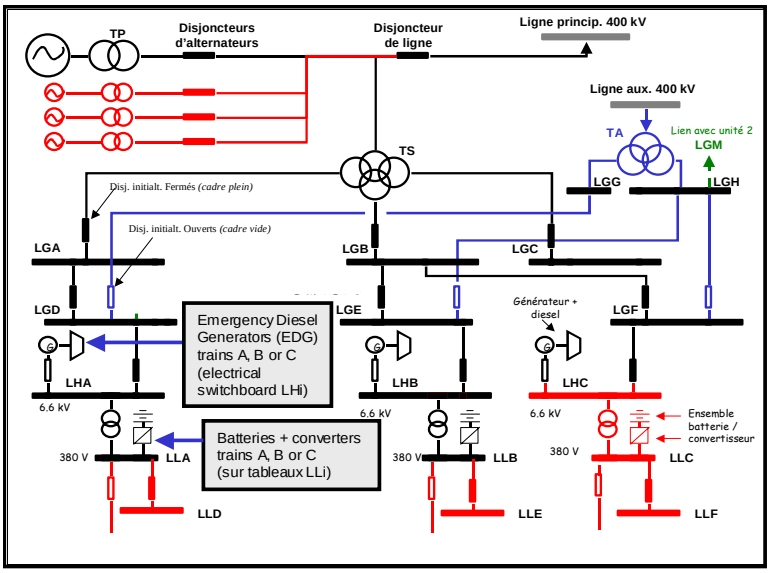


Figure 4. Layout of the electrical supply system

One train supplies all components of one normal and one RHP loop (main blowers, EDV, water pumps, DHR blower). The RLP loop and all isolating devices of the CC, are connected to the third train. As regards to I&C support system, in addition to the reactor instrumentation for scram orders, the concept of two redundant signal channels is retained (without optical cross-link) for reconfiguration after reactor trip.

2. Building process of the preliminary L1PSA model

Three main IEs families were selected: LOCA and LOOP (in order to check the consistency of the DHR systems layout) and spurious reactor trip (similar to LOOP, except control rods already dropped). For this preliminary L1PSA model, the frequencies are based on a review of similar data for other types of reactors (LWR, SFR, HTR) and expert judgment. In addition, in order to mix deterministic and probabilistic approaches, these frequencies are fixed in accordance with the Plant Conditions Categorization (Table 1). The IEs being essential events in a PSA, common to entire groups of sequences, we made a strong assumption of future efforts to reduce uncertainty and respect this specification, then we used a low EF 3.

Table 1. Initiating events frequencies for the preliminary PSA

IE		fq (/y)	
LOCA	Small Break	10^{-3}	Intermediate value of PCC3 [10^{-2}, 10^{-4}]
	Large Break	10^{-4}	Upper value for PCC4 [10^{-4}, 10^{-6}]
LOOP	Short-duration (< 24 h)	10^{-2}	Lower value for PCC2 [1, 10^{-2}]
	Long duration (> 24 h)	10^{-5}	Intermediate value for PCC4
Spurious reactor trip		10^{-1}	Intermediate value for PCC2

A conventional period of 7 days, is retained in relation with the change at 24 hours as defined in the DHR strategy, and the will to handle long-term scenarios following for instance climatic events leading to a long LOOP. In addition, this long mission time gives conservative results for a reactor design still in progress, and a source of margin in design evolution. The Figure 5 presents the event tree developed for a LB-LOCA initiating event. The upper part depicts the systems envisioned to cope with this situation for the two periods.

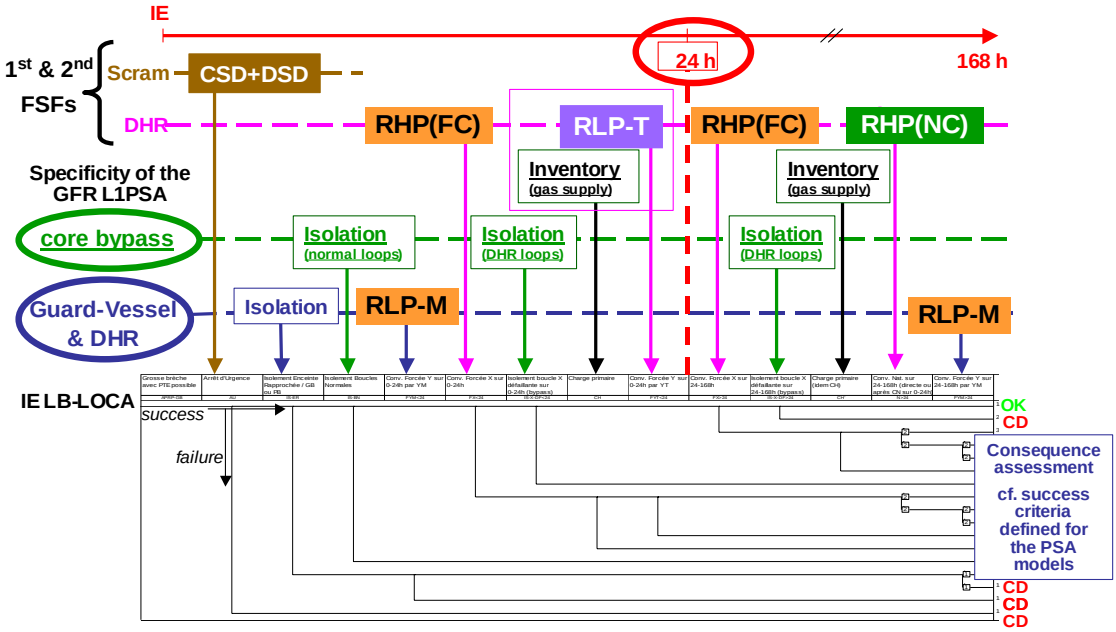


Figure 5. Large Break LOCA event tree

Thanks to Risk Spectrum software and its ET success branches treatment, generic FTs are built for two successive periods, in order to generate time-crossed cut-sets. A recall of the history is made at a lowest level of the FT built for the late phase of RHP system, which also includes basic events related to the early phase.

In line with some deterministic practices leading to combine the frequent IEs (PCC2 and 3) with short LOOP, it appears that a generalized treatment of IEs combined with LOOP could be of interest for a L1PSA in support to the design. Through this way of modeling, this L1PSA provides some relevant results for the design basis events categorization. This point is implemented in the L1PSA by a transfer gate defined in every IE fault trees and also in FT related to failure modes of electrical-driven components.

Reliability data acquisition is of major concern due to the lack of feedback for new reactor concepts (Table 2). Most of components failure rates were issued from common databases: EIREDA (feedback of French PWRs), T-BOOK 6 (Scandinavian LWRs), and EG&G-gas-cooled reactors database. According to their scope, a methodology was based on similar environment assumption. Components belonging to GFR gaseous circuits (i.e. from primary and secondary circuits, nitrogen or helium gas tanks included) are affected by failure rates consistent with the EG&G-gas database, whereas for GFR

water circuits (secondary and ternary circuits of DHR), the EIREDA database is preferred. When databases do not provide a value for GFR components, reachable data are used: 1E-3/d and 1E-6/h. Components with high confidence in data have EF 3, other components have EF 10, the latter correspond to less or no feedback or operating conditions different from those encountered in the GFR (Saignes, 2008).

Table 2. Components failure rates in GFR PSA

Component	fail to run λ (/h)	EF	fail to start γ (/d)	EF
P/Q sensors + transmitters	7.40E-6	3		
Reactivity sensors + transmitters	2.00E-6	10		
Close-containment pressure sensors + transmitters	3.40E-6	3		
Trip sensors + transmitters	2.00E-6	10		
Temperature sensors + trannmitters	1.53E-6	10		
Electronic 2 out of 3 voting device	1.20E-6	10		
Control rod + electromagnet			1.27E-3	10
Trip breakers			5.00E-4	10
Optical cross link	1.00E-7	10		
Blower + motor (RHP/RLP systems)	1.10E-4	10	6.00E-4	3
RLP-Turbofan (RLP system)	2.00E-4	10	2.00E-3	10
Helium-water heat exchanger (RHP/RLP systems)	3.00E-5	10		
Water-water heat exchanger (RHP/RLP systems)	8.30E-7	10		
Water tank (tertiary circuit of RHP/RLP systems)			9.30E-7	10
Normal and DHR loops isolating valve + motor			1.30E-3	10
Helium check valve			1.00E-4	10
Helium relief + motor-operated valve			3.00E-4	10
Pressurizer	6.40E-7	10		
Nitrogen or helium tank	1.00E-8	10		
Nitrogen or helium tank isolating valve			1.00E-3	10
Battery + converter	7.40E-6	3	2.14E-3	3
Emergency Diesel Generator	3.12E-3	3	1.72E-3	3
380V circuit breakers	3.40E-7	3	5.00E-4	3
380V electrical switchboard	7.60E-7	10		
6.6kV circuit breakers	4.60E-7	3	2.60E-4	3
6.6kV electrical switchboard	6.70E-7	10		
Ternary circulation pump	1.00E-5	3	1.00E-5	3
Ternary or secondary isolation valve	4.20E-6	3	1.10E-4	3

The Multiple Greek Letters CCF factors are generic derived from operational feedback of french and german LWRs, supplemented by the EG&G generic reliability database: $\beta(2)=0.05$, $\beta(3)=0.08$, $\gamma(3)=0.25$, $\beta(4)=0.10$, $\gamma(4)=0.40$, $\delta(4)=0.25$.

In a conservative manner, no human action is accounted for in the L1PSA model (except maintenance errors), due to the early design stage. We designed automatic response of the reactor following an IE and put the effort in depiction of I&C and in definition of fail-safe logic for specific components. A future possible step would be to introduce some generic elements regarding post-accidental management by operators (e.g. confirmation of scram orders, specific actions to improve DHR performance). As to the different sources of uncertainty for basic events and assumptions, it appears important to provide a general traceable treatment in the PSA built at a design phase. We mention here 4 kinds of uncertainty described in previous articles (Bassi 2008a, b): Reliability Method for Passive Systems (RMPS), Technological uncertainties (risk of being unable to conceive a component), Physical uncertainties (risk of not being able to prove the performance of a system for mission it was not initially designed for), Data uncertainties.

3. Insights from the preliminary L1PSA

In the preliminary L1PSA, all selected representative IEs use only RHP or RLP systems for DHR. Lessons were erected through preponderant minimal cut-sets screening (Bassi 2008a). Starting from the configuration or architecture of support systems, successive modifications were performed in the probabilistic model (Figure 6 on a relative scale).

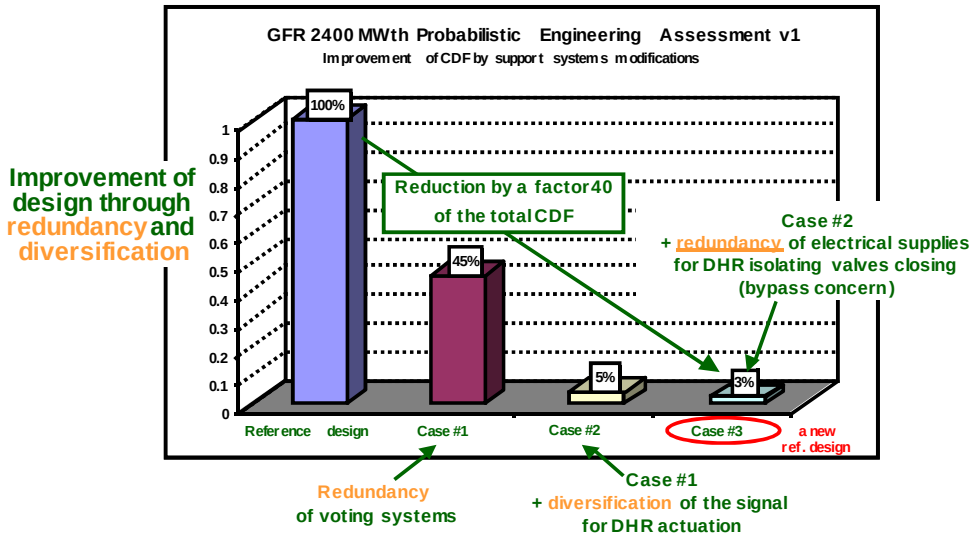


Figure 6. Design improvements through the relative preliminary PSA results screening

An important insight was to make the DHR function more reliable for pressurized situations representing 98% of the overall CDF. A few dependencies exist through heat exchangers and isolating EDVs of the RHP system (this was exhibited by their CCFs). This dependency is increased owing to the dual convection scheme: these components are common for forced and natural convection mode. For technological constraints regarding the diversification of such components, the option was preferred to use normal loops as first provision (figure 7):

· The Auxiliary Feed Water takes benefit from the thermal inertia of water at tertiary side of SGs. This system is inspired from those retained in Rankine thermodynamic cycles (at secondary for PWR, at tertiary for SFR). Note that heat exchange from the primary to the tertiary circuit, is provided after the stop of TM by NC of the gaseous mixture in the secondary circuit.

· The Intermediate Loop Cooling system (isolated in normal operating state, or when AFW is in operation) is mainly based on cooling towers, one per secondary circuit, in which a sufficient heat exchange is provided by air FC. The gaseous secondary mixture operates in NC with an elevation of about 20 meters between the main IHX mid-plane and the cooling tower. In order to enhance the NC performance through the ILC system, a set of EDVs is implemented at TM boundaries in order to avoid the potential SG cold spot.

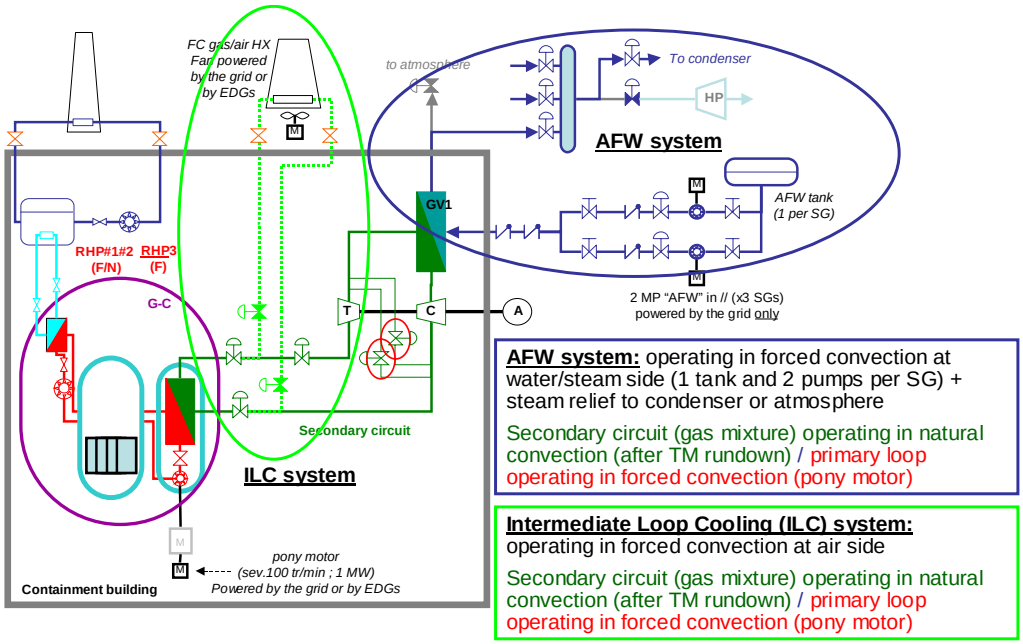


Figure 7. Implementation of AFW and ILC systems for DHR in pressurized situations

For this final L1PSA, in order to define the success criteria of these two additional systems, thermal-pressurized transients (partial or total loss of flow, secondary or tertiary initiators) were calculated with CATHARE2 (GFR dataset version 2007). A fuel temperature limit of 1600°C was taken as decoupling criterion of the deterministic categorization of PCC4, and 1 out-of 3 AFW train or 1 out-of 3 ILC train satisfies this criterion.

The layout of DHR systems is then redefined to include a gradual depending on: the availability of electrical supplies (AFW being not supplied by DGs), and on the reliability of the AFW and ILC systems themselves. Figure 8 shows the progressiveness of DHR provisions settled for pressurized situations in order to cope with the combination of them with partial or total loss of electrical supplies. For frequent situations, all active systems provide the highest level of diversifications to reduce the CDF (through AFW, ILC and RHP/RLP systems). In case of long LOOP or when a frequent IE is combined with a short LOOP, the AFW system is not operating and the DHR strategy relies on ILC as the first line of provision (with a redundancy level depending on the IE, i.e. 0, 2 or 3) and finally on the RHP/RLP systems. For infrequent situations (station black-out or complex sequences), NC through the two RHP dedicated loops becomes required.

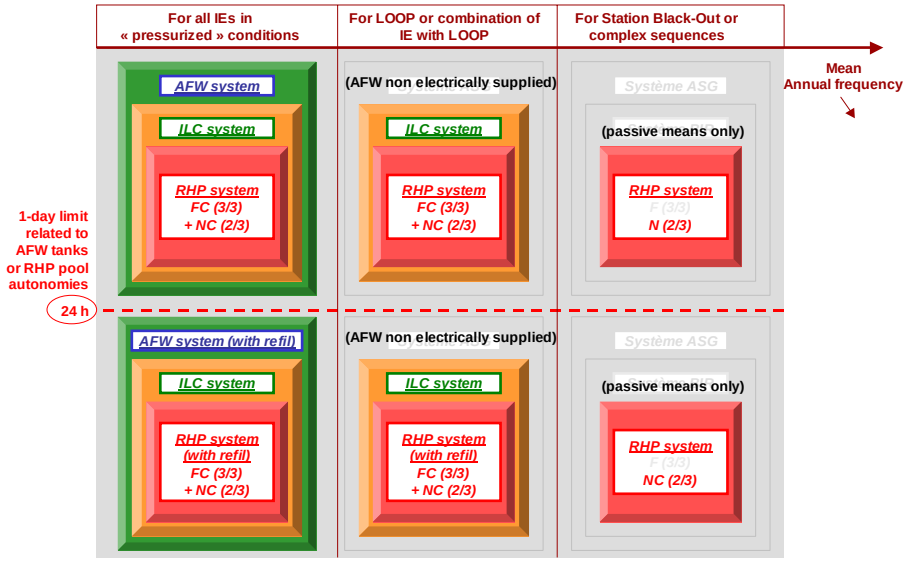


Figure 8. Progressiveness of DHR active / passive provisions regarding electricity for pressurized situations

In addition, the fail-safe concept is implemented for all EDVs: normal or DHR isolating valves, turbo-machine (TM) bypass valves or for ILC isolating valves, in case of the combination of a pressurized initiator with a short LOOP (after a time to be refined, e.g. consistent with the main blowers inertia), a long LOOP, a Station Blackout (SBO), a loss of one electrical switchboard train. If a loss of helium occurs (detected by a low primary pressure in the circuit), possibly combined with a loss of electrical supplies (partial or total), the safe state for normal loops EDVs is closed in order to enhance the RHP/RLP operation (EDVs of the dedicated loops being opened in case of the failure of electrical supplies).

TMs in secondary circuits, may cause missile following a blade rupture. This requires to control TM speed and stop after generator disconnection from grid, by two TM bypass lines connecting the compressor to the turbine outlet volumes, and then decreasing the respective compression or expansion ratios when opened. In case TM bypass EDVs fail to open, we assume missile emission (cond. proba. 1) potentially breaking the secondary envelope (cond. prob.0.5). The fast depressurization of the secondary circuit (6.5 to about 0.1 MPa) would induce unacceptable thermo-mechanical constraints on the main IHX of the affected loop (cond. prob.1E-3). To avoid a close containment bypass (secondary circuit induced break combined with a main IHX induced tubes rupture), the strategy requires to isolate the affected loop by closing dedicated EDVs at IHX secondary boundaries, thanks to appropriate measurements (TM over-speed or secondary depressurization). As ultimate provision, the RLP-M loop would be started.

For each IE, two redundant reactor trip signals have been identified, based on either global measures for events on primary circuit or on local measures for events on separated secondary and tertiary loops. This latter case allows appropriate local protection actions or reconfigurations (TM rundown, secondary circuit isolation…). Control rods in low position (fully inserted) or negative reactivity detect success of the reactor trip and launches all generic actions on the circuits, including DHR configurations. According to the IEs, representative signals are defined for DHR systems reconfigurations. For instance, AFW is always started even for LOHS (SGs temperature increase or low flow rate will start ILC), or for LOCA (IE signal will override by emitting a primary loops isolation signal and RHP/RLP starting signal).

4. Second step in the building process of the L1PSA model

The first work was initiators identification, grouping and frequency estimation. IAEA presents several approaches to identify the set of IEs. Finally for the GFR design in progress, the MLD approach was followed (Cadwallader 1998, Papazoglou 2003), selecting the IEs by looking at the phenomena able to disturb the physics of the reactor concerning each safety function. According to the assumptions

sustaining the GFR L1PSA (radioactive release coming from reactor core, internal events and power state), only the related part of the MLD is developed. At the end, according to the combined Brayton thermodynamic cycle and related components involved in the GFR, a total of 53 representative IEs are defined. A fault schedule approach, based on usable systems and missions, is applied for grouping in 14 representative families of IEs. Their frequencies are chosen by screening former PSAs related to various concepts: Pressurized Water Reactors like AP1000 (Lutz 2009) and EPR (Areva 2007), Sodium-cooled Fast Reactors like SPX (Nuclear Europe issue No.11) and EFR (Framatome 1991), Gas-cooled reactors especially High-Temperature Reactors, like HTGR (General Atomics 1986) and Pebble Bed Modular Reactor (Koster 2003).

The compliance with the representative technologies involved in the GFR is appreciated by expert judgment including operating feedback (French PWRs, SFRs, US HTRs). For specific events initiated by a partial failure of component (e.g. spurious opening or closure of an EDV in gaseous environment), failure rates reported in Table 2 are employed. For a total failure of such components, a generic beta-factor of 5% is retained for the assessment of IE frequency (assuming an availability of 85% at full power). The perimeter covers 6.2 events/y leading to reactor trip, with frequencies given in Table 5, except for the initial total LOCAs taken at 0.12/y, as described hereafter. The primary breaches are initially defined through HTGR frequencies spectrum and CATHARE2 calculations.

For a break over 3 inches, the NC of helium through the RHP loops is not sufficient to avoid 1600°C in the core, even with the improvement of NC by discharge of the nitrogen tanks. This defines the lower limit of LB-LOCAs. Owing to the Helium Supply System (HSS), with an initial helium inventory of 8000 kg, and to the duration of reaching a safe cold depressurized shutdown state for GFR (around 10 h), it is assumed that RCS breaches that could be compensated by the HSS belong to the very SB-LOCA domain. Therefore, the upper limit of the vSB-LOCA domain is calculated to cope with RCS breaches below 0.4 inch in diameter. So, the SB-LOCA domain is defined for break sizes ranging from 0.4 to 3 inches.

With a frequency of 0.12/y was in HTGR PRA, the vSB-LOCA domain represents around 87% of this total, then leading to around 0.1 event/y. The SB-LOCA represents 12%, so that the frequency retained for GFR L1PSA is 1.46E- 2/y. The complement goes for LB-LOCA with a frequency of 1.19E-3/y. This significant increase of LOCA frequencies, by comparison with those defined during the preliminary L1PSA building will have a relative importance for CDF assessment, and will be subject at the end to Sensitivity Analyses.

The second work was re-using representative situations of the preliminary PSA, basically unchanged when extending to all initiators. However, the SB-LOCA event tree is now generic for losses of helium, compensated or not by HSS (new top event). For pressurized situations, the reactor trip and the LOOP transients were defined as prototypical in the preliminary L1PSA, and belong to 1st rank ET category. Now, ETs previously built and involving the RHP/RLP operating modes in pressurized situations, are defined as ultimate rank ETs (downstream). They are considered as generic of RHP/RLP missions that cope with all situations (e.g. LOF transient, inadvertent valve opening or closure, LOHS, turbine trip…). The additional provisions for DHR through the NL are now modeled by a generic 2nd rank ET. Figure 9 presents the ETs arrangement and transfers for the LOOP family. This step-by-step approach for scenarios includes a total of 50 sequences in a dense arrangement of modular ETs. This provides an extension of the preliminary L1PSA without intrusive modifications. At the end, 14 first rank ETs (one per IE family) are implemented in the L1PSA.

An intermediate ET describes the double-break sequences (i.e. induced breaches on a secondary loop and by consequence on the main IHX). This is performed through conditional probabilities of turbine deblading following an uncontrolled TM over-speed and of unacceptable thermo-mechanical constraints on the IHX of the affected loop. In this case, the loop with the induced break on secondary circuit is considered out of operation for DHR.

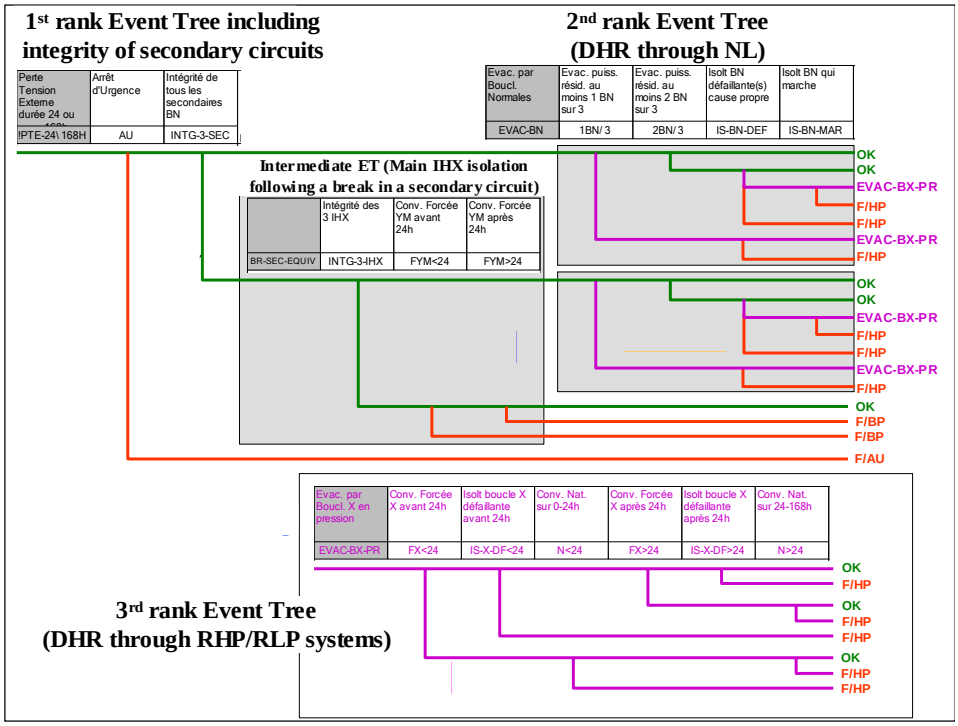


Figure 9. Arrangement of ETs for the LOOP

For the final L1PSA, the assessment of consequences and success criteria have benefited from physical studies for the safety demonstration of GFR with CATHARE2 based on best-estimate calculations (Bertrand 2008). A future could be to account for conservatisms versus uncertainties in the consequence assessment (e.g. RMPS uncertainties would quantify safety margins for the deterministic analysis). For LOCA, rods insertion failure is assumed to be unacceptable. For other IEs, the success of both three normal loops, (AFW or ILC), is sufficient to avoid core damage, thanks to transient assessment. For DHR systems, the failure to maintain vital components at low temperature for a long mission time (i.e. 168 h) is defined consistently with the design safety limits for the PCC4. These limits are 1600°C for fissile core (fuel integrity), and 1250°C for helium temperature in upper plenum (internal structures integrity).

5. Insights and improvements for GFR

To assess the benefit of additional AFW and ILC provisions 4 situations of CDF are distinguished (Figure 10). Note that High-Pressure scenarios mean Helium boundary intact (7.0 MPa), MP scenarios range from 0.5 to 1.5 Mpa, depending on the depressurization kinetic (or break size) and the thermal exchange of the CC with environment, LP scenarios (0.5 Mpa) follow concomitant loss of RCS and CC integrities (handled by RLP-M sub-system only).

HP scenarios only represent 1% of the overall CDF, instead of 98% in the preliminary model, in spite of the extension to all initiators, mostly at high pressure. This is correlated to the implementation of three lines of provisions (AFW, ILC, RHP/RLP) to cope with these frequent situations.

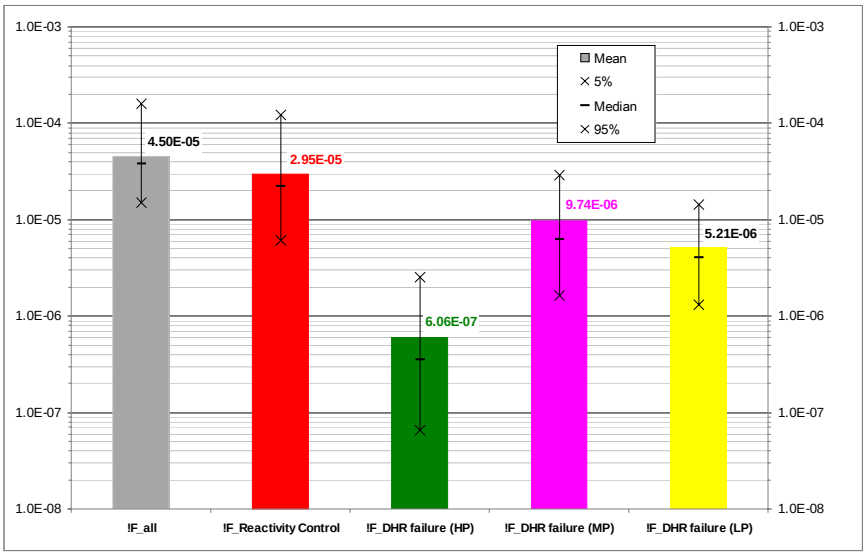


Figure 10. Contribution of typical situations to CDF

The high contribution of core reactivity scenarios (66%) is linked to the Control Rod Absorber withdrawal initiator (2E-2/y). The contribution of DHR failure at MP is 22% of the CDF (9.7E-6/y). This is attributed to LOCA frequencies increase taken from the HTGR PSA. The above results and the Sensitivity Analysises lead to GFR modifications: (1) additional Stroke Limitation Device to cope with the CRA withdrawal. This device has a failure rate of 6.2E-3/d from the Superphenix feedback. (2) Trip breakers diversification (simulated by deleting CCFs between the two CRA groups). (3) Replacement of the RLP-T sub-system by another RLP-M one. (4) Elimination of the RHP#3 loop. This point (4) is an optimization of DHR provisions leading from a "3RHP+2RLP" configuration considered as reference for GFR to an alternative one featuring "2RHP+2RLP-M". This first step of GFR design improvement lead to a slight CDF increase compared to the former result, but stay around values ranging from around 4.8E-5/y to 4.6E-5/y, depending on the refinement of success criteria for reactivity control (Figure 11).

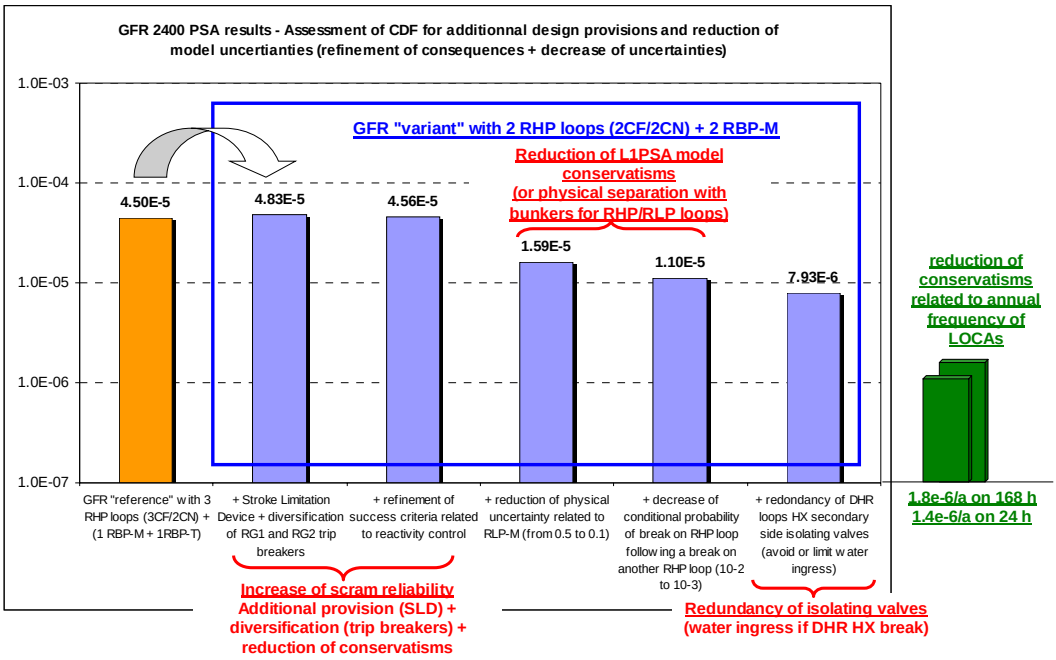


Figure 11. Design improvements through the final PSA results screening

In a second step, some conservatisms of the L1PSA are reduced according to:

· The design of the RLP-M loop and the relaxing of its blower physical constraints. Appropriate T-H calculations showed that FC at very low pressure can cope with substantial core decay heat (up to 24 h) that finally keeps temperature under 1600°C. Therefore, the Physical uncertainty related to this RLP-M loop was reduced to 0.1, resulting in a CDF of 1.6E-5/y.

· The decrease of one order of magnitude applied to the probability of an induced rupture of a RHP loop following a breach on another RHP loop (1E-2 in the reference, 1E-3 in this SA) leads to a CDF of 1.1E-5/y (Figure 11). This modification can be obtained for instance by implementing shielding around these loops.

The third step for GFR design improvement is obtained by implementing redundant isolating EDVs on DHR secondary circuit (at IHX inlet and outlet) in order to avoid a large water ingress in the core region (following a HX tube rupture in the DHR loop). The lack of reliable transient calculations, lead to consider that even a small water ingress in the core is unacceptable. This point should be clarified by coupling neutronics and T-H calculations. The redundancy increase of these EDVs leads to a CDF reduction from 1.1E-5/y to 7.9E-6/y.

Another SA is presented in Figure 11 that relates to LOCA frequencies and to mission times. For reference L1PSA, LOCA frequencies are derived from the HTGR PRA that retained high values (0.12 events/y, based on HTRs operating feedback). For SA, these frequencies are now fixed to 5E-2/y for very SB-LOCA (mean deterministic PCC2), 5E-4/y for SB (PCC3) and 5E-6/y for LB-LOCA (PCC4), with an EF 3. These low values can be faced with those of PWRs (Table 3), that are first based on a synthesis on U.S nuclear power plants (Poloski 1999) or re-assessed for the Standardized Plant Analysis Risk (SPAR) models (Eide 2008). Note that the "low" frequencies retained for this SA are greater by one or two order of magnitude than values reported in Table 3.

Table 3. LOCA frequencies for U.S. PWRs

	Poloski et al, 1999	Eide et al, 2008	
Mean Freq. (/y)	NUREG/CR-5750	method 1	method 2
LLOCA (> 6 in. dia.)	5.00E-06	2.70E-06	1.78E-05
MLOCA (2 - 6 in. dia.)	4.00E-05	1.35E-04	3.26E-04
SLOCA (< 2 in. dia.)	5.00E-04	8.54E-04	7.61E-04
total	5.45E-04	9.92E-04	1.10E-03

As a result of this SA on LOCAs frequencies, an overall CDF of 1.8E-6/y is obtained for the GFR. For example, by accounting for maximum values reported in Table 3, new results can be obtained (see SA#2 results in Table 4[3]).

Table 4. Sensitivity Analysis upon the LOCA frequencies for the CDF of GFR

GFR L1PSA model	Reference	SA #1	SA #2
LB-LOCA located on RCS	1,19E-03	5,00E-06	1,78E-05
SB-LOCA located on RCS	1,46E-02	5,00E-04	3,26E-04
vSB-LOCA located on RCS	1,04E-01	5,00E-02	8,54E-04
LOCA located on secondary	0,318	0,318	1.20E-03 [1]
CDF	**7,90E-06**	**1,47E-06**	**9,30E-07**

In comparison with the previous optimization of the GFR (i.e. CDF=7.9E-6/y), the SA#2 exhibits the weight of the LOCA data. Note that depressurized situations are to date only handled by RHP/RLP systems. So if LOCAs frequencies were to be evaluated at high values (as for HTGR), other provisions should be implemented to cope with these situations (e.g. by isolating the broken loop and removing decay heat thanks to the 2 remaining normal loops through AFW or ILC). This work would constitute a further step for the GFR safety improvement. Finally, by reducing the mission time of DHR systems to 24 h (instead of 168 h), the SA#1 furnishes an overall CDF of 1.5E-6/y. The observation of the slight decrease of the overall CDF (i.e. from 1.8 to around 1.5E-6/y) clearly exhibits the weight of failure to start compared to the failure to run for a long time (7 days). This is explained by gamma

[3] For SA #2, LOCAs on secondary circuits are affected by a frequency = the sum of maximum frequencies obtained from Table 8

parameters (Table 2) being 3 orders of magnitude greater than lambda parameters. Table 5 furnishes the absolute contributions of IEs for CDF, and their normalized contributions (division by frequency).

Table 5. Summary of Initiators, CDFs and normalized CDF

Initiating Event	Fq. (/y)	CDF (/y)	CDF/Fq
LB-LOCA on Reactor Coolant System	**5.00E-06**	5.41E-09	1.08E-03
SB-LOCA on Reactor Cooling System	**5.00E-04**	3.35E-07	6.70E-04
RHP/RLP HX Interfacing LOCA	1.20E-02	2.20E-07	1.83E-05
Main IHX Interfacing LOCA	3.00E-03	1.71E-08	5.70E-06
Very SB-LOCA on RCS	**5.00E-02**	1.63E-07	3.26E-06
SB-LOCA on secondary circuit	3.18E-01	2.81E-07	8.84E-07
Safeguard switchboard loss	1.00E-02	6.96E-09	6.96E-07
CRA Withdrawal AND failure of SLD	*1.24E-04*	4.54E-11	3.66E-07
Generator or Main Turbine trip or fault	1	2.76E-07	2.76E-07
LOOP (<24 h, or >24h)	1.00E-02	9.05E-10	9.05E-08
Loss Of primary Flow	4.66E-01	3.82E-08	8.20E-08
Steam Generator Tube Rupture	2.50E-01	9.63E-09	3.85E-08
Main Steam Line Break	7.70E-02	2.92E-09	3.79E-08
Loss Of Heat Sink	2.57E+00	8.53E-08	3.32E-08
Inadvertent TM rundown	0.229	6.73E-09	2.94E-08
Inadvertent Reactor trip	1.1	2.49E-08	2.26E-08
total	**6.10**	**1.47E-06**	***2.42E-07***

6. Conclusion

This paper demonstrates the benefit of a L1PSA for the design of new reactors. The building approach allows to cope with design modifications all along a project life, through flexibility for new periods definition or for systems integration. The PSA model was developed according to expected and unavoidable design evolutions. Modularity is provided by event trees and fault trees structure for the integration of new or redundant front line systems. Support Systems (electrical supply, I&C) located at low level for modularity concern and adjustment easiness (architecture modification, redundancy, future adding of component cooling systems). Regarding methodology, the L1PSA provides the design team with a set of possible modifications, which lead to a safer architecture. While the design team was focusing on the hard points of feasibility or technology, the exchanges between PSA and design teams resulted in complements in the architecture (e.g. power supplies, signals).

For the safety demonstration, the L1PSA furnishes complementary and independent insights along with the deterministic safety approach. In a global approach, the PSA leads to check the design assumptions as to dependencies, uncertainties and exhaustive scenarios screening. Moreover the evolutionary feature of probabilistic models appears as one major advantage. For situations not associated to well-defined quantitative criteria (e.g. instantaneous total blockage of a sub-assembly) the PSA may convince that they are “practically eliminated”, which is an issue in Generation IV roadmap. The L1PSA furnishes also valuable insights for Severe Accidents R&D prioritization. Furthermore, the slight effort in developing a L1PSA at pre-design phase should be appreciated with regards to the amount and deepness of insights gained, which are also accounting for all kind of dependencies (e.g. support systems, common materials or CCFs) that are inherent in a sophisticated system like a nuclear reactor.

Lessons learnt from the two successive models were of different nature depending on their respective perimeters. The preliminary L1PSA only dealt with IEs used for the deterministic design of RHP/RLP systems, and pointed that more reliable DHR systems were suitable for reducing the so far major contribution of pressurized situations for CDF. In a second step, when all representative IEs of the GFR were handled in model, successive improvements were proposed as additional provisions for reactivity control and for DHR. Finally, reducing conservatism regarding LOCA frequencies, lead to a CDF ranging between 1.0 and 1.8E-6/y (for mission times set to 24 and 168 h).The reach of the probabilistic target assigned to 3rd generation reactors (i.e. less than 1E-6/y) is then nearly guaranteed. In the near future, it could be decided to build L1PSA models to support the design and the preliminary safety demonstration of other reactor concepts such as the 4th generation SFR that is at pre-design phase (Rouault 2009).

7. Acnowledgements

The authors wish to thank all the people at EdF, CEA and entourage, the events and the chance that made this exploratory work and this adventure possible.

8. References

Works citations do not repeat et al, but understand all authors.

AREVA NP Inc (2007). U.S. EPR Final Safety Analysis Report Rev.0.

BASSI C., AZRIA P., BALMAIN M., SAIGNES P. (2008a). Application of PSA in support to the design of CEA 2400 MWth GFR, Proceedings of PSA08, Knoxville TN, USA, September 7-11.

BASSI C., MARQUES M. (2008b). Reliability assessment of 2400 MWth GFR natural convection DHR in pressurized situations. Science and Technology of Nuclear Installations, special issue “natural convection in nuclear reactor systems”, vol. 2008, Article ID 287376.

BENTIVOGLIO F., TAUVERON N., GEFFRAYE G., GENTNER H. (2008). Validation of the CATHARE2 code against experimental data from Brayton cycle plants. Nuc. Eng. Des. 238, 3145-3159.

BERTRAND F., BASSI C., BENTIVOGLIO F., MESSIÉ A., TOSELLO A., MALO J.Y. (2008). Preliminary safety analysis of 2400 MWth GFR, Proceedings of ICAPP '08, Anaheim, USA, June 8-12.

CADWALLADER L.C., TAYLOR N.P., POUCET A.E. (1998). Preliminary Master Logic Diagram for ITER operation. In: Proceedings of PSAM 4, New-York City, USA, September 13-18.

DELANAY M.J., APOSTOLAKIS G.E., DRISCOLL M.J. (2005). Risk-Informed design guidance for future reactor systems, Nuc. Eng. Des. 235, 1537-1556.

EIDE S.A., RASMUSON D.M., ATWOOD C.L. (2008). Estimating LOCA frequencies for the standardized plant analysis risk models. Proceedings of PSA08, Knoxville TN, USA.

FRAMATOME technical document EFRB2-07-4-1315a (1991). Draft fault schedule for the EFR level 1 Probabilistic Risk Assessment.

GENERAL ATOMICS technical document HTGR-86-011 rev1 (1986). Probabilistic Risk Assessment of the modular HTGR plant.

KOSTER A., MATZNER H.D., NICHOLSI D.R. (2003). PBMR design for the future. Nucl. Eng. Des. 222, 231-245.

LUTZ R.J., ANDERSON R.G., SCOBEL J.H., SCHULZ T. (2009). Use of PRA in the design of the Westinghouse AP1000 plant. Proceedings of ICONE 17, Brussels, Belgium, July 12-16.

NUCLEAR EUROPE, No. 11 (1985). Special issue about SUPERPHENIX.

MALO J.Y., ALPY N., BERTRAND F., CADIOU C., CHAUVIN N., DUMAZ P. HAUBENSACK D., GEFFRAYE G., JONQUERES N., LORENZO. D., MORIN F., NICOLAS L., PENELIAU Y., RAVENET A., RICHARD P., STUDER E. (2008). GFR 2400 MWth, end of the preliminary viability phase. Proceedings of the ICAPP 08, Anaheim CA, USA, June 8-12.

PAPAZOGLOU A., ANEZIRIS A.O. (2003). Master Logic Diagram: method for hazard and initiating event identification in process plant. Journal of Hazardous Materials, 97, 11-30.

POLOSKI J.P., ATWOOD C.L., GALEYAN W.J., MARKSBERRY D.G., MAYS S.E. (1999). Rates of initiating events at U.S. NPPs: 1987 – 1995. NUREG/CR-5750, Washington DC.

ROUAULT J., SERPANTIE J.P., VERWAERDE D. (2009). French R&D program on SFR and the ASTRID prototype. Proceedings of FR09 Conference, Kyoto, Japan, December 7-11.

SAIGNES P., (2008). Reliability database for PSA in support to the design of the innovative CEA 2400 MWth GFR. Proceedings of PSAM 9, Hong Kong, China, May 18-23.

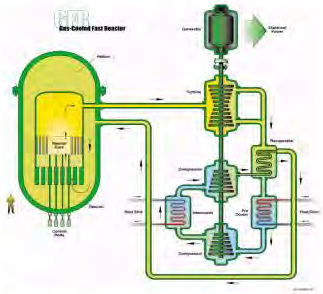
Achievement of a PSA in support to the design of the CEA 2400 MWth Gas-cooled Fast Reactor

M. BALMAIN, C. BASSI, P. AZRIA
EDF, R&D Division, F-92140 Clamart, France
CEA, Nuclear Energy Directorate, F-13108 Saint-Paul-Lez-Durance, France
Corresponding author: michel.balmain@edf.fr

Main objectives:

- to define what could be the contribution of a L1PSA model to support the design and the safety demonstration (with an application for the GFR)
- to exhibit methodological trends for an efficient model L1PSA construction through the project lifecycle

The GFR and GenIV International Forum criteria



The GEN IV initiative

Fast Reactor (FR) missions

Resource utilization
Waste minimization
Economical competitiveness
Improved safety

GFR requirements

Fast neutron spectrum, closed fuel cycle
self-sustainable core (BG~0), TRU recycling

Gas coolant, high core outlet temperature
He, 850°C or higher, direct cycle attractive for power conversion efficiency

Robust and refractory fuel
FP confinement, close retention and resistant (analogy with particle fuel)

GFR
a system combining advantages of FR and HTR/VHTR

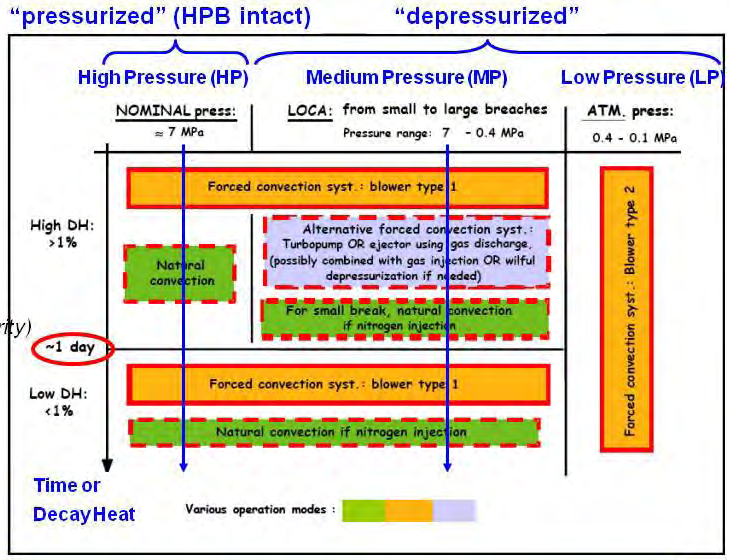
GFR 2400 : DHR strategy and use of Natural Circulation (2nd Safety Function)

A "strategy" and the related means improved in accordance with the design team

Choice of DHR strategy
DHR under dual FC & NC
(0.4-1.0 MPa)
metallic guard-vessel →
- moderate pumping power
- potential for "light" self governing systems

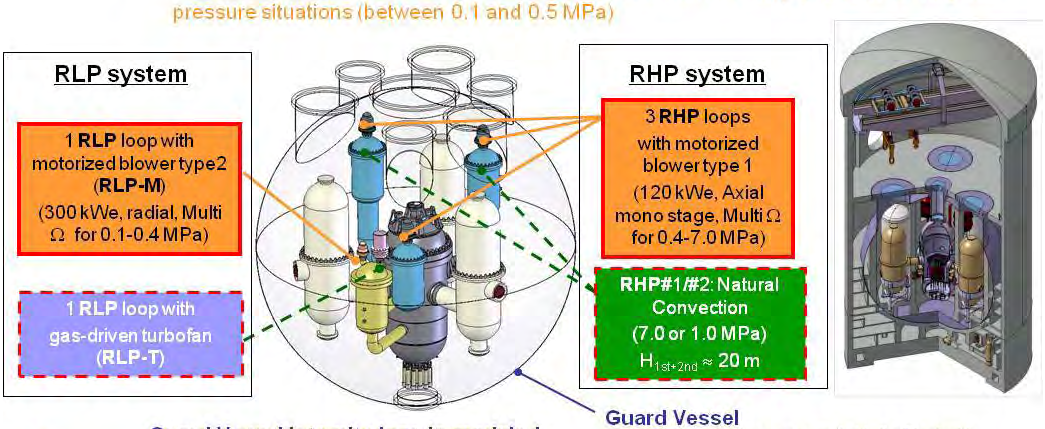
at Low Pressure (LP)
(i.e. loss of guard-vessel integrity)
FC with only 1 RLP-M

Two situations of interest for NCDHR depending on
- *pressure level (HP or MP)*
- *core power*

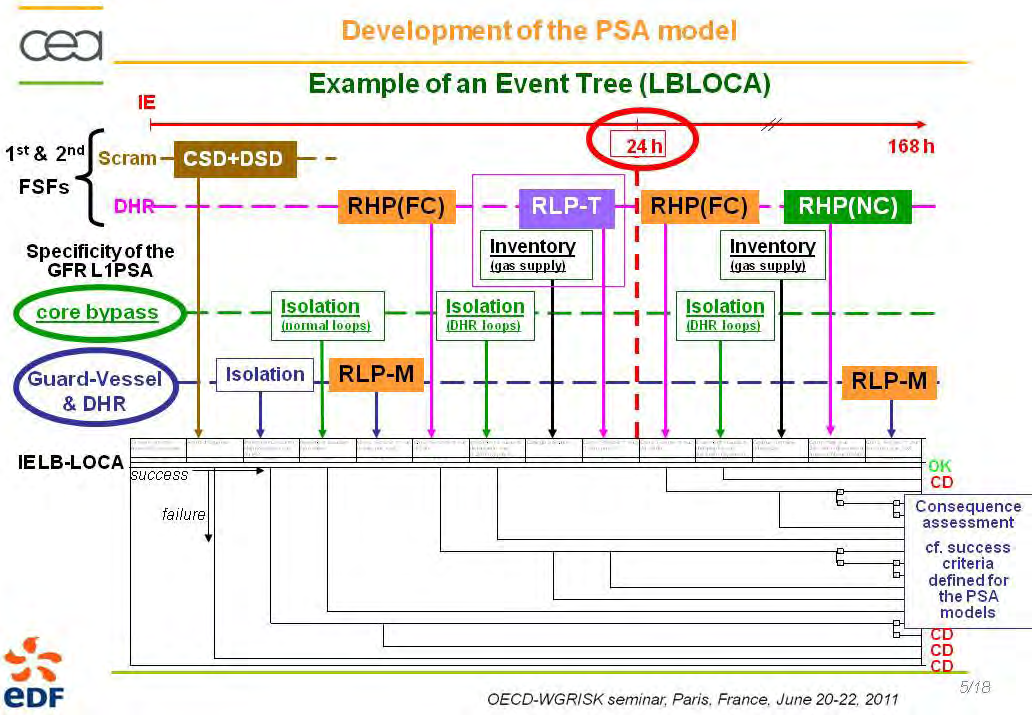


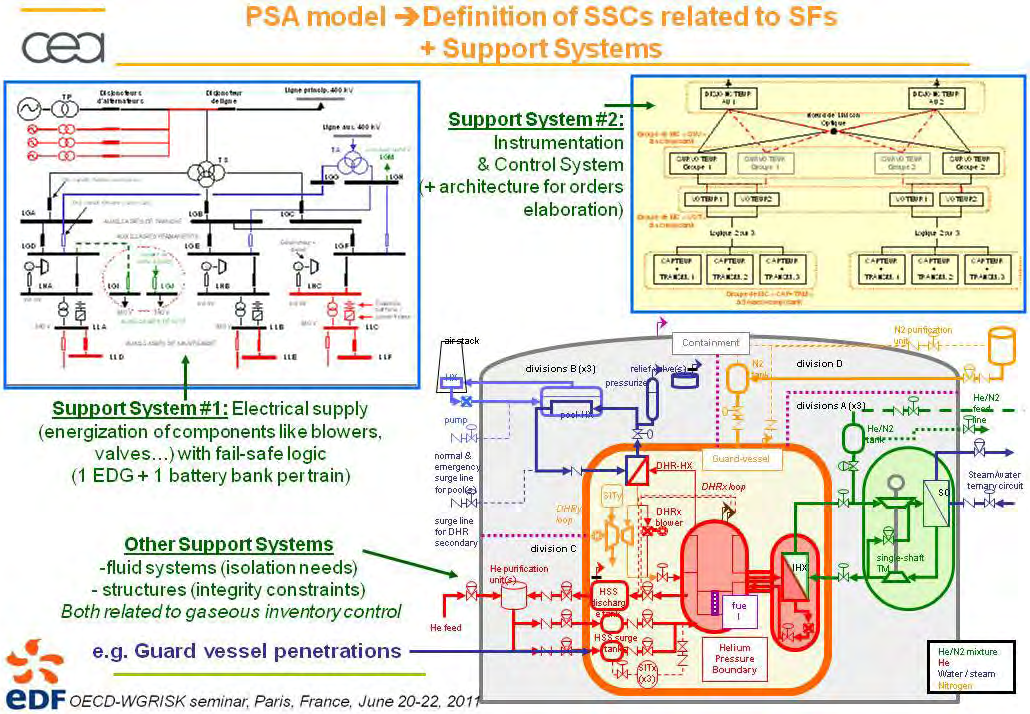
GFR 2400 : Provisions (including SSCs) for DHR (2nd Safety Function)

1. **RHP system** : Forced Circulation of gas through 3 redundant dedicated DHR loops driven by electrically motorized blowers, with a potential for Natural Circulation of gas through 2 DHR loops (**RHP**#1/#2)
2. **RLP system** : 1 dedicated loop (**RLP-T**) allowing essentially for gas-driven helium circulation (turbofan) + 1 electrical blower is modeled on RLP loop (**RLP-M**) for very low pressure situations (between 0.1 and 0.5 MPa)



Guard Vessel integrity loss is modeled owing to its role for NCDHR following LOCA

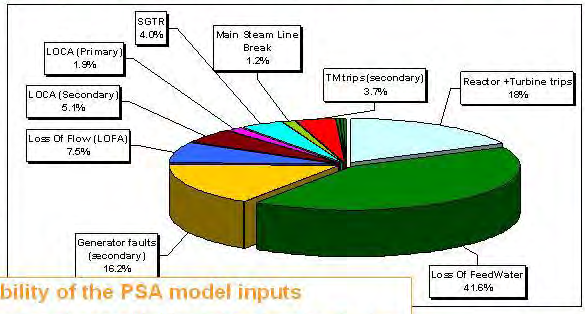

Development of the PSA model
Example of an Event Tree (LBLOCA)
IE
24 h
168 h
1st & 2nd FSFs
Scram
CSD+DSD
DHR
RHP(FC)
RLP-T
RHP(FC)
RHP(NC)
Inventory (gas supply)
Inventory (gas supply)
Specificity of the GFR L1PSA
core bypass
Isolation (normal loops)
Isolation (DHR loops)
Isolation (DHR loops)
Guard-Vessel & DHR
Isolation
RLP-M
RLP-M
IELB-LOCA
success
failure
OK
CD
Consequence assessment
cf. success criteria defined for the PSA models
CD
CD
CD
OECD-WGRISK seminar, Paris, France, June 20-22, 2011
5/18


PSA model ➔Definition of SSCs related to SFs + Support Systems
Support System #2: Instrumentation & Control System (+ architecture for orders elaboration)
Support System #1: Electrical supply (energization of components like blowers, valves…) with fail-safe logic (1 EDG + 1 battery bank per train)
Other Support Systems
-fluid systems (isolation needs)
- structures (integrity constraints)
Both related to gaseous inventory control
e.g. Guard vessel penetrations
Containment
divisions B (x3)
division D
divisions A (x3)
division C
DHR-HX
DHRx blower
Guard-vessel
Helium Pressure Boundary
He/N2 mixture
He
Water / steam
Nitrogen
OECD-WGRISK seminar, Paris, France, June 20-22, 2011

Initiating Events and L1PSA model inputs

1. **Assessment of representative IE by deductive analysis** (aim at ensuring an exhaustive IE list): Master Logic Diagram + review of existing lists for other reactor concepts
   GFR → 50 representative IE
2. **Functional analysis** on safety systems availabilities depending on the IE considered and **grouping of IE** through the functional analysis (each "group" of IE being described with a unique Event Tree in the PSA model)
   L1PSA model #2 → 16 representative IE groups
3. Determination of **IEs annual frequencies** by a review of data relative to several reactor concepts (SFR, LWR or GCR) + expert judgement for adequacy with the GFR's IE or components (L1PSA → total ≈ 6.2 events / year)
4. **Uncertainties on** "IE groups" **frequencies** (LN distribution) **+ Uncertainty Factor (3 or 10)**

IE family	FAO (/y)	%
Reactor +Turbine trips	1.10	17.8%
LOFW	2.57	41.6%
Generator faults (secondary)	1.00	16.2%
LOFA	0.47	7.5%
Secondary circuit LOCA	0.32	5.1%
LOCA	0.12	1.9%
SGTR	2.50E-01	4.0%
MSLB	7.67E-02	1.2%
TM trips	2.29E-01	3.7%
CRW	2.00E-02	0.32%
LOOP	1.00E-02	0.16%
IHX breaks	3.00E-03	0.05%
DHR HX breaks	1.18E-02	0.19%
Loss Of Electrical Switchboar	1.01E-02	0.16%
total	6.2	100%



- Identification and traceability of the PSA model inputs
- Sensitivity studies allowed and potential insights for the design
- Improvement of input data with the design (living PSA)

7/18

Reliability data and uncertainties

How to choose the reliability data for components of an innovative reactor ?

Four databases mainly used:

→ EGG GAZ, for the components of the primary circuit and the components in He

→ EIREDA, for the components of the secondary and tertiary circuits for DHR

For some specific data not provided by the previous database:

→ EGG GENERIC (for some valves and tanks)

→ T-BOOK 6 (for data related to the control rods failure to insert)

If no suitable data has been found, « a priori » failure rates have been used (for instrumentation, transmitters and the control rods electromagnets):

→ γ (per demand) = 10^{-3}/d.
→ λ (under operation) = 10^{-6}/h.

Uncertainty on reliability data: Log-Normal PDF with an uncertainty factor

→ **3** if « **high** confidence » in the value
→ **10** if « **low** confidence » in the value

Aim: Ensuring the traceability of reliability data for the PSA model

Prospects: Values potentially evolving according to the design progress (components technology, operating feedback) and to the weight for CDF of the value used (MCs screening + RIF/RDF)

8/18

OECD-WGRISK seminar, Paris, France, June 20-22, 2011

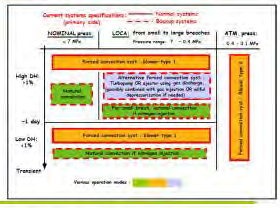
Examples of use in support to the design with relative results and a limited perimeter (PSA model #1)

(2006-2007) PSA model #1 featuring (see PSA-2008 conference publication)

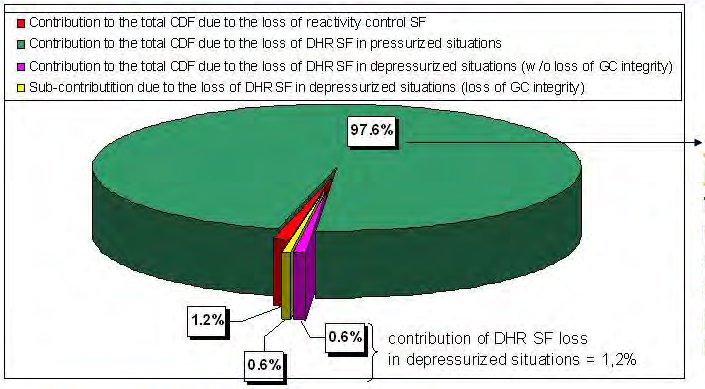
- a restricted perimeter to 3 IE families
  - LOCA : Small and Large Break LOCAs
  - LOOP : short and long duration
  - Inadvertent reactor trip

  These IE families are representative of the DHR strategy: pressurized or not, with two periods according to strategy and systems autonomies (before and after 24 hours)
- annual frequencies defined in accordance with the deterministic categorization (e.g. SB-LOCA=10^{-3}/r.y, LB-LOCA=10^{-4}/r.y)
- failure criteria i.e. "Core Damage" = Loss of 1 SF or core bypass

SF#1 (Reactivity) = Rod Group 1 + Rod Group 2
SF#2 (DHR) = 3 RHP loops (3*100% FC + 2 NC)
+ 1 RLP-T (Medium Pressure)
+ 1 RLP-M (Low Pressure)



Examples of use in support to the design with relative results and a limited perimeter (PSA model #1)



Contributions to the total CDF

1st way for the design improvement: integrating the capability of using the normal loops in the DHR strategy in order to decrease the contribution of pressurized situations (i.e. most frequent)

2nd way for the design improvement:

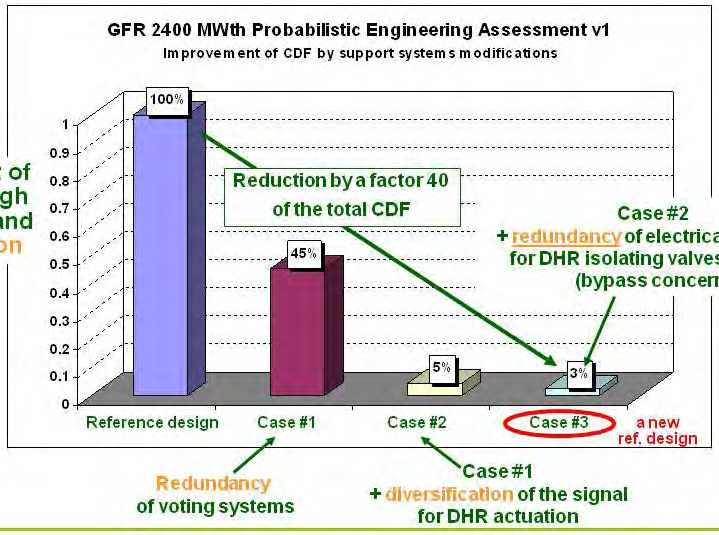
- **improve the DHR reliability for pressurized situations (I&C or components, but a weak point: HX common for FC and NCDHR)**

contributions to the CDF due to the...	total	I&C specific	elec. supplies specific	component specific
loss of reactivity control SF	1.2%	56%	37%	7%
loss of DHR SF in depressurized situations	1.2%	17%	45%	38%
loss of DHR SF in pressurized situations	97.5%	49%	3%	47%

Examples of use in support to the design with relative results and a limited perimeter (PSA model #1)

Design improvements through the PSA results screening (e.g. for support systems I&C + electrical supply)

Improvement of design through redundancy and diversification



Examples of use in support to the design with absolute results and enlarged perimeter (PSA model #2)

(2007-2008) PSA model #2 featuring

- Use of normal loops at first instance for DHR (insight PSA model #1) according to design & performance assessment (i.e. success criteria) of additional systems
- Increase of the model perimeter to all representative internal IEs of the GFR @ full power operating state
- Consolidation of data, reduction of assumptions weight
- Refinement of the consequence assessment thanks to T-H calculations with the CATHARE 2 code (with a calculations priorization derived from PSA results)

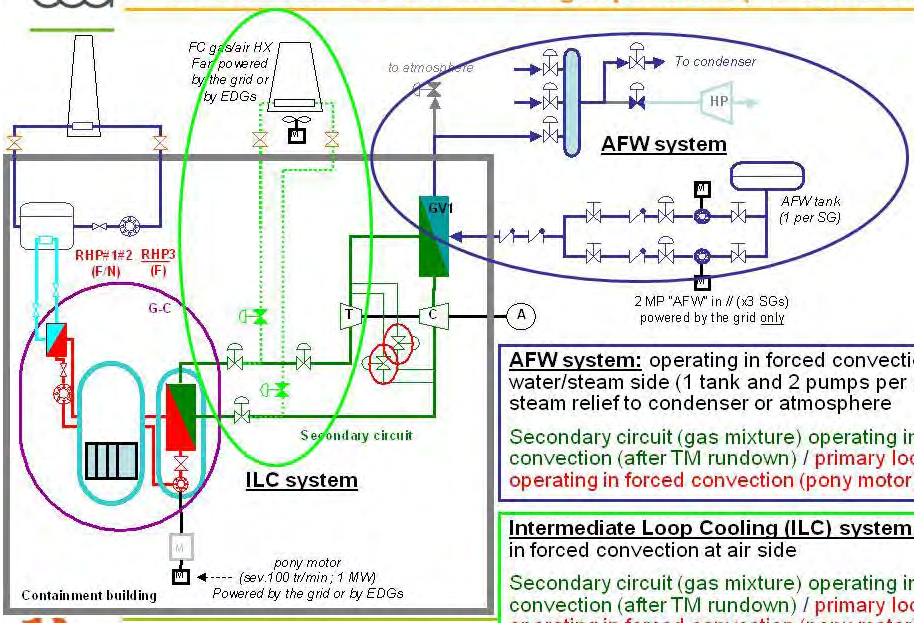
For the model building, the main idea is to benefit from the work performed in the PSA model #1, owing to the choice of representative situations for DHR:

- Pressurized (Helium Pressure Boundary not challenged)
- Depressurized (LOCA IE, or induced interfacing systems LOCA)

At the end, the expected gain is twofold:

- Increased confidence in absolute results and in sensitivity studies
- Reduction of main assumption weight for Core Damage previously defined by the loss of a Safety Function (a priori conservative)

Examples of use in support to the design with absolute results and enlarged perimeter (PSA model #2)



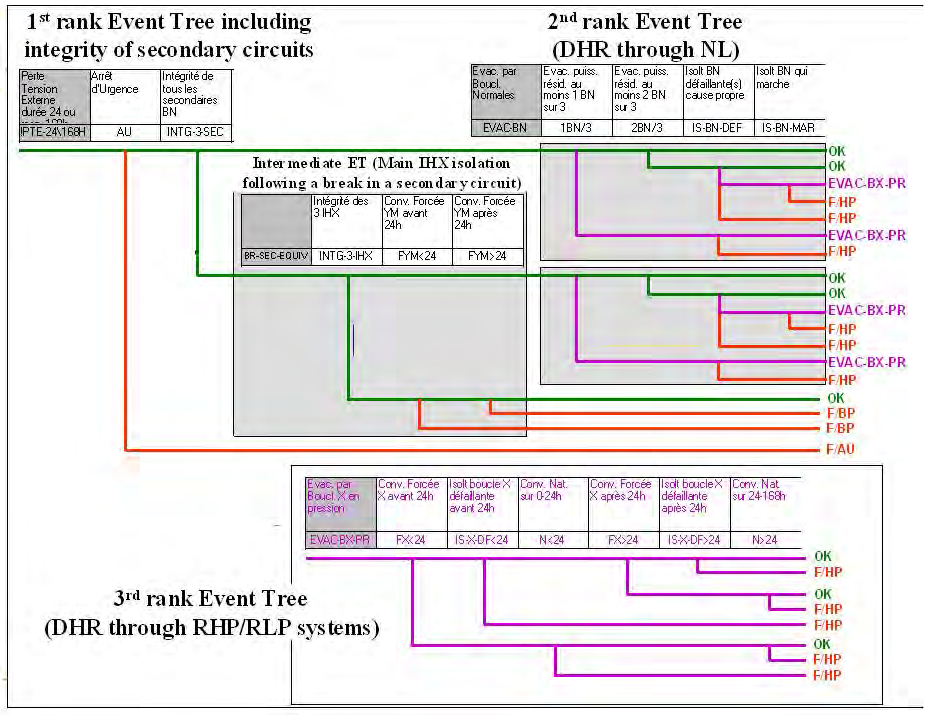
AFW system: operating in forced convection at water/steam side (1 tank and 2 pumps per SG) + steam relief to condenser or atmosphere

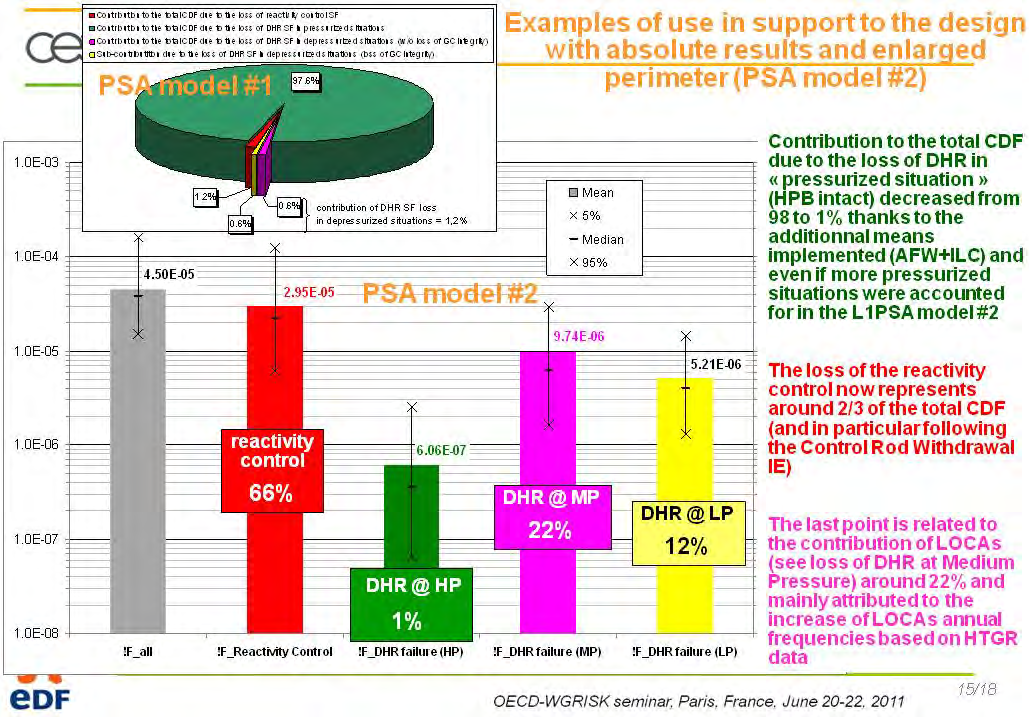
Secondary circuit (gas mixture) operating in natural convection (after TM rundown) / primary loop operating in forced convection (pony motor)

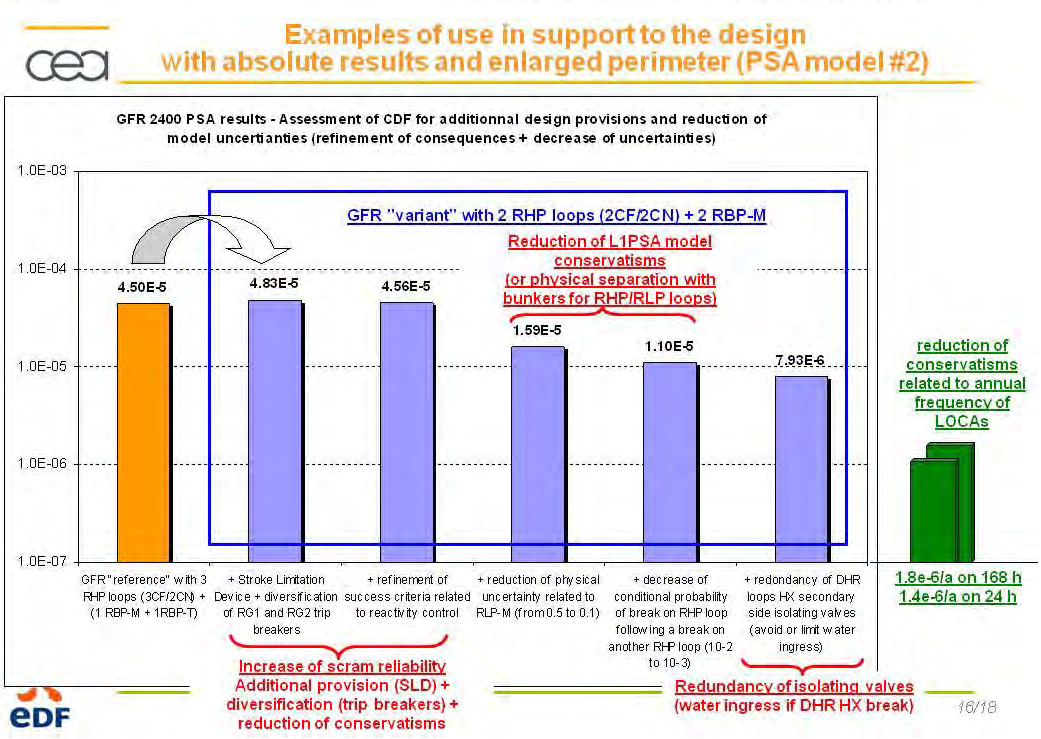
Intermediate Loop Cooling (ILC) system: operating in forced convection at air side

Secondary circuit (gas mixture) operating in natural convection (after TM rundown) / primary loop operating in forced convection (pony motor)

EDF OECD-WGRISK seminar, Paris, France, June 20-22, 2011



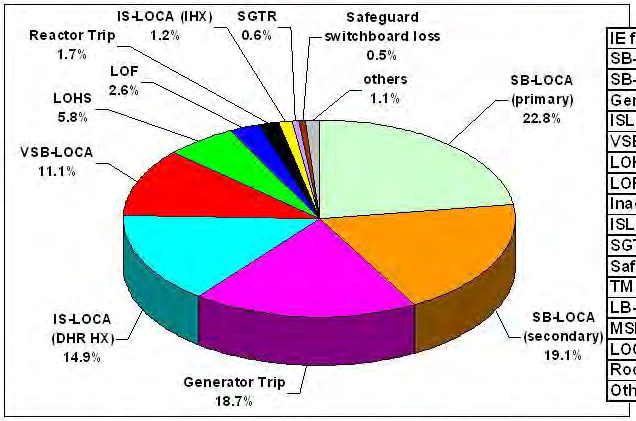

Examples of use in support to the design with absolute results and enlarged perimeter (PSA model #2)
PSA model #1
97.6%
1.2%
0.6%
0.6%
contribution of DHR SF loss in depressurized situations = 1,2%
PSA model #2
Mean
5%
Median
95%
1.0E-03
1.0E-04
1.0E-05
1.0E-06
1.0E-07
1.0E-08
4.50E-05
2.95E-05
6.06E-07
9.74E-06
5.21E-06
reactivity control 66%
DHR @ HP 1%
DHR @ MP 22%
DHR @ LP 12%
!F_all
!F_Reactivity Control
!F_DHR failure (HP)
!F_DHR failure (MP)
!F_DHR failure (LP)
Contribution to the total CDF due to the loss of DHR in « pressurized situation » (HPB intact) decreased from 98 to 1% thanks to the additionnal means implemented (AFW+ILC) and even if more pressurized situations were accounted for in the L1PSA model #2
The loss of the reactivity control now represents around 2/3 of the total CDF (and in particular following the Control Rod Withdrawal IE)
The last point is related to the contribution of LOCAs (see loss of DHR at Medium Pressure) around 22% and mainly attributed to the increase of LOCAs annual frequencies based on HTGR data
15/18
OECD-WGRISK seminar, Paris, France, June 20-22, 2011


Examples of use in support to the design with absolute results and enlarged perimeter (PSA model #2)
GFR 2400 PSA results - Assessment of CDF for additionnal design provisions and reduction of model uncertainties (refinement of consequences + decrease of uncertainties)
GFR "variant" with 2 RHP loops (2CF/2CN) + 2 RBP-M
Reduction of L1PSA model conservatisms (or physical separation with bunkers for RHP/RLP loops)
1.0E-03
1.0E-04
1.0E-05
1.0E-06
1.0E-07
4.50E-5
4.83E-5
4.56E-5
1.59E-5
1.10E-5
7.93E-6
reduction of conservatisms related to annual frequency of LOCAs
1.8e-6/a on 168 h
1.4e-6/a on 24 h
GFR "reference" with 3 RHP loops (3CF/2CN) + (1 RBP-M + 1RBP-T)
+ Stroke Limitation Device + diversification of RG1 and RG2 trip breakers
+ refinement of success criteria related to reactivity control
+ reduction of physical uncertainty related to RLP-M (from 0.5 to 0.1)
+ decrease of conditional probability of break on RHP loop following a break on another RHP loop (10-2 to 10-3)
+ redondancy of DHR loops HX secondary side isolating valves (avoid or limit water ingress)
Increase of scram reliability
Additional provision (SLD) + diversification (trip breakers) + reduction of conservatisms
Redundancy of isolating valves (water ingress if DHR HX break)
16/18

Examples of use in support to the design with absolute results and enlarged perimeter (PSA model #2)

Up-to-date results after GFR design and L1PSA model improvements

Analysis of the IE families contributing to the total CDF

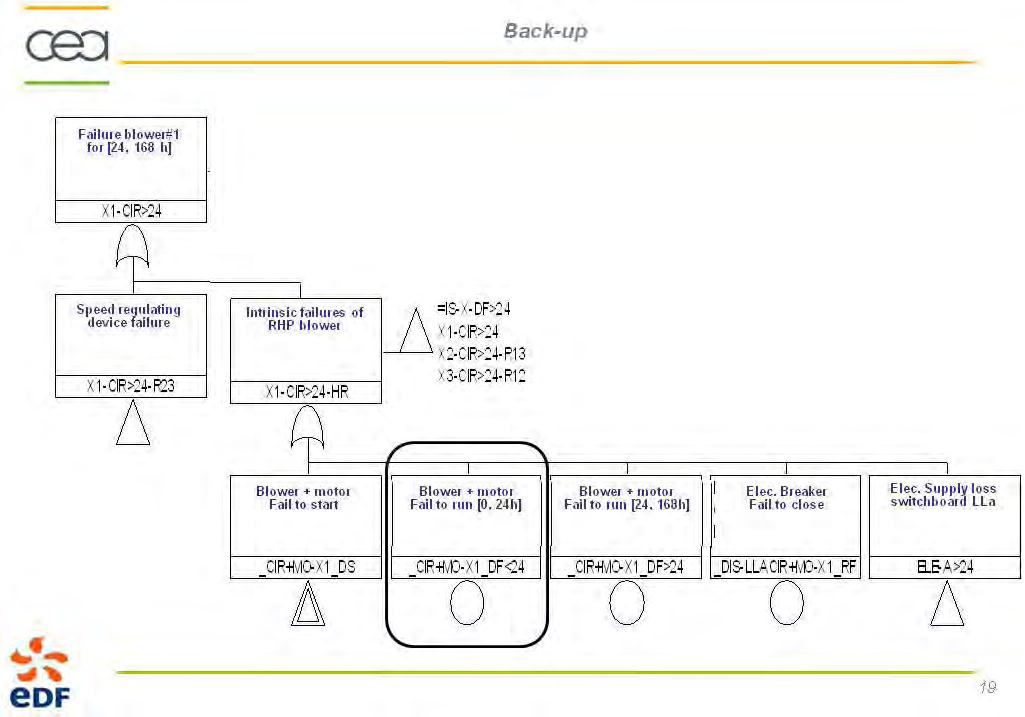


IE family	CDF (/y)	%
SB-LOCA (1ary)	3.35E-07	22.8%
SB-LOCA (2ndary)	2.81E-07	19.1%
Generator trip	2.76E-07	18.7%
ISLOCA (DHX)	2.20E-07	14.9%
VSB-LOCA	1.63E-07	11.1%
LOHS	8.53E-08	5.8%
LOF	3.82E-08	2.6%
Inadvertent reactor trip	2.49E-08	1.7%
ISLOCA (IHX)	1.71E-08	1.2%
SGTR	8.63E-09	0.6%
Safeguard switchboard loss	6.96E-09	0.5%
TM trip	6.73E-09	0.5%
LB-LOCA (1ary)	5.41E-09	0.4%
MSLB	2.92E-09	0.2%
LOOP	9.05E-10	0.1%
Rod withdrawal	4.54E-11	0.0%
Others	1.60E-08	1.1%

Prospects for SB-LOCA (primary): use of normal loops and AFW/ILC systems for DHR ?
for SB-LOCA (secondary), assessment of the conditional probability of IHX rupture
for generator trip; increase of TM bypass valve reliability

Conclusions regarding the reactor design

- At early design phase, the design team focuses on the key-points from a feasibility or technological points of view, in particular for the core and for some components (e.g. heat exchangers)
  - ⇒ the preliminary design of GFR presented an heterogeneous level of design for the various components and support systems
- The exchanges between the PSA and the design teams resulted in proposing complements in the architecture for certain gaps (e.g. power supplies, signals for the reactor trip and the DHR actuation…)
- An iterative process between the PSA and the design teams has been settled and discussions were based on the identified and shared "metric" provided by the PSA model…
- The nature of a L1PSA model (supported by neutronics, T-H, mechanics…) provide a frame for the synthesis of the available knowledge at a design stage (i.e. a kind of "knowledge traceability")
- the L1PSA model also furnish insights owing to a prioritization of computations or programs in support to the concept
- **Prospects…** PSA to support the design of ASTRID-SFR


Back-up
Failure blower#1 for [24, 168 h]
X1-CIR>24
Speed regulating device failure
X1-CIR>24-P23
Intrinsic failures of RHP blower
X1-CIR>24-HR
=IS-X-DF>24
X1-CIR>24
X2-CIR>24-P13
X3-CIR>24-P12
Blower + motor Fail to start
_CIR-HMO-X1_DS
Blower + motor Fail to run [0, 24h]
_CIR-HMO-X1_DF<24
Blower + motor Fail to run [24, 168h]
_CIR-HMO-X1_DF>24
Elec. Breaker Fail to close
_DIS-LLA CIR-HMO-X1_RF
Elec. Supply loss switchboard LLa
ELE-A>24
EDF
19

OECD/NEA WGRisk CAPS on PSA for Advanced Reactors: A Summary of Questionnaires and Answers Report

K. I. Ahn, S. J. Han, S. H. Han, and J. E. Yang

Integrated Safety Assessment Div., Korea Atomic Energy Research Institute (KAERI), 1045 Daedeokdaero, Yuseong-gu, Daejeon, 305-353, Korea, kiahn@kaeri.re.kr

Abstract

Main objectives of the WGRisk CAPS on the probabilistic safety analysis for advanced reactors which was approved by the OECD/NEA CSNI in June 2008, are to (a) characterize the ability of current PSA technology to address key questions regarding the development and licensing of advanced reactor designs; (b) characterize the potential value of advanced PSA methods and tools; and (c) develop recommendations to CSNI for any needed developments. For this purpose, the two following subtasks have been set up: (a) A survey of participating countries regarding the state of PSA technologies for advanced reactors and (b) Organization of an international workshop for detailed follow-up discussions related to the topic. In order to meet the objectives of the CAPS, the questionnaires to elicit the respondents' viewpoints had been distributed to the WGRisk member countries during the period of 2009 to 2010, and answers from the twelve countries (13 organizations) have been collected until February 2010. This paper summarizes the current status of the answers to the questionnaires and the international status and insights into PSA technologies for advanced reactors.

Keywords: OECD/NEA WGRisk, CAPS, Probabilistic Safety Assessment, Advanced Reactors

1. Introduction

1.1 Background

In June 2008, a WGRISK-proposed task on PSA of advanced reactors was approved by CSNI. (The CSNI Activity Proposal Sheet, CAPS) The approved task involved the two following sub-tasks:

- A survey of participating countries regarding the state of PSA technologies for advanced reactors;
- Organization of an international workshop for detailed follow-up discussions related to the topic.

The objectives of the "CAPS on PSA for advanced reactors" are as follows:

- To characterize the ability of current PSA technology to address key questions regarding the development and licensing of advanced reactor designs
- To characterize the potential value of advanced PSA methods and tools
- To develop recommendations to CSNI for any needed developments

In order to meet the objectives of the CAPS, the questionnaires to elicit the respondents' viewpoints had been distributed to the WGRisk member countries during the period of 2009 to 2010, and answers from the twelve countries (15 organizations) (see Table 1) have been collected until February 2010. This paper summarizes the answers to the questionnaire and the international status and insights into PSA technologies for advanced reactors.

Table 1. Respondents to the Questionnaires

Countries	Member Organizations	Respondents	E-mail
Belgium	Bel V	De Gelder Pieter	pieter.degelder@belv.be
	Tractebel Engineering (TE)		
China	Institute of Nuclear and New Energy Technology (INET)	Jiejuan TONG	tongjj@tsinghua.edu.cn
Czech Republic	State Office for Nuclear Safety	Miroslav Svab	miroslav.svab@sujb.cz
Finland	STUK	Jorma Sandberg	jorma.sandberg@stuk.fi
	VTT	Holmberg Jan-Erik	jan-erik.holmberg@vtt.fi
France	IRSN	LANORE Jeanne-Marie	jeanne-marie.lanore@irsn.fr
	CEA		
Italy	ENEA	Luciano Burgazzi	luciano.burgazzi@bologna.enea.it
Japan	Japan Atomic Energy Agency (JAEA)	Kenichi Kurisaka	kurisaka.kennichi@jaea.go.jp
Korea	Korea Atomic Energy Research Institute (KAERI)	Sang-Hoon Han	shhan2@kaeri.re.kr
Slovakia	UJD	Jan Husarcek	Jan.Husarcek@ujd.gov.sk
Slovenia	Slovenian Nuclear Safety Administration (SNSA)	Djordje Vojnovič	Djordje.Vojnovic@gov.si
UK	Health & Safety Laboratory	Shane Turner	Shane.Turner@hsl.gov.uk
USA	USNRC	Jeffery Wood	Jeffery.Wood@nrc.gov

1.2 Objectives and Scope

The answers to the aforementioned questions cover a wide spectrum of reactor types and related development programs. However, the main concerns of this report are primarily limited to common-interests of the member countries which are necessary to be discussed in the CAPS workshop. That is,

- Ability of current PSA technology to address key questions for advanced reactors;
- Potential benefits of advanced PSA methods and tools;
- Recommendations to CSNI.

1.3 Structure of the Report

The collected responses on questionnaire for advanced reactors were spanned wide spectrum of points for discussion. In order to draw out common-interest issues among the member countries, it is primarily necessary to clearly give the definition and developmental status of advanced reactors as a starting point for an effective discussion on the task. Those questions for advanced reactors were mentioned as a key point in the questionnaire responses. It was expected that by the foregoing approach the difference between PSA technologies for different reactors could be reduced. As the result, common issues for the advanced reactors were identified. The structure of this report has been rearranged as follows:

1. Introduction
2. Ability of current PSA to address key questions for advanced reactors
3. Potential benefits of advanced methods and tools
4. Potential recommendations for CSNI

Appendix A: Questionnaires and compilation of responses (to be provided later)

2. Ability of the current psa to address key questions for advanced reactors

2.1 Definition of Reactors and Developmental Status

There is currently a wide spectrum of advanced reactors in the state of proposed and developmental status, but the underlying definitions of advanced reactor seem not to exist. This means that the key questions for advanced reactors could be differentiated according to their definition and relevant terminology, and thus they should be the primary topics to be discussed in the workshop. This report does not provide a specific classification of advanced reactors to avoid distracting arguments over correctness and completeness, etc. The reactors nominated as advanced reactors from the questionnaire responses are listed in Table 2 to support the foregoing process.

Table 2. Reactors Nominated as Advanced Reactors in Questionnaires

Category	Lists of Reactors Nominated for Answering Questions
Non LWRs	SFR, FBR, JSFR, Lead Fast Reactor, GFR, GTMHR, PBMR, VHTR
LWR Types	SWR1000, OPR1000, APR1400, EPR, EPR1600, AP1000, ESBWR ABWR, APWR, VVER MIR-1200, AES-2006
SMR Types	SMR, SMART

2.2 Key Questions Distributed to Member Countries

While many applications of PSA for advanced reactors seem to be made with current PSA technologies, a few countries are considering the development of PSA technologies specialized for the advanced reactors. This means that many portions of the current PSA technologies can be applied to advanced reactors except for some specific issues to advanced features (e.g., the reliability of passive systems). However, further efforts to apply the PSA technologies to advanced reactors are required because the design and development stages of some advanced reactors (e.g., Gen IV reactors) were not clear making the application of the advanced PSA technologies difficult. For reference, the key questions which were posed to advanced reactors from member countries were briefly introduced in the questionnaire to help answers the questions in Table 3. The identification of those questions reflects positions of the regulatory body of each member country. The current regulation which is based on the deterministic approach may require a little effort on a development of PSA technologies for advanced reactors. The current regulation framework which is currently being shifted to the risk-informed approach (employing both deterministic and probabilistic viewpoints) may require a further improvement of the existing PSA technologies from which more reasonable decision-making could be made for the plant risk in a integrated way. Since the risk-informed approach adds the probabilistic insights for their safety evaluation to the existing deterministic viewpoints, key issues to be discussed in the workshop should reflect the following aspects:

- Scope and quality of the PSA insights which are required in the decision-making process for advanced reactors;
- Coincidence of the deterministic principle (e.g., defense-in-depth) with PSA insights in the regulation framework;
- Risk metrics specific to advanced reactors as compared to the existing ones (e.g., CDF/LERF) and the relevant physicochemical characteristics.

Specifically, the following issues could be discussed in the workshop:

- Scheme to determine technical acceptability of PSA for advanced reactors, which is closely related to the preparation of PSA standard to check the quality of PSA and provide its implementation process, together with the well-establishment of surrogate risk metrics for advanced reactors;

- Aggregation of the risk from different hazard types for the inclusion of external hazards into internal hazard.

The key questions collected from the member countries were rearranged so that only technical ones without considering the regulation aspects were classified for the CAPS objectives. The underlying questions are as follows:

- Further improvement of the existing methods (including modelling and analysis of the physical behaviour which is required to determine the PSA information);
  - Applicability of new methods for PSA tools (Non ET/FT methods)
  - Combination of deterministic and probabilistic analysis results
  - Containment performance including severe accident phenomena and their countermeasures
  - Source terms and off-site probabilistic consequence analysis
- Specific issues on advanced reactors PSA;
  - Identification and quantification of initiating events including events classification (AOO/DBA/BDBA)
  - Reliability database for new SSCs and features
    - ✓ Reliability of passive systems by new methods including the aforementioned combined approaches
    - ✓ Reliability of digital I&C systems including new EOP under new design features
  - Human reliability under new design features
- Application of risk information in the design stages.

Table 3. Typical Issues with Which Should be Considered within the Framework of PSA

Category	Specific Issues which should be resolved
PSA scope	- Hazard types: Internal events, External events (fire, flooding, seismic, etc)
	- Operating Modes: Full power PSA, Low power and shutdown PSA
PSA framework	- The applicability of the current PSA frameworks (e.g., Level 1, 2 and 3 PSA). - The definition of risk metrics such as plant damage states (incl. core damage state). - The appropriate methods, models, and tools for the assessment (including source term release categorization and consequence analyses) - The quality of PSA implementation is a supplemental issue in company with PSA scope
Specific technical issues	- Reliability database for advanced reactors (e.g., Initiating events, SSCs, CCF etc) - Reliability of passive systems - Reliability of Digital I&C systems - Human reliability under new advanced design features such as a digital man-machine interface - Containment/confinement performance including severe accident phenomena and their countermeasures - Deterministic source terms assessment - Treatment of multiple reactor modules

2.3 Ability of the Current PSA Technologies

Although there is a large spectrum of the current PSA technologies which can be defined according to their quality, there seems to exist only small problems associated with practical application of the current PSA technologies to PSA for advanced reactors. For the time being, however, the specific technical issues to each of the distinctive features of advanced reactors have to be resolved with the current PSA capabilities. For instance,

- Reliability of passive systems;
- Treatment of severe accidents and their countermeasures;

- Reliability of new SSCs (new features, digital I&C etc) and their treatments;
- Uncertainty and sensitivity.

Additionally, special issues on the nuclear safety (e.g., aircraft crash, physical protection, etc) are raised as an extended scope of PSA. To resolve these special issues, deterministic approaches for physical/mechanical analysis could be required as a basis of PSA implementation.

A major trend of the PSA technologies for fleets of the existing reactors is to extend the PSA scope and to require a precise quantification of uncertainty to reduce an unnecessary burden to conservatism. It is also expected that PSA technologies for advanced reactors be in the same line with the existing reactors. For the time being, the current PSA technologies will also be used in the PSA for advanced reactors without a greater change. This reflects the current situation that some issues on PSA for advanced reactors have not been clearly defined yet. It is expected that a development of PSA technologies for advanced reactors will be improved according to the development status of advanced reactors. Since it is expected that the risk-informed concept will be actively used in the design stage of new and advanced reactors, it is necessary to draw out and discuss the relevant issues in the workshop.

Finally, it is noted that specific PSA technologies have been developed for some advanced reactors such as a VHTR (including relevant risk metrics), although this is a subsidiary part on the development of new PSA technologies thus for.

3. Benefits of advanced methods and tools

3.1 Advanced Methods and Tools in Use

Advanced methods and tools currently exist for the improvement of PSA technologies. Some portions of them involve means to more explicitly tie the phenomenological modelling and uncertainty assessment into the PSA, e.g., RMPS, MOSAIQUE, SM2A, and DDETs. While those methods have a potential value to their application for advanced reactors, there is no clear guidance on how to apply PSA for advanced reactors yet. However, the foregoing items could be considered potential areas to discuss further in the workshop.

The remaining issues to discuss in the workshop are mainly related to the phenomenological models themselves. For example, containment performance including severe accident phenomena, source terms risk, and their countermeasures could be critical in determining the risk of advanced reactors. The forgoing topics could be involved in the realm of PSA where they can be used to more explicitly tie phenomenological modelling in the PSA, an otherwise deterministic area. Currently, there seems not exist any consensus on how to take into account severe accident phenomena for some advanced reactors and on the level of depth to take into account. From the viewpoint of plant risk, they should be included as topics for discussion in the workshop.

3.2 Further Development of Methods and Tools

The following issues on PSA for advanced reactors require further developments of the relevant methods and tools:

- Identification and quantification of initiating events including events classification (AOO/ DBA/ BDBA);
- Reliability database for new SSCs and features;
  - Passive systems by new methods including the aforementioned combined approaches
  - Digital I&C systems including new emergency operation under these new circumstance
- Human reliability under new advanced design features;
- The application of risk information into their designs.

Table 4 shows more detailed questionnaires prepared for respondents, based on the foregoing issues.

Table 4. Key Questionnaires Prepared for Respondents

Category	Key Questionnaires
Improvement of estimation methods	Applicability of new methods for PSA tools (Non ET/FT methods)
	Combination of deterministic analysis and probabilistic analysis
	Containment performance including severe accident phenomena and their countermeasures
	Source terms and off-site probabilistic consequence analysis
Specific issues on advanced reactors PSA	Identification and quantification of initiating events including events classification (AOO/DBA/BDBA)
	Reliability database for new SSCs and features
	Passive systems by new methods including the aforementioned combined approaches
	Digital I&C systems including new emergency operation under these new circumstance
	Human reliability under new advanced design features
The application of risk information into their designs	

4. Potential recommendations for CSNI

4.1 Activities of Other International Organizations

There have been a number of international activities on PSA for advanced reactors, such as:

- The IAEA is developing a proposal for a Coordinated Research Program (CRP) on passive systems reliability;
- The CNRA has formed a Working Group on the Regulation of New Reactors (WGRNR);
- The Generation IV International Forum (GIF) conducts an assistance group as the Risk and Safety Working Group (RSWG) for the risk-informed safety evaluation of Gen-IV reactors.

The understanding of the state of art for the improvement of PSA technology to be drawn from the foregoing activities will help to establish and refine the research and development roadmaps or programs of each country. In addition, the present CAPS will effectively guide the relevant international cooperation, and the relevant findings and insights regarding PSA technologies will be worth coordinating the future activities of advanced reactors PSA.

4.2 Topics for Discussion in the Workshop

Potential topics for discussion in the present CAPS workshop may include:

- Clearer definition of ‘technical issues’ and survey of specific research items that need to be addressed;
- Application of PSA to advanced reactors, extent to which ongoing R&D should address future issues where additional work is needed, and with what priority;
- Potentially beneficial international cooperative activities. For examples,
  - Reactor-specific accident phenomena and issues,
  - Establishment of reactor-specific reliability databases,
  - Redefinition of risk metrics and their evaluation methods,
  - Feasibility of technical neutral framework to advanced reactors.

OECD/NEA Workshop on PSA for New and Advanced Reactors,
June 20- 22, 2011, OECD Headquarter, Paris.

The Current Status of CAPS Activity on PSA for Advanced Reactors

Kwang-Il AHN
(kiahn@kaeri.re.kr)

Korea Atomic Energy Research Institute
(KAERI)

원자력 안전연구 글로벌 리더, **GLOBAL LEADER IN NSR !**

OUTLINES

- **CAPS WS on PSA of Advanced Reactors**
  - **A Brief History**
  - **Overview of the Workshop**
- **CAPS Q/As on PSA of Advanced Reactors**
  - **Main Objectives**
  - **Key Questionnaires & Respondents**
  - **Preliminary Findings** Observations
  - **Recommendation to CSNI**

CAPS Workshop

1. Planned workshop schedule

- **Approved by CSNI June 2008,** a WGRisk-proposed task on PSA for advanced reactors (CAPS) involves the following sub-tasks:
  - A survey of participating countries regarding the state of PSA technologies for advanced reactors;
  - Organization of an international workshop for detailed follow-up discussions related to the topic (**Date/Venue**: 2010.4.6-7, Daejeon, Korea, **KAERI as Lead organization**)

2. Discussions in the 11th WGRisk Annual Meeting (March 2010)

- Due to small number of abstracts received at that time, **Participants discussed and agreed to possible links with the activity on "PSA in the frame of new NPPs"** proposed by IRSN, 2010.

3. Announcement of the rescheduled workshop on "OECD/NEA Workshop on PSA for New & Advanced Reactors" (**Date/Venue:** June 20-24, 2011, OECD Conference Center, **KAERI and IRSN as Lead organizations**)

Korea Atomic Energy Research Institute

3

CAPS Workshop

4. WS Organizing Committees Meeting

- **March 28, 2010,** OECD Marshall Building Meeting Room 2122
- **Discussion on**
  - Common workshop & session organization
  - Status of preparation of each CAPS report
  - Issuing a common report raised by the WGRisk Chair and position of both task group leaders

5. Preparation of the Relevant CAPS Report

- **Feb, 2011 :** A summary of the member countries' responses to the CAPS questionnaires, submitted to the WGRisk Secretariat and Chairman.
- **June 2011 :** Summary report on the workshop to be prepared.
- **June 2012 :** CSNI task report to be published as a common report.

Korea Atomic Energy Research Institute

CAPS Workshop

6. A Summary of Papers to be presented in the workshop

National contributions (35 papers from 12 countries)

	France	USA	Korea	China	Japan	Germany	Others	Total
Papers	8	9	4	3	2	2	7	35

(*) Others (1 paper per country) : Belgium, Finland, Italy, Russia, UK, India, IAEA

Category	France	USA	Korea	China	Japan	Germany	Others	Total
New	3	4		3			3	13
Advanced	4	3	3		2	1	1	14
Common	1	2	1			1	3	8

(*) **New:** Gen-III/III+(EPR/AP1000/ABWR…); **Advanced:** Gen-IV (HTGR/VHTR/FBR/SMR…)

Category	France	USA	Korea	China	Japan	Germany	Others	Total
Level 1	7	1	2	2	1	1	2	16
Level 2	1	1			1	1	1	5
Common		7	2	1			4	14

Korea Atomic Energy Research Institute

5

CAPS Workshop

Workshop Program (Final)

	June 20 (Advanced)	June 21 (New)	June 22 (Common)	June 23-24
Morning	N. SIU	JM. LANORE	G. GEORGESCU	Editing of Summary Report - TG Leaders - Supporting group
	Tech. session (4 papers)	Tech. session (4 papers)	Tech. session (3 papers)	
	A. BAREITH	R.J. LUTZ	T. LEAHY	
	Tech. session (4 papers)	Tech. session (4 papers)	Tech. session (4 papers)	
Afternoon	M. MARQUES	R. VIROLAINEN	L. BURGAZZI	
	Tech. session (4 papers)	Tech. session (4 papers)	Tech. session (4 papers)	
	K. AHN	G. GEORGESCU	A. AMRI	
	Break-up session (PSA of advanced reactors)	**Break-up session** (PSA for new designs)	**Common discussion session**	

Korea Atomic Energy Research Institute

CAPS Q/As for advanced reactors

- **Objectives of the "CAPS on PSA for advanced reactors" :**
  - To characterize the ability of current PSA technology to address key questions regarding the development and licensing of advanced reactor designs;
  - To characterize the potential value of advanced PSA methods and tools;
  - Recommendations to CSNI for any additionally needed developments.

- **Objectives of the Questionnaires**
  - To elicit the respondent's viewpoints on a number of topics relevant to the objectives of the CAPS;
  - The answers to the questionnaires, combined with the results of follow-up discussions in the Workshop, will provide the basis for the final draft report, presenting the international status and insights of PSA technologies for advanced reactors.

Korea Atomic Energy Research Institute

7

CAPS Q/As for advanced reactors

- **Key Questionnaires Distributed:**

Category	Key Elements
General questions	▪ R&D status for advanced reactors ▪ Types of advanced reactors under consideration ▪ Regulation framework for advanced reactors ▪ The current status of advanced reactors' PSA
Technical issues on PSA of advanced reactors	▪ Use of PSA in RIDM for advanced reactors, ▪ PSA modelling for advanced reactor-specific features ▪ Regulatory issues for advanced reactors
Research activities on PSA of advanced reactors	▪ Technical issues and PSA topic areas ▪ Technical approaches to solve those issues ▪ Lead organizations for R&D activities ▪ Milestones & status for R&D activities ▪ Regulatory application of PSA for advanced reactors
International cooperation	PSA-relevant topics for further intl. collaboration

Korea Atomic Energy Research Institute

8

CAPS Q/As for advanced reactors

❒ **Respondents to the Questionnaires** (12 countries. 15 organizations)

Regulatory Body	Research Institutes	Academia
BEL V/TE-Belgium NRC-USA SNSA-Slovenia STUK-Finland SUJB-Czech R. UJD-Slovakia	CEA/IRSN-France ENEA-Italy HSL-UK JAEA-Japan KAERI-Korea VTT-Finland	INET-China

❒ **Contributors to the Answers**

Answers	Member Countries	R&D Status for Advanced Reactors
Major	China, France, Japan, Korea, USA	Ongoing, Major Activities
Limited	Czech R., Finland, UK	Planed, but Minor Activities
Minor	Belgium, Italy, Slovenia, Slovakia	No Plan or Little Activities

Korea Atomic Energy Research Institute

9

CAPS Q/As: Findings and Observations

❒ **General Points:**

- The questionnaire answers were spanned wide spectrum of reactor types and associated programs, i.e., mixture of new/evolutionary and advanced reactors ?

Reactor Types	Typical Reactors
New/Evolutionary LWRs with advanced safety features	ABWR, APWR, AP1000, EPR, ESBWR, APR1000, APR1400, SWR 1000, WWER MIR-1200, iPWR, etc
New LWR of modular types	SMR, SMART, etc
Non-LWR types (Gen-IV)	Liquid-cooled reactor (LMR, SFR, FBR), Gas-cooled reactor (HTGR, VHTGR, GTMHR, PBMR, GFR) ...

- **The questionnaire answers** seem reflect reactors in answers (*either new/ evolutionary or advanced reactors, or both*).
- **In order to draw out common-interest issues among the member countries and classify PSA technologies required specially for different reactors, it seems necessary to clearly discriminate a difference between evolutionary and advanced reactors.**

Korea Atomic Energy Research Institute

10

CAPS Q/As: Findings and Observations

- **A few questionnaire answers are addressing the potential use of regulatory approaches where risk plays a greater role.**
  - *However, these activities have not yet led to actual changes in regulation and moreover many other countries in answer are not developing new approaches for advanced reactors and relevant PSA technologies yet.*
- **The questionnaire answers seem to express differing viewpoints on scope of hazards, and framework and technology of the PSA** to be treated in advanced reactors, similarly with operating reactors.
  - Some respondents express the applicability of Level 1/2/3 for some reactor types, others have no issue;
  - Some respondents expect treatment of all modes and all hazards, others are more limited;
  - *Some respondents think current ET/FT technology is fine, some are doing research, some are using different methods for certain problems, e.g., simulation-based approaches such as RMPS and BEPU for passive systems.*

Korea Atomic Energy Research Institute

11

CAPS Q/As: Findings and Observations

A.4 Answers to the current status of advanced reactors PSA?

Members	Hazard types	Operating modes	PSA Levels covered	Any special PSA method	Reactors being applied
China	Internal hazard & earthquake	all operating modes	Level 1 & 2	No special PSA method	HTGR
France	all hazards				SFR & GFR
Japan	Internal hazard & earthquake				SFR
Korea	all hazards		Level 1 - 3	No special PSA method, except PSR	advanced non-LWRs (SFR, VHTR)
USA				No programs for special PSA method	advanced non-LWRs (SFR, HTGR/VHTR)
Czech R.			Level 1 & 2	N/A	New & Evolutionary LWRs (Expected)
Finland					
UK			Level 1 - 3		
Others	N/A				

Korea Atomic Energy Research Institute

12

CAPS Q/As: Findings and Observations

- **The questionnaire answers express many technical and regulatory issues which should be resolved for advanced reactor designs.**
  However, many of them do not seem to think that advanced reactors pose fundamentally different types of challenges or that methodological work for digital, passive systems, HRA, etc. is expected to be generally applicable for a wide variety of designs. Nevertheless they may have relatively greater importance to advanced reactors.

CAPS Q/As: Findings and Observations

Key Elements for PSA of Advanced Reactors

Category	Specific Issues which should be further discussed
PSA scope	▪ Hazard types: Internal events, External events (fire, flooding, seismic, etc) ▪ Operating Modes: Full power, Low power and shutdown
PSA framework	▪ Applicability of the current PSA frameworks (e.g., Level 1, 2 and 3 PSA) ▪ Applicability of the current risk metrics (CDF and/or LERF/LRF) ▪ Appropriate methods, models, and tools for the assessment (including CD, PDS, STC and consequence analyses) ▪ Quality of PSA implementation as a supplemental issue in company with PSA scope
Specific technical issues	▪ Reliability database for advanced reactors (e.g., IEs, SSCs, CCF etc) ▪ Reliability of passive safety systems and Digital I&C systems ▪ Human reliability under advanced design features such as a digital MMI ▪ Containment/confinement performance including severe accident phenomena and their countermeasures ▪ Deterministic source terms assessment ▪ Treatment of multiple reactor modules

CAPS Q/As: Findings and Observations

- **Advanced Methods and Tools:**
  - **Much of the questionnaire answers take into account *a direct extension of the existing PSA methods to new reactor systems*** *(e.g., reliability databases, development and application of appropriate PSA models for advanced reactors)*
  - **Some questionnaire answers address *development of new methods-related work for challenging topics*** *(e.g., DI&C, HRA, Level 2 under advanced design features)*
    - *However, they do not seem to be aimed at specific reactor types.*
  - **A few questionnaire answers express *the use of the non-ET/FT methods/tools as a mean to more explicitly tie phenomenological modeling into the PSA*** *(e.g., RMPS, DDETs)*
    - *While those methods have a potential value for their application to advanced reactors, however, there is no clear guidance on how to incorporate into the PSA framework for advanced reactors yet.*

CAPS Q/As: Findings and Observations

- **A few questionnaire answers also address *the need of advanced reactor-specific SA analysis models, definition of source terms risk, and their countermeasures*** *which could be critical in determining the risk of advanced reactors*
  - *While they could be involved in the realm of PSA, however, there seems not currently exist any consensus on how to take into account those issues for some advanced reactors and on the level of depth to take into account.*
- **Regarding non-traditional topics for advanced reactors, there is little respondents in answers** *(e.g., non-probabilistic methods for dealing with uncertainties, use of formal modeling concepts to support model standardization and review).*

CAPS Q/As: Findings and Observations

Items for Further Discussion

(1) Further improvement of the existing methods
- Applicability of new PSA methods/tools for advanced reactors (Non ET/FT methods)
- Combination of deterministic and probabilistic analysis results
- Containment performance including SA phenomena and their countermeasures
- Source terms and off-site probabilistic consequence analysis

(2) Specific issues on advanced reactors PSA
- Identification and quantification of IEs including events classification (AOO/DBA/BDBA)
- Reliability database for new SSCs and features
  - Reliability of passive systems by new methods including the aforementioned combined approaches
  - Reliability of DI&C systems including new EOP under new design features
- Human reliability under new design features

(3) Application of risk information in the design stages

Korea Atomic Energy Research Institute

17

CAPS Q/As: Findings and Observations

❒ **Regulation and Risk-informed Approach:**

- **The regulation framework which is currently being shifted to the risk-informed approach** *may require a further improvement of the existing PSA technologies from which more reasonable decision-making could be made for the plant risk in a integrated way.*
- **Key issues to be considered for advanced reactors:**
  - ☐ Scope and quality of the PSA insights *which are required in the decision-making process for advanced reactors;*
  - ☐ Coincidence of the deterministic principle *(e.g., defence-in-depth) with PSA insights in the regulation framework;*
  - ☐ Risk metrics specific to advanced reactors *as compared to the existing ones (e.g., CDF and LERF/LRF) and the relevant physicochemical characteristics.*

Korea Atomic Energy Research Institute

18

CAPS Q/As: Findings and Observations

Items for Further Discussion

Scheme to
- **determine technical acceptability of PSA for advanced reactors, which is closely related to the preparation of PSA standard to check the quality of PSA and,**
- **provide its implementation process, together with the well-establishment of surrogate risk metrics for advanced reactors**

- **Aggregation of the risk from different hazard types** for the inclusion of external hazards into internal hazard.

CAPS Q/As: Potential Recommendation to CSNI

For the Use of PSA in Design, RIDM, and Regulatory Phases,

- Further survey to address future issues where additional work for advanced reactors, the extent to which ongoing R&D should address those issues, and with what priority.
- Clearer definition regarding accident sequences for PSA modelling to advanced reactors and adequacy of current phenomenological models to support the analysis;
- Assessment for the possibility of potential severe accidents as early as possible during the pre-conceptual design phase.

R&D Topics for Future International Collaboration:

- Reactor-specific accident phenomena and issues,
- Establishment of reactor-specific reliability databases,
- Redefinition of risk metrics and their evaluation methods,
- Feasibility of technical neutral framework to advanced reactors.

CAPS Q/As: Potential Recommendation to CSNI

D.1 Answers to the PSA-relevant topics for future intl cooperation?

Members	Key Responses
China	All the international activities will be helpful for the advanced reactor PSA
France	▪ **Harmonization of the regulatory requirements regarding PSA (safety goals);** ▪ **Sharing of reliability DBs for components and initiators** specific to different reactor concepts; ▪ **Development of a methodology to take into account severe accidents** as early as possible during the pre-conceptual design phase.
Japan	▪ **Effectiveness SA measures of SFR for the regulatory body** ▪ **Pilot PSA study for SFR (e.g., Monju)**
Korea	▪ **Surrogated safety goals** for advanced non-LWRs; ▪ **Development of standard or guidance on technical acceptability** for advanced non LWR PSAs; ▪ DI&C PSA and HRA under digital environment; ▪ HRA for shutdown PSA and external event PSA; ▪ Seismic PSA (to reduce uncertainty) and Aircraft crash risk analysis; ▪ Collection of possible non-LWR specific initiating events or its guidance for selecting; ▪ **Reliability of passive safety systems and Methodology and tool for SA analysis.**
USA	**The MDEP discussions focusing on advanced reactor designs** may share experience and understand technical issues encountered in the licensing process of other regulators, **including**

Korea Atomic Energy Research Institute

21

Thank you !

Korea Atomic Energy Research Institute

22

APPLICATION OF FAULT TREE METHODOLOGY TO MODELING OF THE AP1000®[4] PLANT DIGITAL REACTOR PROTECTION SYSTEM

David S. Teolis, Stacy A. Zarewczynski, Heather L. Detar
Westinghouse Electric Company LLC, 1000 Westinghouse Dr., Cranberry Twp., PA 16066 USA
teolisds@westinghouse.com

Abstract

*The reactor trip system (RTS) and engineered safety features actuation system (ESFAS) in nuclear power plants utilizes instrumentation and control (I&C) to provide automatic protection against unsafe and improper reactor operation during steady-state and transient power operations. During normal operating conditions, various plant parameters are continuously monitored to assure that the plant is operating in a safe state. In response to deviations of these parameters from pre-determined set points, the protection system will initiate actions required to maintain the reactor in a safe state. These actions may include shutting down the reactor by opening the reactor trip breakers and actuation of safety equipment based on the situation. The RTS and ESFAS are represented in probabilistic risk assessments (PRAs) to reflect the impact of their contribution to core damage frequency (CDF). The reactor protection systems (RPS) in existing nuclear power plants are generally analog based and there is general consensus within the PRA community on fault tree modeling of these systems. In new plants, such as **AP1000**® plant, the RPS is based on digital technology. Digital systems are more complex combinations of hardware components and software. This combination of complex hardware and software can result in the presence of faults and failure modes unique to a digital RPS. The United States Nuclear Regulatory Commission (NRC) is currently performing research on the development of probabilistic models for digital systems for inclusion in PRAs; however, no consensus methodology exists at this time. Westinghouse is currently updating the **AP1000**® plant PRA to support initial operation of plants currently under construction in the United States. The digital RPS is modeled using fault tree methodology similar to that used for analog based systems. This paper presents high level descriptions of a typical analog based RPS and of the **AP1000**® plant digital RPS. Application of current fault tree modeling techniques to the digital system is reviewed, and unique issues related to accounting for common cause failures and software failures are discussed.*

Key Words: Reactor Protection, Instrumentation and Control, Analog, Digital

1. Introduction

The reactor protection system (RPS) for Westinghouse (W) Nuclear Steam Supply System (NSSS) plants is compromised of the reactor trip system (RTS) and the engineered safeguards features actuation system (ESFAS). The function of the RPS is to sense abnormal transient situations and initiate a reactor trip and actuate specific safety related components to mitigate the events. 10 CFR 50 Appendix A, Criteria 20 states "The protection system shall be designed; 1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and, 2) to sense accident conditions and to initiate the operation of systems and components important to safety". With regard to reliability, Criteria 21 states "… Redundancy and independence designed into

[4] AP1000 is a trademark or registered trademark in the United States of Westinghouse Electric Company LLC, its subsidiaries and/or its affiliates. This mark may also be used and/or registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function…". These criteria are applicable regardless of the basis of the design of the RPS; analog or digital. Section 2 provides a high level description of a typical W NSSS RPS. Digital based protection systems perform similar functions; however, signal processing and communications are performed by processor and communication modules that use digital signals instead of analog signals. Section 3 provides a high level description of the **AP1000®** plant digital based RPS. Planned application of traditional fault tree methodology to the **AP1000®** digital RPS is discussed in Section 4. Unique digital system issues related to availability of failure data and software failures are also discussed.

2. Current W NSSS RPS description

The W NSSS RPS consists of process sensors or transmitters, the process protection system, the logic cabinets, and the reactor trip breakers and actuation relays. Figure 1 shows the RPS. The process protection system includes a number of analog channels which process or condition the signal received from a sensor and provide a signal to each of two logic cabinets. In the logic cabinet, the actuation logic is performed and signals are provided to the RTBs and actuation relays. The actuation relays consist of master and slave relays. The master relays received the signal from the logic cabinet and control a number of slave relays. The slave relays typically control the safeguards equipment. In the current plants, the process protection system is analog, such as the 7300 system, or digital, such as the Eagle 21 system. The logic is performed either by solid state components and combinations of relays.

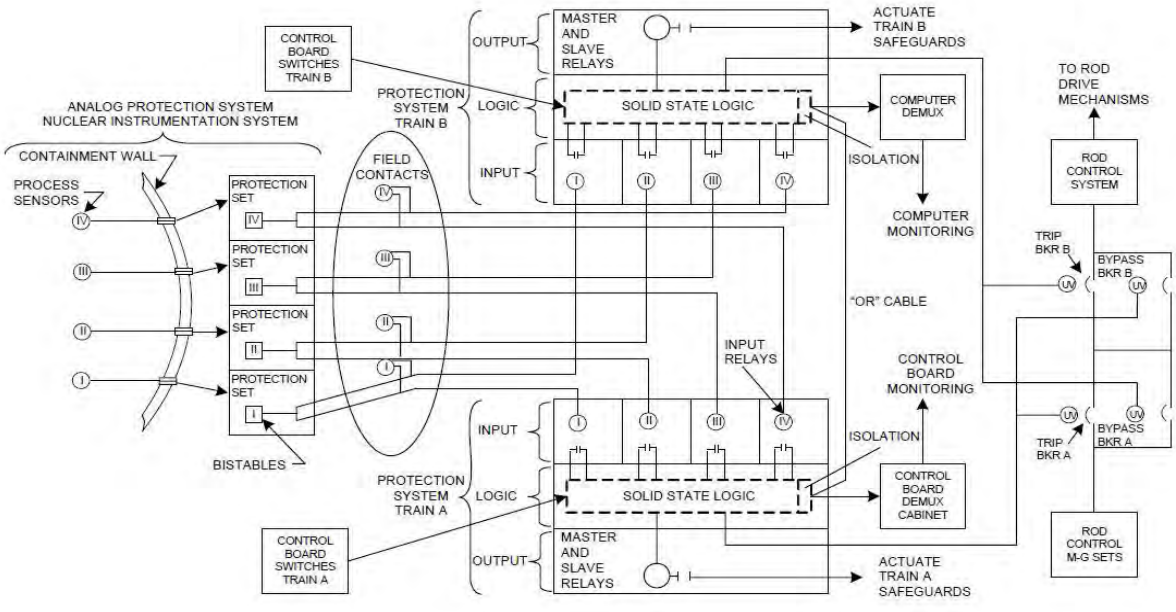


Figure 1. RPS Simplified Diagram

A typical analog channel consists of a sensor, a channel power supply, signal conditioning circuits, and a comparator which is the output device to the logic cabinet. The sensor measures physical parameters such as temperature, pressure, level, etc. The measurement is converted to an electrical signal and transmitted to the protection racks for signal conditioning. Each analog channel is also dependent on its corresponding DC power supply. The signal conditioning modules perform a number

of functions including amplification, square root derivation, lead/lag compensation, integration, summation and isolation. A signal comparator, usually a bistable device, compares the conditioned signal to a predetermined setpoint and turns the output off or on if the voltage exceeds the setpoint. Each bistable controls two relays; one for Train A logic and the other for Train B logic.

The combinational logic is performed in the logic cabinet. This is where the one-out-of-two, two-out-of-three, or two-out-of-four logic is evaluated for actuation of the RTBs or master and slave relays. Each logic cabinet consists of the input bay which contains the input relays, the logic bay, and the output bay which contains the master and slave relays. The input bays are arranged such that all inputs are physically and electrically isolated. The logic bay is where all the logic decisions are made and where the majority of SSPS system tests are performed. The output bays are the interface between the logic circuits and the safeguards equipment. There are some variations to this configuration with multiple output bays.

The SSPS receives inputs from the analog channels via the input relays. This is accomplished using relays in either an energized or de-energized state, as determined by the output of the comparator. When a comparator senses a trip condition the corresponding input relay will energize as appropriate, applying a ground to a specific logic input. The logic inputs are applied to universal logic boards which are the basic circuits of the protection system. These boards contain one-out-of-two, two-out-of-three, or two-out-of-four logic circuits. Grounding of the appropriate number of universal board inputs will cause a signal to be generated. Output signals from the universal boards are connected to other universal boards, undervoltage output boards, or safeguard output boards as described:

1. Connection to other universal boards enables additional logic combinations. For example, auxiliary feedwater may be started by low level in one steam generator as sensed by 2 of 3 channels. Each of the three steam generator channels for one steam generator would input to a 2 of 3 universal boards. For a three-loop plant there would be three such circuits. The output of each of these universal boards would input to a 1 of 3 universal boards to achieve the desired logic.

2. Connection to undervoltage output boards to drive the undervoltage relays to trip the RTBs which results in a reactor trip.

3. Connection to safeguard output boards to drive the master relays which in turn drive the slave relays which actuate safeguards equipment.

The master and slave actuation relays function to start the safeguards equipment which is used to mitigate events. This is accomplished by a combination of relay operations initiated by the output of the logic circuit. Each master relay energized by the logic circuit closes contacts which energize one or more slave relays. The number of master and slave relays is dependent on the particular protective function. The more complex the function, the greater the number of relays energized. Each slave relay, when energized, closes contacts in the actuation circuits for one or more pieces of equipment.

3. AP1000® Plant digital RPS description

Similar to the analog based RPS in current plants, the **AP1000®** plant digital protection system provides detection of off-nominal conditions and actuation of appropriate safety-related functions necessary to achieve and maintain the plant in a safe condition. The Protection and Monitoring System (PMS) controls safety-related components in the plant that are operated from the main control room (MCR) or remote shutdown workstation. In addition, the PMS provides the equipment

necessary to monitor the plant's safety-related functions during and following an accident as required by Regulatory Guide 1.97 [1].

The **AP1000®** plant digital RPS consists of four redundant divisions designated A, B, C, and D, as described in WCAP-16675 [2] and depicted on Figure 2. The system performs the necessary safety-related signal acquisition, calculations, setpoint comparison, coincidence logic, RT/ESF actuation functions, and component control functions to achieve and maintain the plant in a safe shutdown condition. It also contains maintenance and test functions to verify proper operation of the system. The system includes four redundant safety displays, one for each division, located in the MCR. Four redundant divisions are provided to satisfy single failure criteria and improve plant availability.

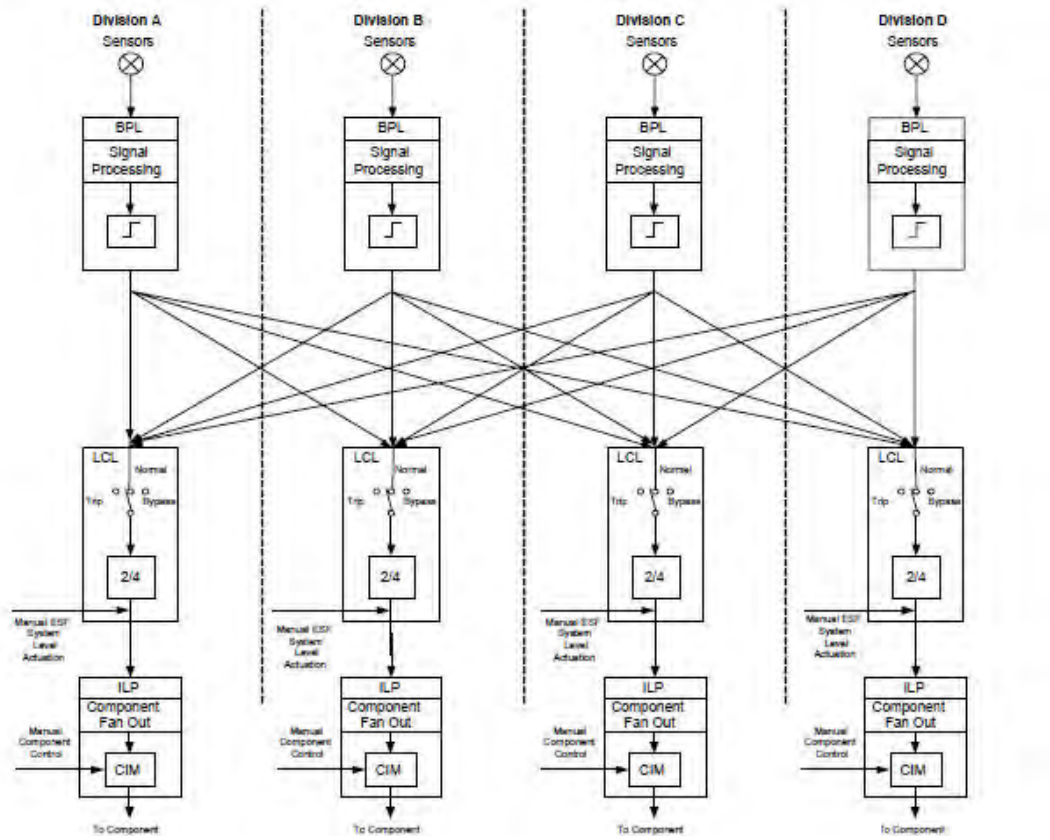


Figure 2. AP1000® Plant Digital RPS Simplified Diagram

Related sensors and the reactor trip switchgear are, for the most part, four-way redundant for I&C equipment used for reactor trip and ESF actuation functions. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic. Four redundant measurements of each variable for reactor trip criteria are obtained by the use of four separate sensors. One measurement is processed by each division. Analog signals are converted to digital form by analog-to-digital converters (ADCs) within the division's bistable processor logic (BPL). Signal conditioning is applied to selected inputs following the conversion to digital form. Following necessary calculations and processing by the BPL, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a parameter is generated if the channel's measurement exceeds its predetermined or calculated limit. Processing of variables for reactor trip is identical in each of the four redundant divisions of the protection system.

The local coincidence logic (LCL) in each division is capable of generating a reactor trip signal if two or more of the redundant channels for a single variable are in the partial trip state. The reactor trip

signal from each of the four divisions of the PMS is sent to that division's reactor trip circuit breakers (RTCBs). Each division controls two RTCBs. The reactor is tripped when two or more actuation divisions output a reactor trip signal opening their breakers. This automatic trip demand signal initiates the following two actions. It de-energizes the undervoltage (UV) trip attachments on the RTCBs, and it energizes the shunt trip (ST) devices on the RTCBs. Consistent with the undervoltage trip and shunt trip devices in a current PWR design. Either action causes the breakers to open. Opening the appropriate trip breakers by two divisions removes power to the rod drive mechanism coils, allowing the rods to fall into the core. Bypass of a protection channel that generates a reactor trip signal and bypass of a reactor trip actuation division is permitted because the single failure criterion is met even when one channel or division is bypassed. Bypassing two or more redundant channels or divisions is not allowed and is handled via the design.

The LCL subsystem acts to initiate a reactor trip or ESF actuation when a pre-determined condition in 2 out of 4 independent safety divisions reaches a partial trip or partial actuation state. The LCL also provides for the bypass of trip or actuation functions to accommodate periodic tests and maintenance. The LCL subsystem performs two primary functions:

1. The reactor trip coincidence logic performs the logic to combine the partial trip signals from the BPL subsystems and generates a fault tolerant trip output signal to the reactor trip switchgear and initiation logic.

2. The ESF coincidence logic performs the logic to combine the partial actuation signals from the BPL subsystems along with automatic and manual permissives, blocks, and resets to generate a fault tolerant actuation output signal to the integrated logic processor (ILP) subsystems.

The ESF subsystem performs two primary functions:

1. The ESF coincidence logic function performs system-level logic calculations, such as actuation of the passive residual heat removal system. It receives inputs from the BPL subsystems, the MCR and Remote Shutdown Room (RSR) fixed-position switches.

2. The ESF component control function consists of the ILPs, which perform the component fan-out for each ESF system-level actuation, and component interface modules (CIMs) that provide the capability for on/off control of individual safety-related plant components. The CIMs receive inputs from the ILPs and from the plant control system (PLS).

The primary functions of the ESF logic processors are to process inputs, calculate system level actuation, combine the automatic actuation with the manual actuation and manual bypass data, and transmit the data to the ILPs. To perform the ESF coincidence logic calculations, the ESF processors require data from the BPL subsystems, and also use manual inputs (such as setpoint and system-level blocks and resets) from the MCR and the remote shutdown workstation. The ESF logic processors perform the following functions:

1. Receive bistable data supplied by the four divisions of BPL subsystems and perform 2 out of 4 voting on this data.

2. Implement system-level logic and transmit the output to the ILP processors for ESF component fan-out and actuation.

Process manual system-level actuation commands are received from the MCR and RSR. The ESF component control function is implemented with redundant ILPs and CIMs that provide a distributed interface between the safety system and the plant operator for control of non-modulating safety-related

plant components. CIMs provide the capability for on/off control of individual safety-related plant components. The CIMs receive inputs from the ILPs and from the PLS. Non-modulating control relates to the opening or closing of solenoid valves and solenoid pilot valves, and the opening or closing of motor-operated valves and dampers.

4. Modeling of the AP1000® plant digital RPS

The **AP1000®** plant design certification PRA is being updated to support initial operation of plants currently under construction in the United States. This effort includes refinement of the probabilistic models which represent the digital RPS and is focused on addressing the unique issues associated with modeling digital based systems. Traditional PRA methods are being used to perform this work. Specifically, fault trees are being utilized to represent the digital RPS following the outline of desirable characteristics identified in NUREG/CR-6962 [3]. The following sections summarize how these characteristics will be addressed in the PRA:

4.1 Level of Detail

The level of detail in the digital RPS model will be based on the combination of the system design and the availability of failure data. At a high level the system is comprised of four redundant divisions. Within each division, there are sub-divisions that are dedicated to 1) monitoring plant parameters and determining if a safety function should be actuated, 2) gathering information from the other divisions and performing coincidence logic, and 3) sending actuation signals to the appropriate components. Each of these sub-divisions includes a combination of sensors and transmitters, microprocessors, input modules, output modules, and component interface modules (CIMs). Based on the availability of failure data, each of these components will be represented by a basic event in the PRA model. This is consistent with how analog systems in current plants are modeled where basic events are included for components that perform similar functions. These components in current analog plants include equipment such as process sensors and transmitters, bistables, safeguard driver cards, universal logic cards, and master and slave relays. The level of detail will permit evaluations that support determining the importance of specific components as well as common cause failures for processors and modules that perform similar functions.

4.2 Identification of Failure Modes

A failure modes and effects analysis (FMEA) has been performed for the **AP1000®** plant protection system and will be used as part of the process to identify system failure modes. This will be accomplished by reviewing the failure modes tabulated in the FMEA and assessing the effects of the failure modes on the PRA success criteria. The FMEA was performed by first analyzing failures of the system at a high level, and then successively refining the analysis by looking at failure modes of major components, and then failure modes of microprocessors, input modules and out modules. The identification of failure modes in a digital system is completed by the redundancy associated with having multiple channels (i.e.; two of four channels must vote in order for a safety function to be actuated), and redundant signal processing occurring within a channel (i.e.; one of two processors determine that a plant parameter is exceeded). The FMEA will be used to assure that failure modes related to these design features are accounted for in the PRA.

4.3 Addressing Software Failures

Digital systems are unique relative to analog systems because they contain software. Failures of digital systems due to software failures have occurred in the airline industry and can have a significant impact on safety. Software is developed in stages that start with a concept and culminate in a code that is executed by a computer processor. Faults may be introduced during code development and it may not be apparent that such faults exist until a specific combination of a fault and other conditions, such as interaction with input data from field sensors, trigger an undesired response. Because of the difference in failure mechanisms between hardware and software (hardware fails due to factors such as

aging, while software fails due to a fault in the code in combination with the occurrence of a specific set of input data), it cannot be assumed that software failures are included in hardware failure data. In order to reflect this, it is desirable that the PRA model explicitly include software failures in the logic model so that the contribution to system reliability and CDF is accounted for. Therefore, in addition to common cause failure (CCF) events for hardware faults, the **AP1000®** plant digital I&C system logic model will include CCF events that reflect CCF of software. The CCF events will be developed based on specific functions (e.g.; all microprocessors that monitor field data will be included in two CCF groups, one for hardware faults and one for software faults). For example, the BPLs in each division included process modules that are programmed to specifically monitor data from field sensors and determine when a safeguards action is required. These process modules will be included in a CCF group that represents failure due to hardware faults, and a CCF group that represents failure due to a software fault. In addition, a CCF event will also be developed to represent a global failure of all software within the system. Representation of software failures in this fashion will facilitate a range of sensitivity analyses to assess the uncertainty associated with software failure probabilities.

4.4 Identification of Common Cause Failure Groups

As discussed in the previous section, CCF events due to hardware faults will be developed to account for the redundancy associated with multiple field sensors, redundant process modules, and multiple signal transmitters to safety components. However, development of the CCF events must also account for the unique features associated with a digital system. The components in a digital system communicate through buses, hardwired connections, and networks. It is necessary that CCF events are identified that represent the propagation of failures through communication devices and their effects on related components in the system. The types of failure propagation that will be considered include:

- Inter-system failure propagation when data is shared (i.e.; equipment status is shared between the digital RPS and PLS).

- Inter-channel failure propagation to account for the communication of redundant divisions amongst each other. For example, the BPLs in each division provide output to the LCLs in all divisions.

- Intra-channel failure propagation when redundancy within a division is used. In the **AP1000®** RPS, each division includes two each of the BPL, LCL, and ILP subracks.

This is similar to the approach in vintage ESFAS and RTS modeling, where the key elements of a standard approach for applying common cause include [1]:

- Common cause failures are modeled within each signal, but not across signals. For example, a common cause group is assigned for all of pressurizer pressure bistables. A separate common cause group is assigned for the low steam generator level bistables.

- Common cause failure is modeled between components in trains A and B performing the same functions. This is similar to the concept of modeling common cause across channels such as the BPLs in each division.

4.5 Digital System Component Failure Data

In PRAs, it is preferred that component failure data be based on operating experience from components that are similar to those included in the logic model, and also that are in a similar application and operating environment. The data used for analog based RPS in current plants comes from various sources. NUREG/CR-6928 provides generic data for transmitters/sensors and bistables. Data for reactor trip breakers, undervoltage driver cards, safeguard driver cards, and universal logic

cards was developed as part of PWROG projects such as documented in WCAP-15377-NP-A, Revision 1 [1]. Data for components in newly designed digital systems generally scarce or unavailable. For the **AP1000®** plant digital RPS, failure data is being developed using industry accepted reliability prediction methods such as Military Handbook 217F [4]. These methods are used to estimate failure rates for electronic components and systems based on part counts and part stresses. At a minimum; stress factors due to quality, operating temperature, component rating, duty cycle, and cycle rate are considered in these estimates. Although there is uncertainty associated with the use of such methods, they have been proven to be successful in achieving reliable estimates to support evaluation of system reliability. Development of software failure probabilities for complex digital systems is a subject area where there is no consensus in the technical community on a method to estimate the reliability of this kind of software. For example, methods based on testing the software may be inadequate because the test environment is not identical to the operating environment, the software tests may not be representative of actual operating conditions, and exhaustive tests are not practical. Since there is no consensus on a method for determining software failure probabilities, estimates will be included in the model and appropriate sensitivity analyses will be performed to assess the associated uncertainties as suggested in NUREG/CR-6962 [3].

4.6 Identification of Uncertainties

Given the limitations associated with representing the function of a digital I&C system with fault trees, and the scarcity of component and software failure data, it needs to be recognized that there is a great deal of uncertainty associated with the contribution of digital system failure to CDF. This uncertainty in data will be estimated as part of the data analysis task and propagated throughout the model to assess the impact on CDF. The sources of model uncertainty such as identification of CCF groups and sparseness of data to support independent failure probabilities will be identified along with their associated assumptions in the PRA documentation. In addition, sensitivity analysis will be specified and performed for each combination of uncertainty and assumption and included in the PRA documentation.

4.7 Integration into the PRA Model

The **AP1000®** plant digital RPS fault tree will be directly integrated into the PRA model in a fashion similar to that used for current plants. The methodology ties each initiator or sequence to the applicable signals and RPS functions required to mitigate the event. For example, LOCAs can be tied to signals for low pressurizer pressure and high containment pressure, and the components required to initiate safety injection. As part of the process, each initiator group can be evaluated to determine what signals will occur in response to the initiators and be incorporated into the model to ensure that diverse means are provide to actuate the safety components. This approach allows all dependencies of the digital system on other systems (such as its support systems) and vice versa to be explicitly modeled. Since all the dependencies are explicitly modeled in the logic model of the fault trees and event trees, both qualitative and quantitative results can be obtained directly from analysis of the PRA model. This will also permit review of the reasonableness of cutsets that include digital system failures, and provide importance measures for the digital system components.

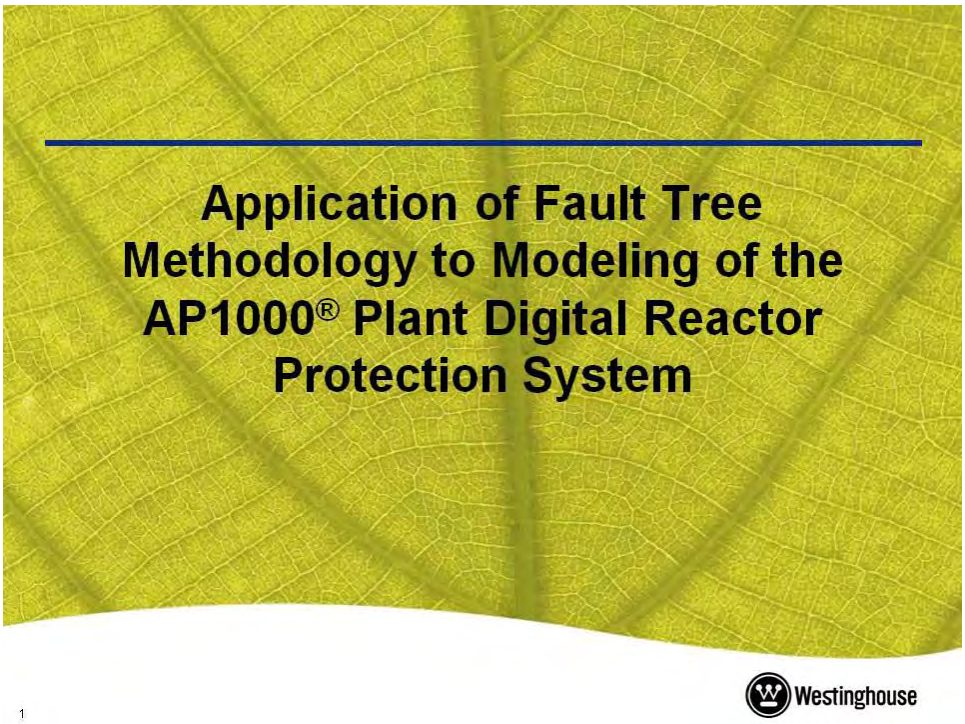
5. Conclusions

This paper discussed representation of analog and digital protection systems in PRA models. The RPS systems in existing nuclear power plants are generally analog based and there is general consensus within the PRA community on fault tree modeling of these systems. In new plants, such as the **AP1000®** plant, the RPS is based on digital technology. Digital based systems are more complex combinations of hardware components and software and result in the presence of faults and failure modes unique to digital based systems. Research is currently being conducted by the NRC to develop a methodology for including probabilistic models of digital systems in PRAs; however, no consensus methodology exists at this time. Westinghouse is currently updating the **AP1000®** plant PRA to support initial operation of plants currently under construction in the United States. The digital I&C

systems are being modeled using traditional fault tree methodology with a focus on addressing the key characteristics of such a model per the guidance provided in NUREG/CR-6962 [3]. A high level description of the **AP1000®** plant digital RPS relative to a typical analog based RPS system was provided. In addition, the key characteristics of an acceptable digital system PRA model were discussed in terms of how they are planned to be addressed for the updated **AP1000®** plant PRA.

References

1. Regulatory Guide 1.97, Revision 4, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," June 2006.
2. WCAP-16675-NP, Revision 5, "AP1000 Protection and Safety Monitoring System Architecture Technical Report," November 2010.
3. WCAP-15377-NP-A, Revision 1, "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times," March 2003.
4. NUREG/CR-6962, "Traditional Probabilistic Risk Assessment Methods for Digital Systems," October 2008.
5. MIL-HDBK-217F, Notice 2, "Military Handbook-Reliability Prediction of Electronic Equipment," February 1995.


Application of Fault Tree Methodology to Modeling of the AP1000® Plant Digital Reactor Protection System
Westinghouse
1

Outline
Background
Legacy plant Reactor Trip System (RTS) and Engineered Safeguards Features Actuation System (ESFAS)
Digital based Protection and Monitoring System (PMS)
Application of fault tree methodology to digital systems
Westinghouse
2

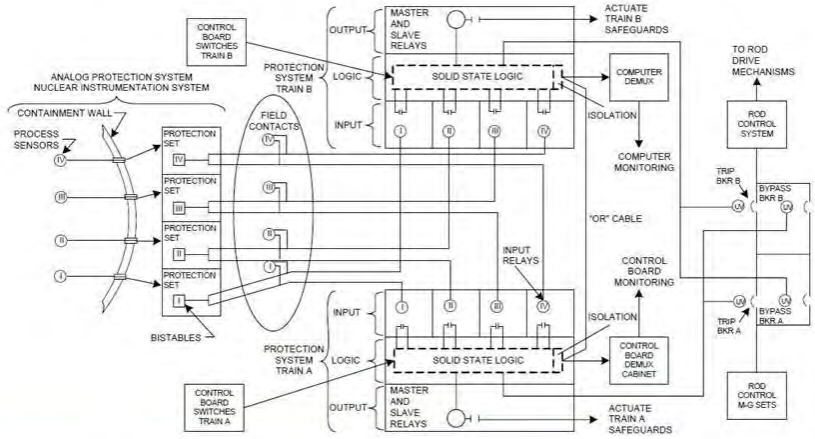
Background

- Most legacy plants have analog/solid state based RTS and ESFAS that are represented in PRAs by fault trees.
- Digital systems are more complex combinations of hardware components and software.
- Unique faults and failure modes may impact a digital RPS.
- Research on the development of probabilistic models for digital systems is ongoing.
- No consensus methodology currently exists.

Legacy Plant RPS Description

- Analog channels process sensor input and provide signals to two logic cabinets.
- Actuation logic is performed and signals are provided to the RTBs and actuation relays.
- Master relays control slave relays.
- Slave relays control the safeguards equipment.
- In legacy plants, the RPS can be analog or digital.
- Solid state components and a combination of relays perform logic.

Simplified Legacy Plant RPS



Westinghouse

AP1000® PMS Description

- Four redundant divisions receive independent signals.
- Signals are sent to two independent bistable process logic (BPL) modules in each division.
- Each BPL sends partial reactor trip and ESF actuation signals to two independent local coincidence logic (LCL) modules in each division.

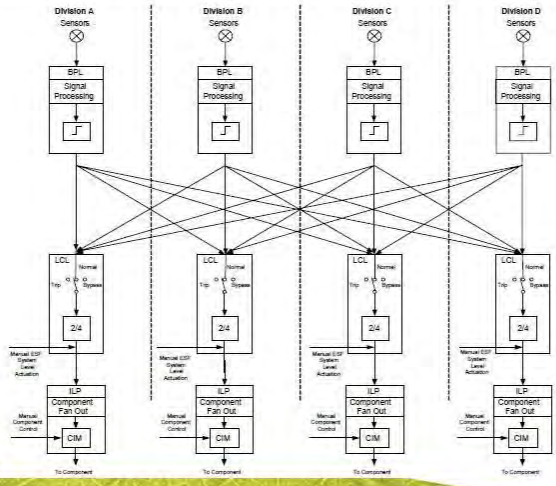
Westinghouse

AP1000® PMS Description

- Reactor trip signal from LCLs is sent to the division's reactor trip circuit breakers (RTCB) based on 2 of 4 logic.
  - Each division controls two RTCBs
  - Opening of any two division's RTCBs will trip the reactor.
- ESF actuation signals are sent to two redundant integrated logic processer (ILP) subsystems.
- Each ILP sends ESF actuation signals to component interface modules (CIMs)
  - CIMs provide on/off control for individual safety –related components

7 Westinghouse

Simplified AP1000® Digital PMS



8 Westinghouse

Modeling the AP1000® PMS

- Consensus methodology for modeling digital systems does not yet exist.
- NUREG/CR-6962 provides an outline of desirable characteristics for digital system reliability models
  - "Traditional Probabilistic Risk Assessment Methods for Digital Systems"
  - Includes examples based on fault tree methodology and Markov model
- Monitoring ongoing NRC research on modeling digital system

Desirable Characteristics

- Level of detail
  - Independent sensors provide data to each division
  - BPL, LCL, and ILP subsystems include a combination of microprocessors , input and output modules, and CIMs
  - Each of these components will be represented by a basic event
  - Supports detailed importance sensitivity analyses
- Identification of failure modes
  - Existing FMEA will be used to asses affect of failure modes on the PRA success criteria
  - Assures that unique design features are accounted for

Desirable Characteristics (Cont'd.)

- Addressing software failures
  - Common cause failure basic events will be developed to represent software failures
  - CCF events for software based on function.
    - Data monitoring process modules share common program
  - CCF event to represent total system failure due to software fault
- Identification of CCF Groups for hardware
  - CCF groups for redundant sensors, processors and other modules
  - CCF groups to represent propagation of failures through communication devices
    - Inter-system, inter-channel, and intra-channel propagation

11

Desirable Characteristics (Cont'd.)

- Digital system failure data
  - Generally scarce or non-existent
  - Failure data being developed using reliability prediction models
  - No consensus method for determining software failure probabilities
  - Based on expert judgment
- Identification of uncertainties
  - Recognize that there is a high degree of uncertainty
  - Limited data
  - Identification of CCF groups
  - PRA documentation will include several sensitivities

12

Desirable Characteristics (Cont'd.)

- Integration into the PRA model
  - Current plan is to link the PMS fault trees directly into the model similar to how current plants represent RTS and ESFAS
  - Tie each initiator to the applicable signals and functions required for mitigation
  - Allows dependencies on other systems and vice versa to be explicitly modeled
  - Facilitates reasonableness review of cutsets that include digital system failures.

I&C modelling in the IRSN EPR Level 1 PSA

Author principal: J. Delache, IRSN

Institute for Radiological Protection and Nuclear Safety (IRSN)
Reactor Safety division
System and Risk Protection Assessment Department

Postal Address

B.P. 17 92262 Fontenay-aux-Roses Cedex – France

E-mail: Julien.delache@irsn.fr

ABSTRACT

Today in France, an EPR Unit is under construction at the Flamanville site. The creation authorization was granted in April 2007 and the plant commissioning is planed for 2012.
The plant operator (EDF) provided for the construction license several PSA studies. The IRSN, as TSO, wishes to dispose of the appropriate knowledge and tools for the independent verification of the operator studies and so developed its own model of PSA level 1. The goal is not to rebuild the plant operator PSA (with a full scope etc…) but to dispose of a simplified model able to clearly point out specific important issues.
In the IRSN model a particular effort has recently been done on the Digital I&C modelling. The I&C is modelled in the IRSN EPR PSA by using Fault Trees. Instead, EDF EPR PSA applies the COMPACT model to simplify the command and instrumentation logics. The IRSN model is more detailed in order to be more accurate in the global analysis of the Digital I&C. For instance the communication ways between automates are considered as well as the failure of support systems. The model is still under development mainly in order to define the CCF which may be considered.

Keywords

I&C, PSA, fault trees, logic

1. Introduction

For the European Pressurized Water Reactor (EPR), the PSA was developed from the beginning of the design by the reactor designer (AREVA). This PSA was used for early design verification, several design improvement being defined based on these PSA insights and following the discussions with the French and German safety authorities.
Today, in France, at the Flamanville site, an EPR unit (named Flamanville 3) is under construction. The creation authorization was granted by the French Nuclear Safety Authority (ASN) in April 2007. After the first tenders had been awarded and the requisite permits had been granted, site preparatory works began during the summer of 2006. The first pouring of concrete for the nuclear block took place on December, 2007 and the plant construction phase will continue for 54 months, with commissioning planned for 2012.
In the frame of Flamanville 3 construction license application the plant operator (EDF) provided a level 1 and a level 1+, internal events PSA and it is expected that for commissioning request EDF will provide an “as-built” full scope PSA for the reactor and for the spent fuel pool. This study will cover the internal events, the internal hazards and the external hazards and will include a full scope level 2 PSA.
In France the PSA is developed and used according to the Basic Safety Rule “Development and utilization of PSA” in reference [1].

The PSA is playing an important role in the frame of the Institute for Radiological Protection and Nuclear Safety (IRSN) missions for EPR Project assessment, as the French Safety Authority (ASN) technical support organization. In this context IRSN develops its own limited scope PSA model, in parallel with EDF, in order to dispose of the appropriate knowledge and tools for the independent verification.
In the conception of new reactors the digital I&C (Instrumentation and Control) take an important place as far as many safety operations are partially or totally automatically worked.
The following paragraphs present mainly the modelling of Instrumentation and Control systems in the Level 1 PSA in the frame of the risk-informed activities at IRSN.

2. EPR design

The EPR is a French and German next-generation 1600 MWe class PWR. It is an evolutionary power reactor based on PWR technology originally developed in the United States. Its design evolved globally from mature and proven technologies, in particular the N4 and Konvoi plants, the most modern nuclear plants in France and Germany.
The reactor is designed to ensure the respect of the highest safety standards. In fact, the EPR design takes advantage of over 30 years of operating experience acquired by French and German designers and operators. The design was developed by electricity producers and manufacturers in conjunction with both countries' nuclear safety authorities.
In 2000, following the review of the conceptual design of EPR by the French and German nuclear safety authorities (by German experts after 1998), technical guidelines governing the project's nuclear safety options and defining the requirements for detailed studies were issued. These technical guidelines, formalized in the document "Technical Guidelines for the design and construction of the next generation of NPPs with Pressurized Water Reactors", become official in France in September 2004 (letter ASN in reference [2] "Safety Options for the EPR Reactor").
The main safety objectives indicated by the ASN by its letter are, compared with the existing reactors, the followings:

- reduction of the number of incidents by a better systems reliability and better consideration of the human factor,
- the core damage risk should be significantly reduced (a global frequency of core melt of less that 10^{-5} per plant operating year, hazards being taken into account),
- the radioactive releases should be also significantly reduced:
    - no population evacuation in case of accident without core damage,
    - practical elimination of the large early releases,
    - limited protection measures (in time and in space) in case of late releases.

In practice, these safety objectives can be achieved by special features of the EPR design.
Some examples are:

- tight double containment,
- built-in severe accident features (as for example the special device inside containment to collect and to cool the core in case of core melt),
- external anti-aircraft crash shield covering the containment, the spent fuel building and two out of four safety systems buildings,
- four electrical trains including two series of diversified Diesel generators (four main Diesels and two SBO Diesels),
- four 100% trains, physically separated, for the main safety systems and related support systems,
- high quality human-machine interface, based on up to date technology.

In France, as for the operating reactors, demonstration of the safety of the design of future reactors is based on deterministic studies. The PSA is used as a supplemental tool in safety assessment.

3. Principle of I&C modelling

In the conception of new reactors the digital I&C (Instrumentation and Control) may represent a main contribution of risk as far as many safety operations are partially or totally automatically worked.
So, to be able to evaluate the safety demonstration of the new reactors design produced by operators, IRSN as the French TSO, decides to model I&C systems in its own PSA level 1. The IRSN decided to use fault trees to consider I&C.

As for the "compact model", defined by the operator, an I&C chain is assumed to be possibly divided in three main parts which are interconnected in the IRSN model:

- An acquisition part
- A part with logic treatment (software)
- An actuator part

The actuator part is supposed to be specific to one action. It is on one hand composed with the contactors assigned to the actuator used to realised the action (for instance the opening/closing of a motoring valve) and in the other hand with all the modelled orders which trigger the action.

The acquisition and logic treatment parts may be used in several signals and a signal is often used to trigger different actions. So the modelling implies to interconnect numerous sub-divisions of I&C systems.

The acquisition part is specifically composed of redundant captors used in the checking of the same parameters. This part includes the vote logic using "K/N" gates in the fault trees.

In order to simplify the modelling, which easily risks becoming very tricky, it was assume to model mainly the common cause failures with macroscopic events in the logic treatment part. This assumption comes from the fact that common cause failures are known to be the major contributors of risk in most of redundant systems with reliable components.
So the logic treatment part is mainly composed with:

- the hardware components necessary for the signal treatment (plant Bus, net, etc.),
- the software involved with common cause failure between trains,
- possible faults identified between different software/hardware technologies in the same train (for instance due to mistake in the order transmission),
- the platform (for instance TXS or TXP on EPR)
- the items used for communication between automates (Gate ways, MSI, etc.).
- the support systems (ventilation and electrical support)

4. Methodology

The modelling of I&C in the IRSN PSA level 1 is constructed to be an iterative process which needed the cooperation between I&C and PSA experts. The modelling is in fact build based on macroscopic faults of items of I&C systems, which standing for all kinds of microscopic errors which may appear. The probabilistic values attributed to basic events associated to those faults are assumed to be conservative.
Due to the lack of support studies to define those probabilistic values, some expert judgements are used and sensitivities studies should be lead to validate the importance of the values considered.

Globally, the goal is to check which Minimal Cut-Set (MCS), and so, in which scenario, the I&C systems are main contributors. Once those dominant scenarios are pointed out, thanks to the conservative values attribute to I&C parameters and to modelling of support systems, an analysis have to be realised in order to precise if it may be demonstrated that it is realistic or not. This analysis has to lead to identify the possible weakness in the interaction between safety systems and I&C design.

The aim to identify and analyse possible weakness justify the choice to be conservative not only in the parameters attributed but also in the modelling and in the macroscopic basic-events definition.

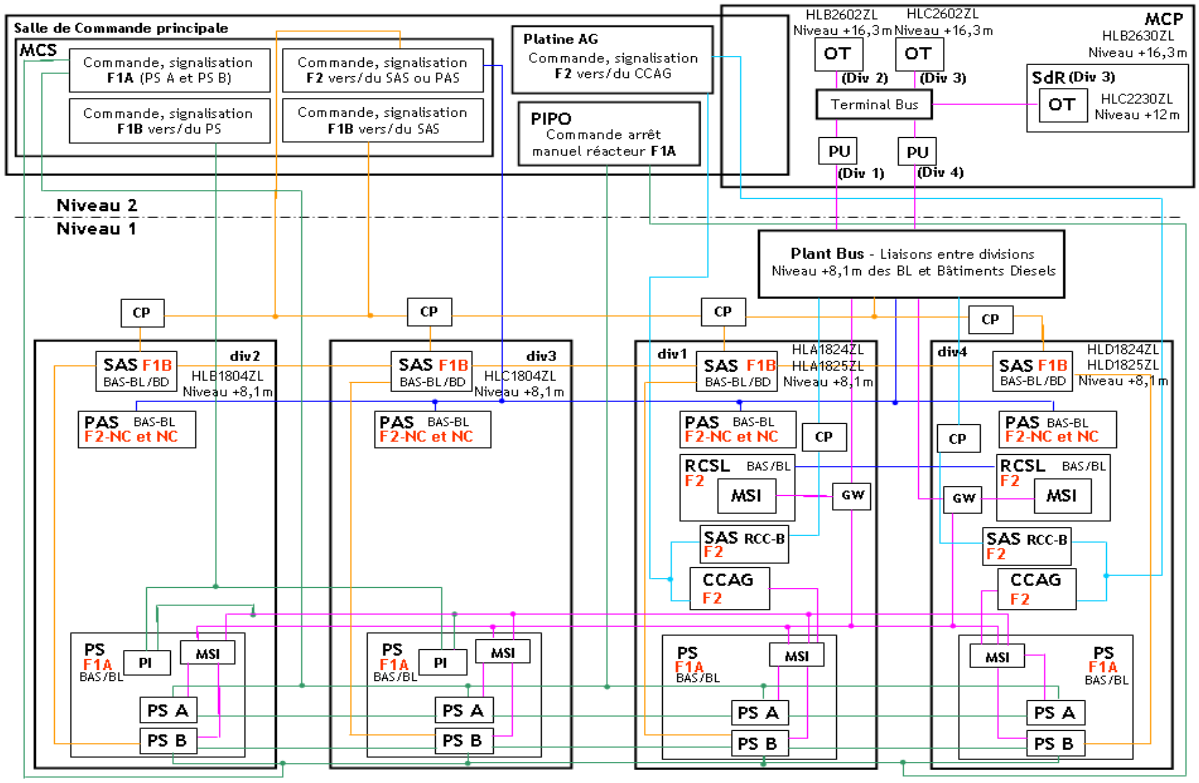
5. Main faults considered

The modelling of I&C in the IRSN PSA level 1 is still under construction and some modifications in the faults considered may always be done easily. The faults considered are macroscopic and in some cases conservative in the meaning that they may have to be detailed linked to realistic potential failure modes if an exhaustive list of failure modes may be demonstrated. For now, we do not have any study which allowed being less conservative with a sufficient level of confidence in the exhaustively of failure modes. So in a first step of its study, the IRSN considered mainly the following faults list[5]:

Automate	Faults considered
PS	Common logic for PS
	PS net (communication specific between PS)
	Erroneous order transmitted between PS and SAS for one division
	Specific fault of the TXS platform
	CCF between TXS and TXP platform
	Faults of support systems (electrical and ventilation)
SAS	Erroneous order transmitted between PS and SAS for one division
	Common logic for SAS
	SAS net (communication specific between PS)
	Specific fault of the TXP platform
	Support systems (electrical and ventilation)
MCP/Sdr	MCP panel
	OT (operator post)
	Plant BUS (link between PU and automates)
	PU (calculators redundant division by division)
	Terminal Bus (link between OT and PU)
	Support systems (electrical and ventilation)
	Gate way and MSI (interface between I&C level for PS/MCP)
	CP (communication processor interface for SAS/MCP)
MCS	CP (communication processor interface for SAS/MCS)
	MCS panel
	Support systems (electrical and ventilation)
	PI (panel Interface communication between PS / MCS)
	MSI (interface between PS/MCS)

[5] This list is not exhaustive in that all automates considered do not appear as for example PAS, or CCAG but it is representative of the faults considered.

Those faults are defined based on a general architecture of the I&C systems established thanks to the participation of I&C specialists to simplify the global architecture in macroscopic elements. This participation leads to the following picture which stands for the architecture of EPR.



I&C architecture of EPR modelled by IRSN

In this picture, each caption stands for an I&C component which is model with at least one basic events and potentially support by ventilation and electrical support. The lines stand for net communication between components which have to be also considered.

6. Preliminary fallout

In its preliminary evaluation of the operator level 1 PSA for the French EPR performed during 2010, the IRSN concludes, concerning digital I&C, that the modelling of the operator complies with the state of the art. Nevertheless to conclude on the validity of modelling, IRSN asked for I&C modelling justifications and mainly:

- an analysis of failure modes of I&C systems and the plant impact,
- I&C systems dependencies identification and analysis which should conduct to produce a dependence matrix,
- an analysis of the impact of the failure of systems used for thermal conditioning.

Moreover, IRSN has estimated that the following items should be taken into account by the operator:

- An exhaustive analysis realized for identifying initiators for I&C spurious actuation signals on the basis of system final design.
- Initiators of loss of I&C.
- The update of I&C components failure probabilities according to existing EPR I&C reliability analyses.
- I&C support systems: electrical supply and ventilation
- Sensors mis-calibration due to pre-accidental human errors

7. Acknowledgments

The paper is based on the on going actives at IRSN related to the licensing of the FLA3 NPP. The contribution of all participants in the mentioned tasks is gratefully acknowledged.

8. References

1. ASN, “Règle Fondamentale de Sûreté - Développement et utilisation des études probabilistes de sûreté" (2002).
2. “Rapport Preliminaire de Sûreté de Flamanville 3 – version publique”, EDF (2006).
3. ASN, lettre CODEP-DCN-2010-064949 Réacteurs électronucléaires – EDF Palier EPR - Instruction anticipée en vue de la mise en service du réacteur de Flamanville 3 - Instruction du rapport de sûreté. Etudes probabilistes de sûreté de niveau 1

IRSN
INSTITUT DE RADIOPROTECTION ET DE SÛRETÉ NUCLÉAIRE
Enhancing nuclear safety

I&C development in L1 PSA developed by IRSN (EPR example)

J. Delache and G. Georgescu

IRSN France

OECD/NEA Workshop on PSA for New and Advanced Reactors, Paris, 20 - 24 June 2011

Summary

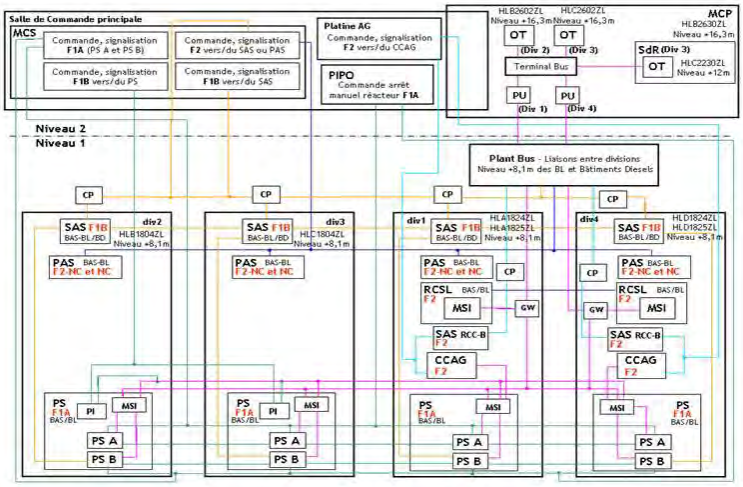
Introduction
Nuclear Reactors safety principles

- In France, as in other countries having a nuclear power program, the nuclear safety is based on deterministic principles (barriers, defense in depth, etc.)
- The safety demonstration is then based on deterministic approach
- The probabilistic approach, due to its particular investigation methods, progressively completes the deterministic approach
- In France the PSA for power reactors is developed in parallel by IRSN and EDF

Digital I&C system modelling in IRSN PSA
Generality

- IRSN develops its own EPR PSA model
  - Independent verification of EDF PSA
  - Tool to perform sensitivity studies
- I&C is modelled by using Fault Trees
  - EDF digital I&C model: COMPACT: *Not presented here*
  - EDF data if applicable
  - modelling of support systems (power, ventilation)
- The model is not yet finalized:
  - Dependencies and CCF between different modules are now under investigation by I&C specialists
    - Systems (PS, PAS, SAS, Severe accident)
    - Networks
    - Operator interfaces
  - Plant I&C architecture is not finalized (Hard Kernel under discussion)

Digital I&C system modelling in IRSN PSA
EPR model



Digital I&C system modelling in IRSN PSA
Principle

- IRSN model may be divided in three parts interconnected
  - I&C modelling may be divided between acquisition (with logic), treatment (hardware and software) and actuation
- Main software and hardware elements are modelled using macroscopic elements which stand for :
  - The platform (Teleperm XS or SPPA T2000 for EPR)
  - The software (PS, SAS, PAS, etc.)
  - The Hardware components (Plant BUS, etc.)
  - The sensors (with the acquisition logic)
  - The communication between main softwares (MSI, PI, etc.)

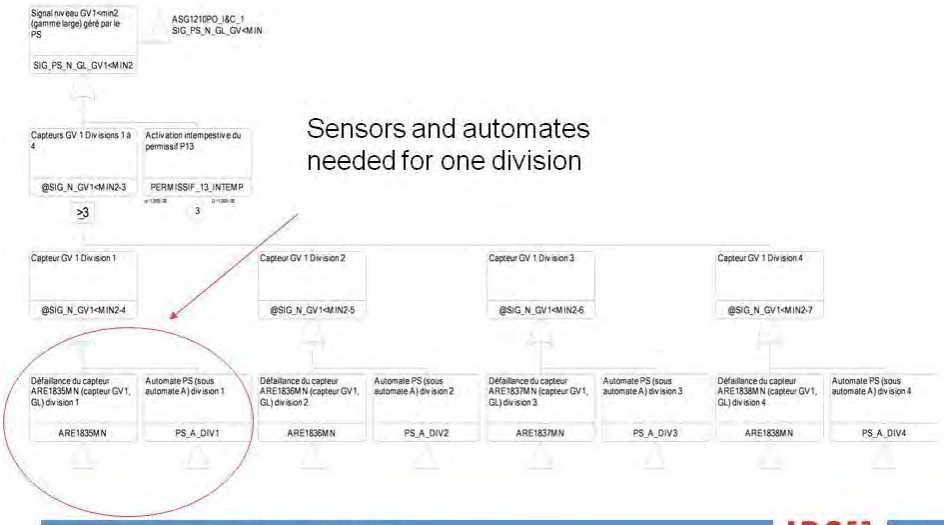
Digital I&C system modelling in PSA
IRSN model : faults considered (preliminary list)

Automate	Faults considered
PS	Common logic for PS
	PS net (communication specific between PS)
	Erroneous order transmitted between PS and SAS for one division
	Specific fault of the TXS platform
	CCF between TXS and TXP platform
	Faults of support systems (electrical and ventilation)
SAS	Erroneous order transmitted between PS and SAS for one division
	Common logic for SAS
	SAS net (communication specific between PS)
	Specific fault of the TXP platform
	Support systems (electrical and ventilation)

Digital I&C system modelling in PSA
IRSN model : faults considered

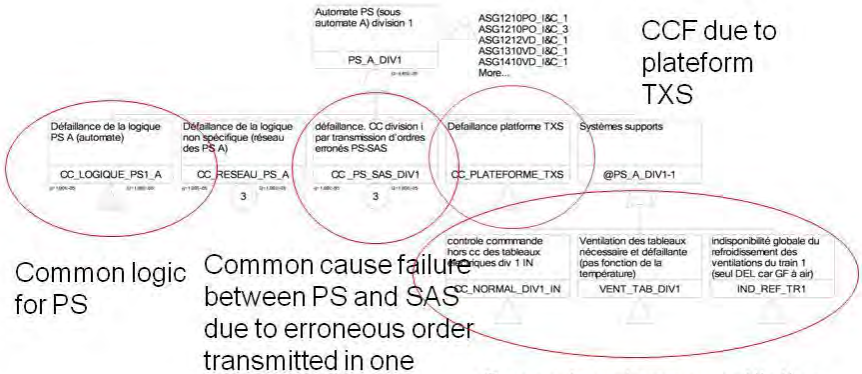
MCP/Sdr	MCP panel
	OT (operator post)
	Plant BUS (link between PU and automates)
	PU (calculators redundant division by division)
	Terminal Bus (link between OT and PU)
	Support systems (electrical and ventilation)
	Gate way and MSI (interface between I&C level for PS/MCP)
	CP (communication processor interface for SAS/MCP)
MCS	CP (communication processor interface for SAS/MCS)
	MCS panel
	Support systems (electrical and ventilation)
	PI (panel interface communication between PS / MCS)
	MSI (interface between PS/MCS)

Digital I&C system modelling in PSA
IRSN model : Acquisition example ASG start on SG level



Sensors and automates needed for one division

Digital I&C system modelling in PSA
IRSN model : Example for PS



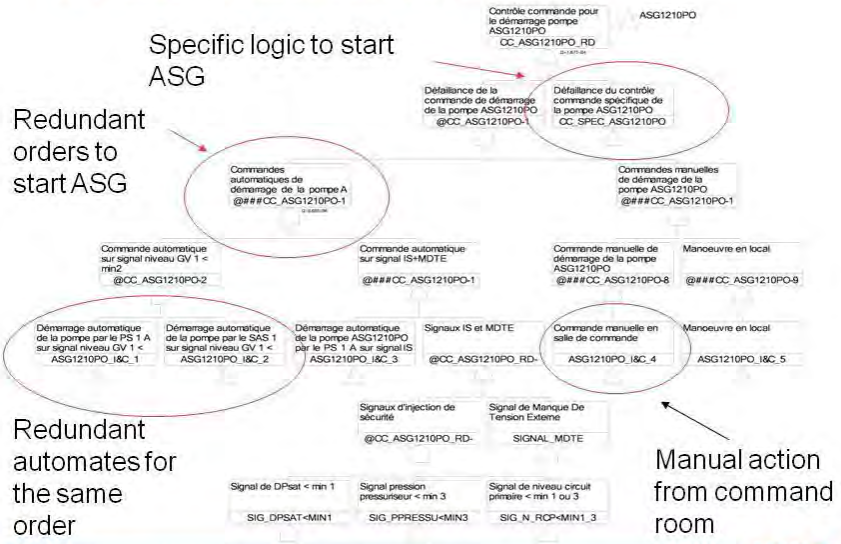
CCF due to plateform TXS

Common logic for PS

Common cause failure between PS and SAS due to erroneous order transmitted in one division

Support systems : ventilation (mechanic and cooling) and electrical support

Digital I&C system modelling in PSA
IRSN model : Actuation example for ASG start



Digital I&C system modelling in IRSN PSA
preliminary results

Preliminary results:

- Main contributions in Minimal cutsets linked to I&C are due to common cause failures
- The model seems to be conservative
  - Sensitivity studies to be performed
  - This is an iterative study which suppose the participation of I&C specialists to analyze the potential weakness
    - the aim is to be able to evaluate the global interaction between I&C and safety systems.

Digital I&C system modelling in PSA
Instruction of FA3 Reactor

- For FA3, until now, the digital I&C has been mainly assessed according to a deterministic approach
- Preliminary assessment of level 1 PSA for EPR was performed in 2010 (IRSN advice emitted in August 2010, letter ASN in January 2011)

Digital I&C system modelling in PSA
Instruction of FA3 Reactor

- IRSN Conclusion:
  - I&C modelling in EDF level 1 PSA complies to the state of the art.
  - Nevertheless, to conclude on the validity of modelling, IRSN asked for I&C modelling justifications:
    - An analysis of failure modes of I&C systems and the plant impact
    - I&C systems dependencies identification and analysis (dependence matrix)
    - An analysis of the impact of the failure of systems used for thermal conditioning.

Digital I&C system modelling in PSA
Instruction of FA3 Reactor

- Moreover, IRSN has estimated that the following items should be taken into account by EDF:
  - Exhaustive analysis realized for identifying initiators for I&C spurious actuation signals on the basis of system final design
  - Initiators of loss of I&C
  - The update of I&C components failure probabilities according to existing EPR I&C reliability analyses
  - I&C support systems (electrical supply and ventilation)
  - Sensors mis-calibration pre-accidental human errors

Design-Reliability Assurance Program Application in ACP600

Huang Zhichao, Zhao Bo

Technical Integration Division, CNNC China Nuclear Power Engineering Co., Ltd.

N°117, xisanhuanbeilu Haidian District Beijing 100840 P.R. of China)

Abstract

Design Reliability Assurance Program was used in AP1000 which developed the III Generation Nuclear Power Plant by Westinghouse Company of U.S., and acquired the certification of NRC. Reliability Assurance Program Guidebook for Advanced Light Water Reactors which published by IAEA provides the basis theory and practice procedure of the Design and Operation Reliability Assurance Program. ACP600 is the CNNC devoting to develop newly III Generation NPP, and all its general goals and performance indicators are meeting the next generation NPP indicators requirement. In this paper will use the D-RAP technical and Risk-Informed requirements, establish the RAM and PSA model to optimize the ACP600 design. After the iterative loop of analyzers with the designers information exchanges, achieving the goal of ACP600 primary design improving and optimizing.

Key Words: D-RAP，PSA，ACP600，Risk-Informed

1. Introduction of ACP600

ACP600 is a newly nuclear power plant technology of CNNC in China which based on the Generation III NPPs design experience and general safety goals. ACP600 is the newly NPP which with independent technical innovation and intellectual property rights. The ACP600 Design Reliability Assurance Program (D-RAP) is implemented as an integral part of the ACP600 design process to provide the confidence of the plant reliability and auxiliary design decision. Figure 1 is the inspiring chart of ACP600 project.

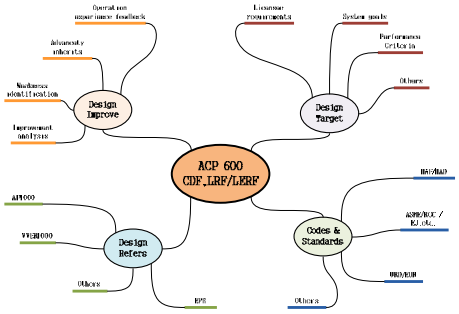


Figure 1 Inspiring Chart of ACP600

1.1 General Design Rules

ACP600 is based on the domestic NPPs' design and operation experience, inherits the technical research results and follow the advanced standards, codes and the rules as follows:

- Keep to the standing domestic codes, such as HAFs and HADs, guidelines and related

standards, IAEA and other advanced specific are the supplementary references, and;
- Absorbed the international existing suchlike AP1000,EPR and VVER advanced Generation III NPPs' design experiences, and;
- Advanced and proven technical used in the ACP600, promoting the key components and equipments localization, and;
- Combine the research work and the engineering, before the detail design, development some research and test verification needed.

1.2 General Design Targets

The general design targets of ACP600 showed in the table 1.

Table 1 ACP 600 general design targets

No.	Technical indicators description	Unit	Value
1	Plant Designed Life Cycle	year	60
2	Plant Layout		Single
3	Containment Type		Double
4	Refueling Cycle	month	18~24
5	Core Damage Frequency (CDF)	1/yr	<1.00E-05
6	Large Release Frequency (LRF)	1/yr	<1.00E-06
7	Plant Capacity	%	>90
8	Instrument and Control System		DCS
9	Server Accident Mitigating and Management Ability		Mature

2 D-RAP Applications in ACP600

A reliability assurance program (RAP) is a formal management system which assures the collection of important characteristic information about plant performance throughout each phase of its life and directs the use of this information in the implementation of analytical and management process which are specifically designed to meet two specific objects, etc, confirm the plant goals and cost effective improvements. In general, typical reliability assurance program have four broad functional elements:
- Goals and performance criteria;
- Management system and implementing procedures;
- Analytical tools and investigative methods, and;
- Information management.

2.1 D-RAP in ACP600

Design review process is the important and major program element of Reliability Assurance Program in design phase (D-RAP). Design review must not only follow the conventional practice in reviewing and comparing the design to all deterministic criteria and requirements imposed by owner and regulatory authorities, but also compare the predicted performance of the design with its prescribed probabilistic criteria. Another important element of D-RAP is focusing the attention onto the reliability and maintainability of SSCs.
In ACP600 project, we use simplified the D-RAP to allocation the safety system's goals and performance criteria, utilizes PSA for the analytical tool to quantify the importance of critical SSCs, etc, by the means of Fussel-Vesely and Risk Achievement Worth to identify and classify the SSCs. Figure 2 is the flow chart of reliability assurance program in ACP600 design phase.

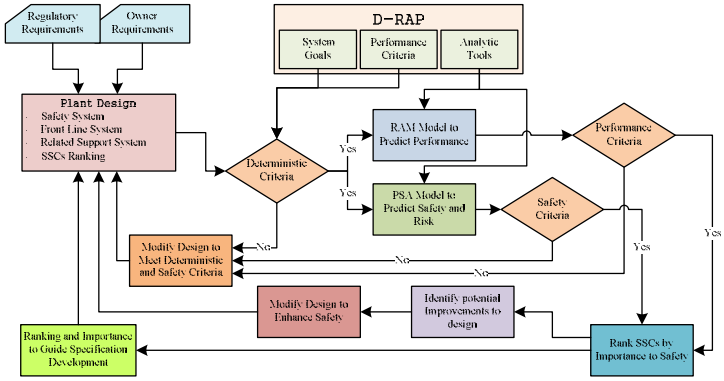


Figure 2 Flow Chart of Reliability Assurance Program in ACP600 Design Phase

ACP600 composites the reference plant design and operation experience, some safety system, safety related system and their support systems, we need to optimize and improve the system design to meet with the requirements of owner and regulatory, such as HAF102, HADs and URD/EUR. First we should get ready for the data input which needed, set the plant safety goals, and then allocate the system goals, for example, reliability, maintainability, availability and etc by the meaning of main logical chart and/or success tree. PSA and RAM models to quantify the performance criteria, unreliability and unavailability which are determined in the system goals. The PSA and RAM results can use to identify and rank the safety important SSCs. Figure 3 is the sketch of design optimize and improve by D-RAP in ACP600 project.

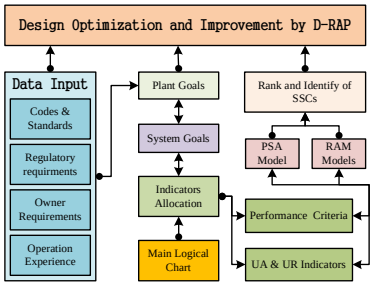


Figure 3 Flow Chart of Design Optimization and Improvement by D-RAP of ACP600

In ACP600 project, passive and motile safety system are used to enhance the safety goals and the reliability of these front line system which play an important role in mitigating and terminating the accidents and transients events, at the same time, ACP600 has the ability to mitigate and manage the severe accidents to satisfy with the URD or EUR requirements. D-RAP is a deductive method, in other words, from the plant top goals such as safety goals, economy goals, and performance criteria and so on. Especially, we are focus on the safety goals in ACP600, tracing the significant important safety function, we add some new passive safety systems to mitigate and manage during the plant at accidents or severe accidents. Figure 4 is the matrix of system and safety function in ACP600 preliminary design.

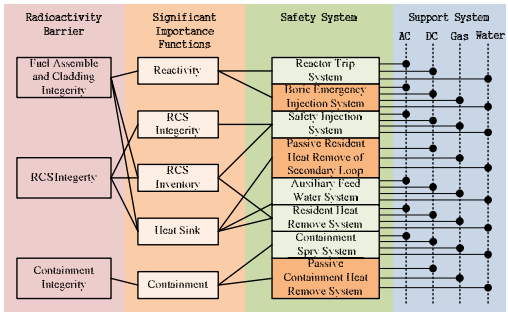


Figure 4 Matrix of System and Safety Function of ACP600

2.2 Scope and Content of Level 1 PSA

Level 1 PSA evaluates accident sequences from the initiating events and failure of safety function to core damage. The frequency of core damage and identification the dominant contributors are determined from the PRA results, and use the PSA as an effective analytical tool to quantitative analysis the importance of SSCs. In the D-RAP if the events that meet the threshold risk achievement worth (RAW) and/or risk reduction worth, then should pay more attention to these events and take action to enhance or degrade the relative SSCs important level.

In ACP600, for the time and ACP600 is ongoing concept design, the analysis scope and content of level 1PSA is localized in the internal events included the loss of offsite power and loss of heat sink events, but exclude the internal flooding and fire events when plant at power. Low-power and shutdown state is conducted to address concerns about risk of operations during shutdown conditions or encompasses operation when the reactor is in subcritical state or in a transition between subcritical and power up to 2%.

The PSA model update is a iterative process, with the design in detail, the performance criteria and system allocation before determined, we momentarily adjust the systems and components' reliability indicator in needed. Figure 5 is the PSA of D-RAP update during design phase.

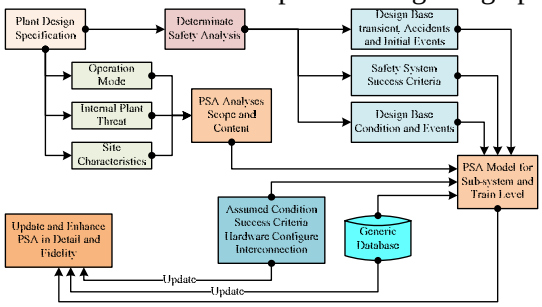


Figure 5 PSA Update during Design Phase of ACP600

2.3 Database for D-RAP of ACP600

The ability to perform quantitative reliability analyses to predict the performance of ACP600 depends very much upon the mathematical analog and the database which used in PSA and RAM models. There are many diverse source of component reliability database, some public, some proprietary, generally, generic database, plant specific data, company generic database and sister plant operating data used in PSA models. Since the database is one of the important input conditions and element of the PSA and RAM models.

In ACP600 project, the analysis contents of database are the following types:

- Methodology, include the definition for hardware reliability and unavailability, parameter assessment, distributor type, error factor, data update and data collection;
- Database source, by the now, there are some choice to select the generic database, so should select the most appropriate database for the ACP600, and;
- Specific data for the ACP600, for example, the site information, expert judgment and engineering analyses method.

Establish the reasonable and applicably database is the most important cornerstone of all the work, and it's the requirement that the regulatory focus on. Figure 6 shows the database system for PSA and RAM models.

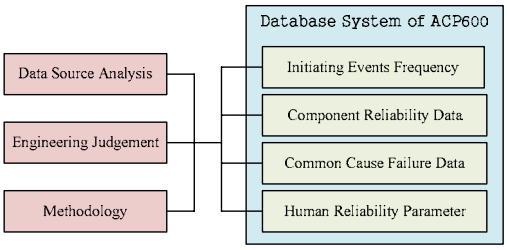


Figure 6 Database System for PSA and RAM Models

2.4 Organization Hierarchy of D-RAP

Any organization to implement a formal reliability assurance program will require a fully capable support group which is able to transfer the needed technical skills to existing organization, based on the definition processes which needed in D-RAP of ACP600 developing, provide procedural and technical guidance, develop and apply the analytical tools, techniques and methods which are an integral parts of the quantitative decision making process of D-RAP. An effective D-RAP organization will probably need a highly skilled group of specialists in RAM models, PSA model development. Figure 6 is the organization hierarchy of D-RAP in ACP600.

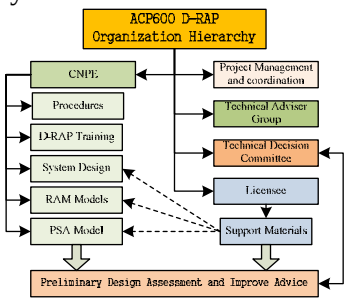


Figure 6 D-RAP organization of ACP600

2.5 Analysis Tool

In D-RAP we use the importance such as Fussel-Vesely and Birnbaum which come from the PSA and RAM models. Because the importance is a key factor to providing the focus needed by the design team, so the design team members to understand the physical relationship of the importance is essential. Usually, the Fussel-Vesely importance and Risk Achievement Worth (RAW) are used to rank the importance of SSCs, specifically in light of maintenance activities. The more detailed approach is suggested by “Evaluations and Utilizations of Risk Importance” (NUREG/CR-4377). In this model, the area bounded by the system RAW importance measure, plotted on the ordinate axis, and the system F-V importance measure plotted on the abscissa, is divided into four quadrants as shown in figure 7:

- Quadrant I, significant impact on safety assurance, (RAW>2 and F-V<5.0E-3);
- Quadrant II, significant impact on risk reduction and safety assurance, (RAW>2 and F-V>5.0E-3);
- Quadrant III, insignificant impact on risk reduction and safety assurance, (RAW<2 and F-V<5.0E-3);
- Quadrant V, significant impact on risk reduction, (RAW<2 and F-V>5.0E-3);

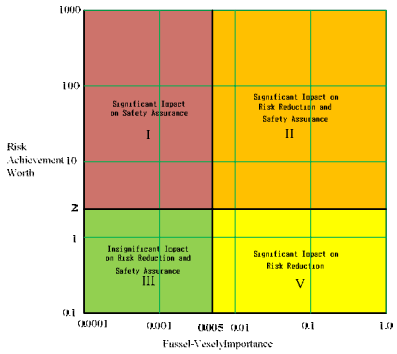


Figure 7 Importance Measures Categories of SSCs

3. Conclusions

ACP600 is a new nuclear plant design that CNNC is devoting into develop, which is a new generation III of ALWRs. D-RAP is one of the most effective and useful information management system and analytical tool, especially in developing new nuclear plant in the design phase. The D-RAP is the first time for CNNC using in developing newly advanced light water reactors, which based on the Risk-Informed regulatory requirements, establish the corresponding PSA and RAM models to rank the significant safety and risk reduction SSCs. Compared with design process as before, the D-RAP is more competent for the higher design targets and requirements, with more creativity and highlight of breakthrough. By using D-RAP, the plants goals, system goals, performance criteria and safety criteria can be easier to realize, and the design can be optimized and more rational.

4. References

1. IAEA-TECDOC-1264, 2001.11, Reliability Assurance Program Guidebook for Advanced Light Water Reactors,

2. APP-GW-GRR-099, 2008, AP1000 Design Reliability Assurance Program

3. J.P. Poloski, USNRC, 1998, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995 (Draft), NUREG/CR-5750,

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

D-RAP Application in ACP600

Huang Zhichao & Zhao Bo

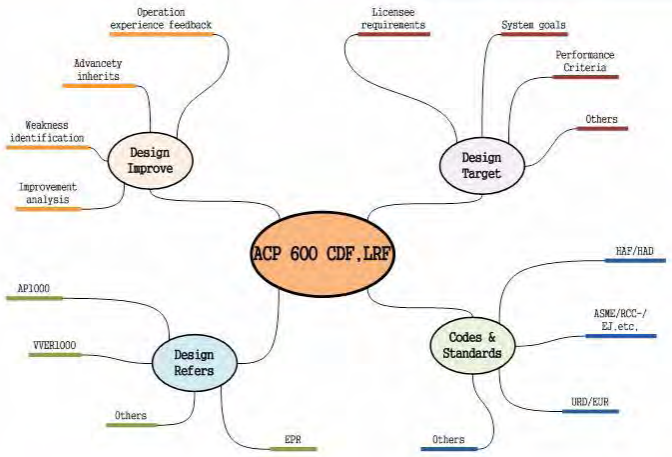
CNNC China Nuclear Power Engineering Co., Ltd.

21/June/2011 Paris

CNPE CNPE CNPE CNPE CNPE CNPE CNPE CNPE CNPE CNPE CNPE CNPE CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

Inspiring Chart of ACP600



第 2页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

Background of ACP600

- ACP600 is a newly advanced reactor which meets the 3rd Generation of NPP's safety and economy goals;
- Refers to the international advanced reactor technology and proven technical;
- Bases on the operation and design experience, and,
- Independent technical innovation and intellectual copy right of CNNC.

第 3页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

Design Rule and Criteria

- Keep with the standing domestic codes, standards, and others
- Refer to the international advanced reactor design experience, such as AP1000 and EPR, etc,.
- Active and passive safety system used in ACP600 to enhance the reliability of safety system, proven technical are broadly utilized
- Combine the research and engineering design, validation and verification in conceptual and preliminary design phase

第 4页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

General design targets

No.	Design Target Description	Target Value	No.	Design Target Description	Target Value
1	Plant design life	60years	6	Large release frequency	< 1.0E-5/yr
2	Reactor layout at site	single	7	Plant capacity	>0.9
3	Containment	Double deck	8	Instrument and control system	DCS
4	Refueling cycle	18~24 Months	9	Server accident mitigation and management ability	Mature
5	Core damage frequency	< 1.0E-5/yr	10	Emergency procedure	SOP SAMG

第 5页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

Introduction of D-RAP

Reliability Assurance Program in design Phase (D-RAP) is a formal management system of plant performance and safety information.

- Goals and performance criteria
- Management system and implementing procedures
- Analytical tools and investigative methods
- Information management

第 6页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

D-RAP in ACP600

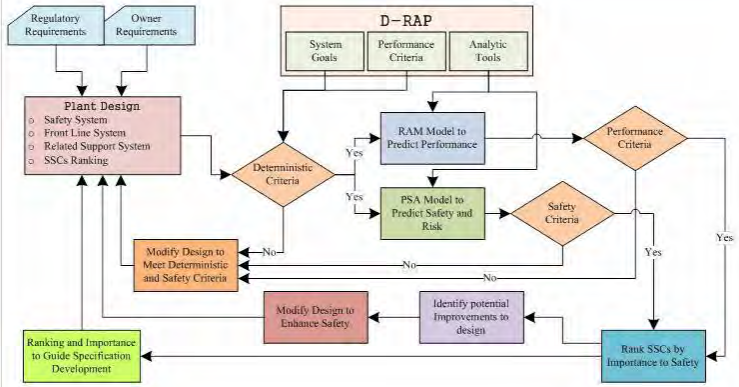
- Conceptual design
  - Performance criteria and goals setting
  - Design input (codes, standards, rules, requirements and reference plant)
  - Goals and safety validation
- Preliminary design
  - System design draft
  - Simply system assessment (determiner and probabilistic)
  - PSA and RAM models development
  - Models update
- Detailed design
  - Update PSA and RAM models in detail
  - Database update (especially plant specific data)
  - System design optimize and improve
  - SSCs classification (base on the importance of SSCs)

第 7页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

Flow chart of D-RAP

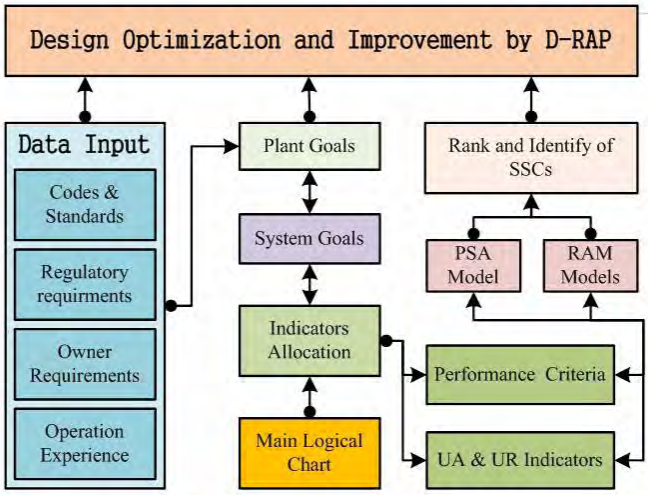


第 8页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

System optimize and improve



第 9页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

Preliminary design of ACP600

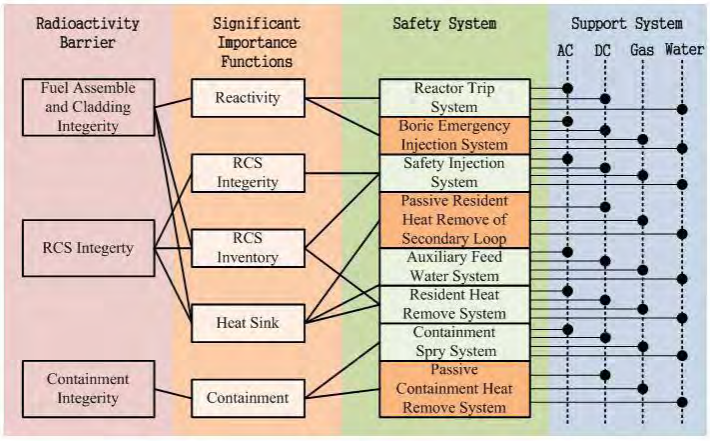
- Improve refer source
  - Based on the general goals of ACP600
  - Refers to the PSA result
  - Historical design and operation experience
  - International advanced light pressure water reactor design experience
- Important improve items in plan
  - Passive resident heat remove system (new)
  - Active emergency high concentration boric acid injection system (new)
  - Passive secondary heat remove system (new)
  - Safety injection system improve
  - Active cavity immerge system in server accident condition (new)
  - Abundant release valve for server accident condition (new)
  - Risk-informed SSCs classification and system reliability, availability, and maintainability assessment
  - Other design improve

第 10 页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

Matrix of system and safety function



第 11 页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

PSA scope and content

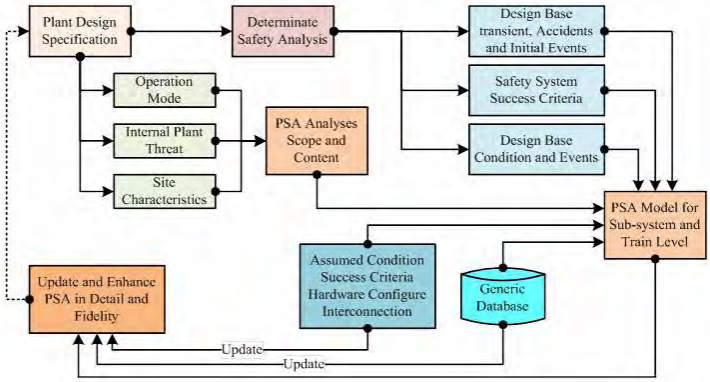
- PSA L1
  - Internal Events (LOSP included)
  - At power (exclude low power and shutdown)
  - Internal flooding and fire will be engaged in detail design phase
  - PSA is analytical tools for quantitative importance of SSCs
  - System improve by PSA result, such as reliability, availability and maintainability

第 12 页

CNPE

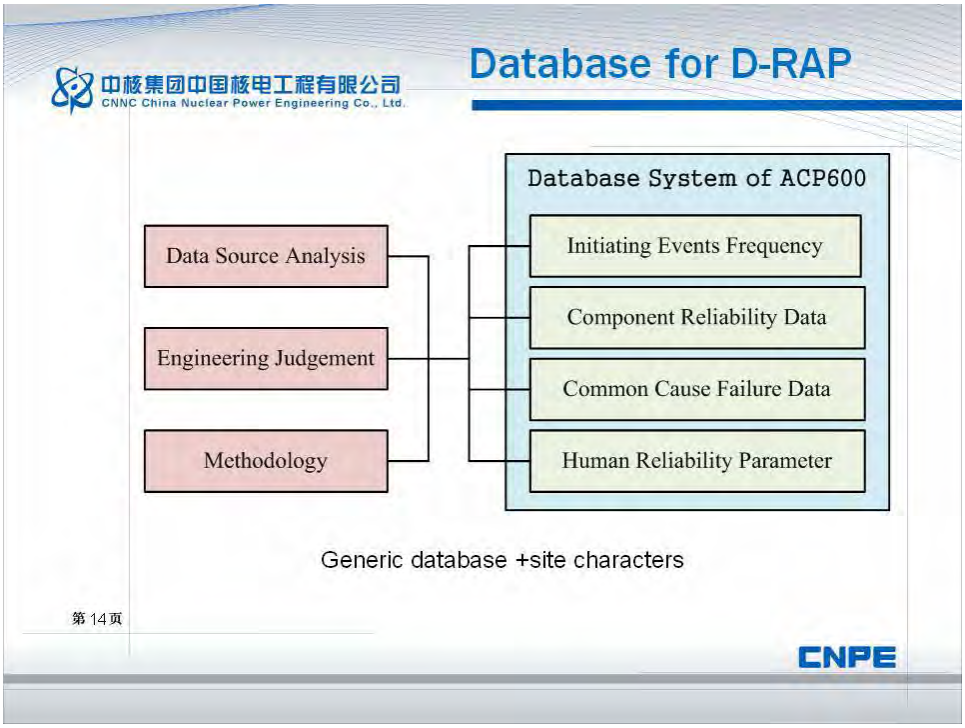
中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

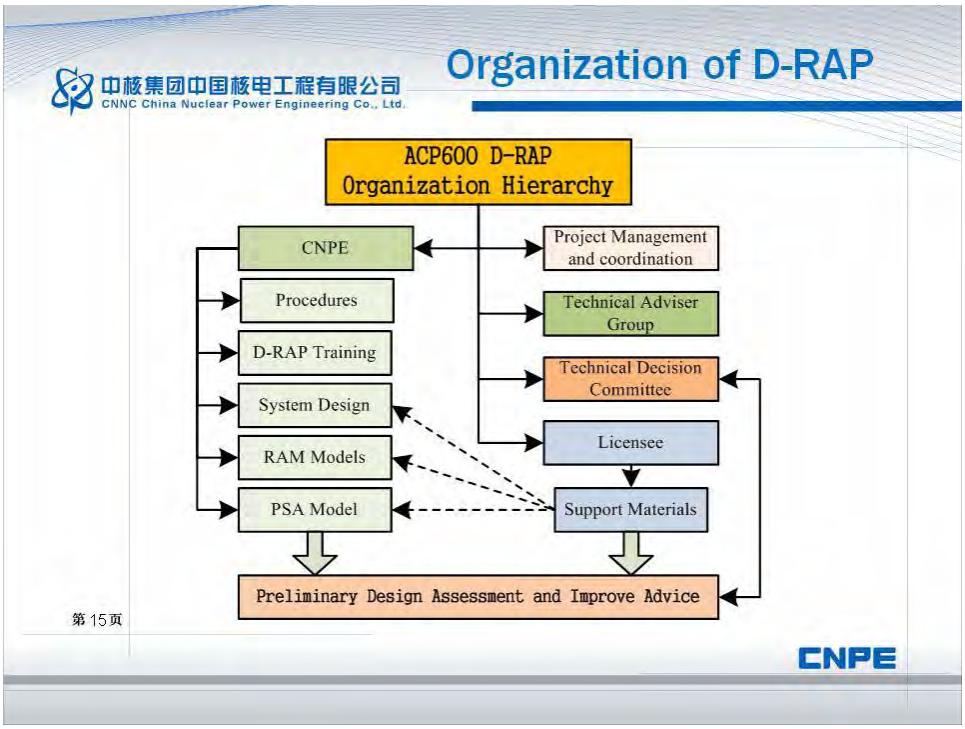
PSA model update in D-RAP



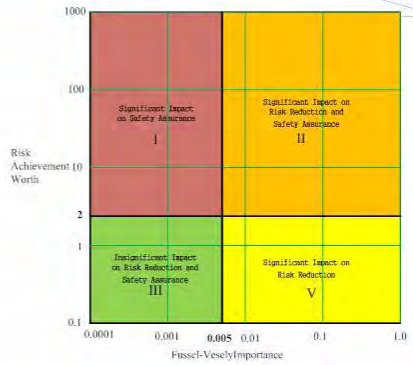
第 13 页

CNPE


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
Database for D-RAP
Database System of ACP600
Data Source Analysis
Engineering Judgement
Methodology
Initiating Events Frequency
Component Reliability Data
Common Cause Failure Data
Human Reliability Parameter
Generic database +site characters
第 14 页
CNPE


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
Organization of D-RAP
ACP600 D-RAP
Organization Hierarchy
CNPE
Procedures
D-RAP Training
System Design
RAM Models
PSA Model
Project Management and coordination
Technical Adviser Group
Technical Decision Committee
Licensee
Support Materials
Preliminary Design Assessment and Improve Advice
第 15 页
CNPE

Importance analytical tool



- Fussel-Vesely importance
- Birnbaum importance
- Risk achievement worth (RAW) importance

第 16 页

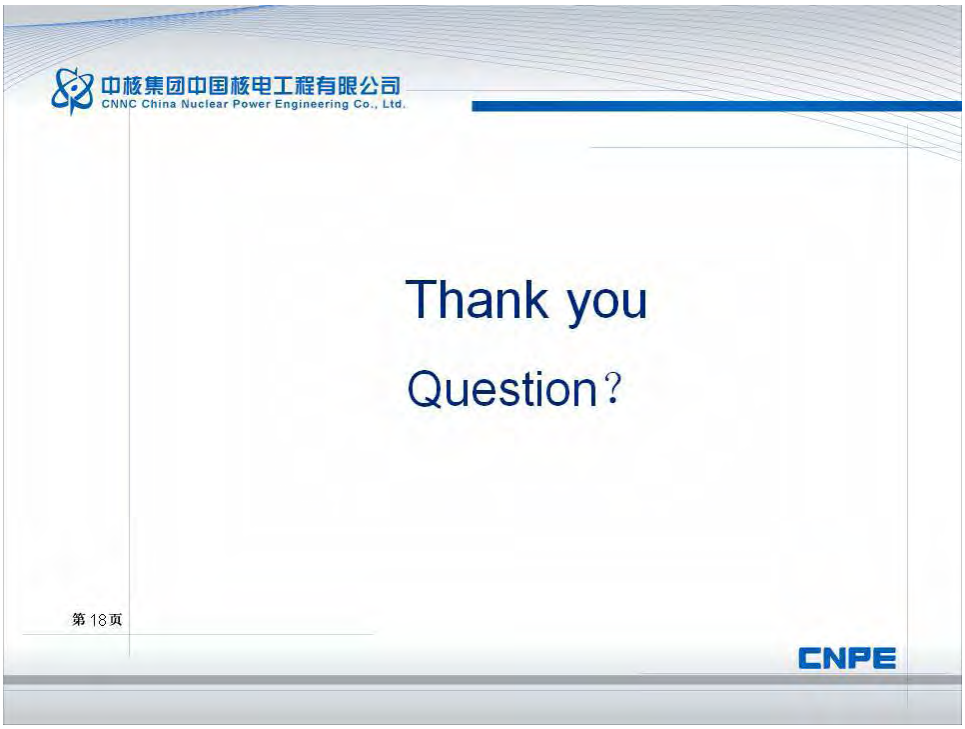
CNPE

Conclusion

- D-RAP is a useful analytical tool for new reactor technical development and effective information management tool
- D-RAP combines the advantage of deterministic and probabilistic analyses methods
- D-RAP has been used in AP1000 design
- D-RAP is the first time for CNPE to develop ACP600
- D-RAP can help to achieve the performance criteria and safety goals
- More details of D-RAP will be found in realize development work

第 17 页

CNPE


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
Thank you
Question?
第 18 页
CNPE

In-Vessel Retention Modeling Capabilities in MAAP5

Chan Y. Paik[1], Sung Jin Lee[1], James H. Scobel[2], Quan Zhou[1], Wison Luangdilok[1], Robert W. Reeves[1], Robert E. Henry[1], and Martin Plys[1]

[1]Fauske and Associates
16W070 83rd Street
Burr Ridge, Illinois 60527
Paik@Fauske.com

[2]Westinghouse Electric Company
1000 Westinhouse Drive
Cranberry Township, Pennsylvania 16066
scobeljh@westinghouse.com

Abstract

New and improved models to address the complex phenomena associated with in-vessel retention (IVR) were incorporated into MAAP5.01. They include: (a) time-dependent volatile and non-volatile decay heat, (b) material properties at high temperatures, (c) finer vessel wall nodalization, (d) new correlations for natural convection heat transfer in the oxidic pool, (e) refined metal layer heat transfer to the reactor vessel wall and surroundings, (f) formation of a heavy metal layer, and (g) insulation cooling channel model and associated ex-vessel heat transfer and critical heat flux correlations. In this paper, the new and improved models in MAAP5.01 are described and sample calculation results are presented for the AP1000® passive plant. For the IVR evaluation, a transient calculation is useful because the timing of corium relocation, decaying heat load, and formation of separate layers in the lower plenum all affect integrity of the lower head. The key parameters affecting the IVR success are the metal layer emissivity and thickness of the top metal layer, which depends on the amount of steel in the oxidic pool and in the heavy metal layer. With the best estimate inputs for the debris mixing parameters in a conservative IVR scenario, the AP1000® plant results show that the maximum ex-vessel heat flux to CHF ratio is about 0.7, which occurs before 10,000 seconds when the decay heat is high. The AP1000® plant results demonstrate how MAAP5.01 can be used to evaluate IVR and to gain insight into responses of the lower head during a severe accident.

1. Introduction

The capability to retain the molten core material inside the reactor vessel during a rare event of severe core damage is highly desirable. The in-vessel retention (IVR) of core debris, where the lower head integrity is maintained by flooding the reactor cavity and submerging the reactor vessel, is an important severe accident management strategy adopted by some advanced reactor designs such as AP1000® and APR1400. The success of IVR depends on the delicate balance between the decaying heat load in the corium pool, highly effective nucleate boiling heat transfer on the outside, radiative heat removal on top of the overlying metal layer, and enhanced lateral heat flow in the floating steel melt to the vessel wall often referred to as the heat "focusing effect". In addition, the formation of a heavy metal layer, when the unoxidized Zr in the corium reduces UO_2 to U metal, may be postulated to remove some of the steel in the light metal layer, making the "focusing effect" worse. Even with water outside, a high heat flux to vessel wall threatens integrity of the reactor vessel when the critical heat flux is exceeded or when the wall has thinned sufficiently due to melting.

Modular Accident Analysis Program (MAAP) is an integrated severe accident analysis code for both light water and heavy water reactors. The MAAP code was developed and is maintained by Fauske and Associates, LLC under the sponsorship of Electric Power Research Institute (EPRI). The MAAP code calculates fuel heatup, oxidation, dissolution, and relocation to the lower plenum, formation of separate metal and oxide layers in the lower plenum, and the thermal and structural response of the

lower head.

This paper describes new models and improvements made in MAAP5.01 specifically to address complex phenomena important for IVR. In particular, MAAP5.01 has a three-layer corium pool model, so-called "MASCA" configuration proposed by Salay and Fichot (2004). Also, the insulation cooling channel model was added, including heat transfer and critical heat flux (CHF) correlations applicable to specific insulation cooling channel types. MAAP5.01 is used here to evaluate the IVR in the AP1000® passive plant as an example. This represents one of the first integrated, transient calculations for evaluation of IVR.

2. General code improvements for IVR

2.1 Decay Heat

The decay power model in MAAP is based on ANSI-1979 (ANS, 1979). It was compared against the ANSI-1994 (ANS, 1994) and ANSI-2005 (ANS, 2005) standards and was found to be nearly identical. The modeling of fission product decay heat has been improved in MAAP5.01 to allow for the input of decay power fraction curves as functions of time for each of the fission product groups. Accurate modeling of the decay power distribution is important for investigating any sequence where debris coolability is an issue. In these sequences, the fission products that have been liberated from the core debris typically account for 20 to 25% of decay heat.

2.2 Material Properties

Material properties for steel were upgraded to the latest data from testing performed in the High Temperature Test Laboratory (HTTL) at the Idaho National Laboratory (INL) (Daw, Rempe & Knudson, 2010). The data collected at INL marks a significant step forward in the quantification of high temperature properties for materials used in existing light water reactors. Specifically, the materials analyzed were SA533 Grade B Class 1 low alloy steel and Stainless Steel 304. These correspond to MAAP materials carbon steel and stainless steel, respectively. In MAAP5.01, density, thermal conductivity, specific heat capacity, and specific energy of carbon steel and stainless steel were improved.

To accommodate uncertainty in the radiation heat transfer rate on top of the corium pool, the emissivity of the metal layer is made into an input parameter. Also, the view factors for the radiation from the metal layer to the core barrel, and then to the cold vessel wall are considered.

2.3 Lower Head Nodalization

In MAAP4, the lower head wall is nodalized to 5 axial and 5 radial nodes. In MAAP5.01, the number of axial nodes is user controlled and the maximum number of axial nodes is limited to 100. In the IVR application, the number of axial nodes is set to 25 resulting in the node height of 0.08 to 0.09 m. Since the metal layer thickness is in the order of 0.3 to 0.7 m depending on reactor type, several nodes will be submerged by the metal layer such that the 25 axial nodes are sufficient to model the corium debris pool response including the metal layer heat transfer.

2.4 Convective Heat Transfer Rates in Molten Pool

As shown in Figure 1, MAAP assumes formation of a molten pool of oxidic core materials surrounded by the lower crust along the curvature of the lower head wall from bottom to the top of the pool and the upper crust on the top surface of the pool. Unoxidized metals are assumed to separate from the molten oxidic pool and form a separated metal layer on top of the upper crust. MAAP also assumes that the initially fragmented frozen debris particles remain as a particle bed on top of the metal layer. The heavy metal layer is formed after the whole core collapses when the oxidic pool temperature

exceeds the miscibility gap transition temperature. Heat transfer in a molten corium pool is characterized by natural convection in a large self-heated molten pool at very high internal Rayleigh numbers in the neighborhood of 10^{16}-10^{17}. The convective flow in such pool is highly turbulent and the heat flux imposed on the vessel wall varies greatly over the azimuthal angle θ. The heat flux is very low at the bottom of the pool (θ=0) and rises to substantial values at the top elevation of the pool (θ=90°). In MAAP, the molten pool is represented with a single average temperature. In

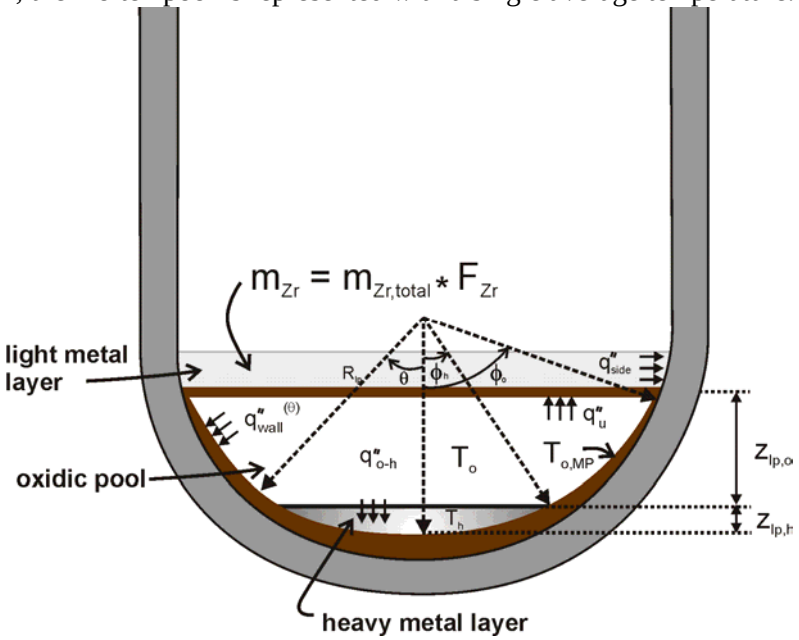


Figure 1 Stratified layers in lower head

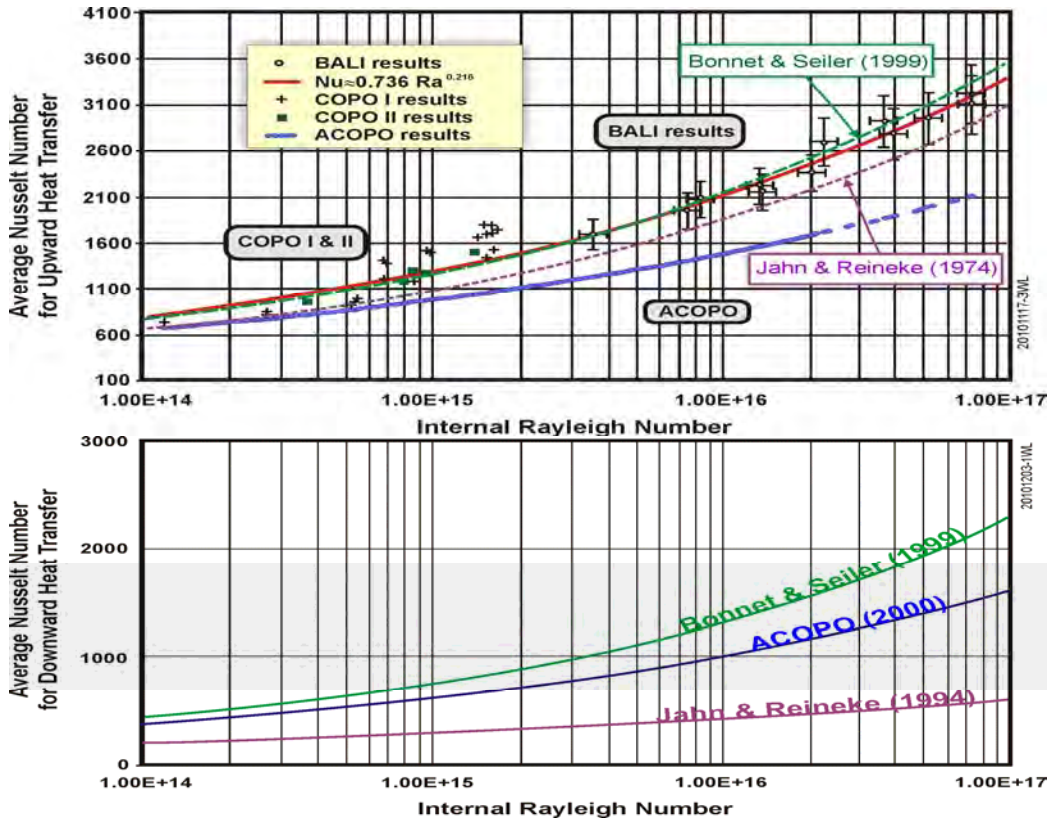


Figure 2 Comparison of average Nusselt number for upward and downward heat transfer data from COPO, BALI, and ACOPO experiments and correlations used in MAAP5.01.

MAAP4, two heat transfer correlations are available to choose from: Jahn-Reineke correlation (Jahn and Reineke, 1974) and Bonnet correlation (Bonnet and Seiler, 1999). In MAAP5.01, ACOPO correlation (Theofanous, 1997) was added. Figure 2 shows comparison between the three correlations.

2.5 Heat Transfer in the Light Metal Layer

1. The model assumes formation of a metal layer over the oxidic debris bed as a consequence of immiscibility and density difference between fuel, structural and control materials. The metal layer may naturally evolve during the melting of the steel structures by radiative heat transfer from the debris or by the submergence of vessel internal components in the molten debris bed. For a molten metal layer, the heat transfer coefficient at the top and bottom surfaces in the molten metal layer, The Globe-Dropkin correlation is used.

MAAP5.01 uses the Churchill and Chu (1975) correlation for the heat transfer between the metal layer and the reactor vessel wall, which is given by

$$\mathrm{Nu} = 1 + \frac{0.15\left(\mathrm{Ra}\cdot\sin\theta\right)^{1/3}}{\left(1+\left(\frac{0.492}{\mathrm{Pr}}\right)^{9/16}\right)^{16/27}} \qquad (1)$$

for Gr > 10^9, where $\Delta T = \bar{T}_{ss} - T_{CS,mp}$. For Gr < 10^9, the laminar natural convection heat transfer coefficient is used:

$$\mathrm{Nu} = 0.68\,\mathrm{Pr}^{1/4}\cdot\left(\mathrm{Pr}+\frac{20}{21}\right)^{-1/4}\cdot\left(\mathrm{Ra}\cdot\sin\theta\right)^{1/4} \qquad (2)$$

Note that the above metal layer to vessel wall heat transfer correlation is based on a model of uniform temperature throughout the melt layer, except across the thermal boundary layer within the steel melt at the vessel wall which represents the only thermal resistance to lateral heat transfer within the steel melt (Figure 3). This model yields the non-physical trend of a monotonically increasing wall heat flux with decreasing steel melt layer thickness. In MAAP5.01 the theory of steel melt layer heat transfer is extended to include the thermal resistances associated with both the vessel wall region and lateral-turbulent free-convection within the central region – that is, in the cylindrically symmetric region of the melt layer sufficiently far from the wall. This new model reveals the expected behavior of wall heat fluxes that tend toward zero as the steel melt layer thickness decreases toward zero.

Figure 4 shows a sketch of a horizontal steel melt layer overlying a corium pool. A frozen corium crust separates the steel melt layer from the molten corium pool. Because of the existence of the crust one can assign a constant uniform heat flux q_p from the corium pool to the base of the metal layer. The metal layer loses heat by thermal radiation off its surface to the exposed surfaces of the steel structure and the inner vessel wall above, all assumed to be at the melting temperature T_{mp} of steel. For a very thin layer, natural circulation plume (the cell-like structure) is effective to transfer heat in axial direction, but ineffective in lateral direction. This leads to assumption that thermal eddy diffusivity is the dominant mode for lateral heat transfer (ignore any momentum flow) and the turbulence that drives this diffusion is isotropic (that is, the same in the vertical and lateral directions).

An empirical thermal eddy diffusivity model (correlation) for heat transfer in the axial direction has been developed by Cheung and Novas (1980). Given the assumption that the diffusion process is isotropic, eddy diffusivity in the lateral direction is assumed equal to an average in the axial direction

as

$$\bar{\varepsilon}_H = 5.22 \times 10^{-3}\ \alpha\, Ra_m^{2/3} = 5.22 \times 10^{-3} \alpha \left(\frac{gH^4 \beta q}{\alpha \nu k} \right)^{2/3} \quad (3)$$

where α is thermal diffusivity, Ra_m is modified Rayleigh number, g, H, β, ν and k are gravity acceleration, thickness of the layer, thermal expansion ratio, kinetic viscosity, and heat conductivity respectively. The q term in the Ra_m is the radiation heat flux leaving the top surface. Eventually, this leads to an energy equation in the lateral direction as

$$-\frac{H}{r}\frac{d}{dr}\left[r \left(k + \rho c_p \bar{\varepsilon}_H \right) \frac{dT}{dr} \right] = q_p - q \quad (4)$$

where q_p is the heat flux from the corium pool to the base of the metal layer. Zero temperature gradient is assumed in the center (r=0) for the above equation; boundary condition at the outer boundary (r=R) is given by

$$-\left(k + \rho c_p \bar{\varepsilon}_H \right) \frac{dT}{dr}\bigg|_{r=R} = 8.68 \times 10^{-2} k \left(\frac{g\beta}{\alpha \nu} \right)^{1/3} \left(T(R) - T_{mp} \right)^{4/3} \quad (5)$$

where the left hand side is the heat flux from the model; the right hand side is simply the heat flux from Churchill-Chu correlation. The energy equation is solved numerically to obtain the lateral temperature distribution in the steel layer. The heat flux from the steel layer to the wall is then simply given by the right hand side of Equation (5).

For typical properties of steel, Figure 5 shows the predicted wall heat flux as a function of the steel melt layer thickness for q_P = 1 MW m^{-2} and R = 2.0 m. The lower curve is the locus of results obtained with the present model which incorporates the effect of eddy diffusivity. The upper curve is constructed from the model without the eddy diffusivity consideration; that is, the heat flux is based on a uniform temperature distribution in the steel layer. Both models agree in the thick steel melt layer limit. As the steel layer becomes thinner, the heat flux increases as expected. However, the eddy diffusivity model predicts the heat flux to turn around after reaching a maximum value. Unfortunately, the maximum heat flux predicted by the eddy diffusivity model is around 6 MW m^{-2}, well above typical CHF, and will not help to mitigate the "focusing effect" in practice.

2.6 Formation and Composition of Heavy Metal Layer

During a severe accident, the corium pool formed in the lower plenum may stratify in layers. If most of zirconium (Zr) in the corium has been oxidized, the corium pool is primarily comprised of a light steel layer at the top and a heavy oxidic layer at the bottom. If there is significant amount of un-oxidized Zr present in the corium, some experiments such as RASPALV and MASCA indicate that Zr will reduce UO_2 to elemental U. The elemental U can carry Zr and iron to form a separate heavy metal layer on the bottom. This phenomenon may be postulated to reduce the upper metal layer thickness and make the focusing effect worse.

In MAAP5.01, the heavy metal layer is formed only once after the whole core has collapsed and when the oxidic pool temperature exceeds the miscibility gap transition temperature, a user input parameter. The approach used by Salay and Fichot (2004), which is based on the U-Zr-O-Fe quaternary phase diagram, is used to determine the composition of the heavy metal layer formed. Following assumptions are made in the model:

a) The corium pool is primarily comprised of UO_2, ZrO_2, Zr metal and stainless steel. The amount of steel in the corum pool, as oppose to in the light metal layer, is a user input parameter. Once the heavy metal is formed, the remaining steel stays in the oxidic pool; the amount of steel in the light metal layer is not affected and is always in deficit of the user input value.

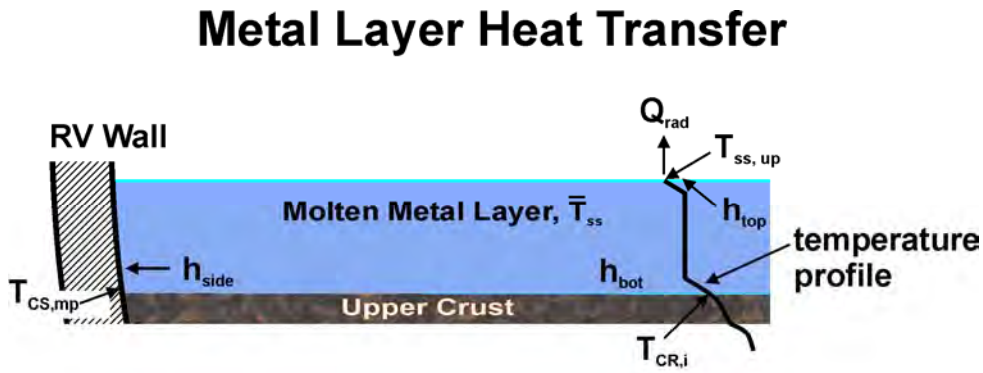


Figure 3 Metal layer heat transfer.

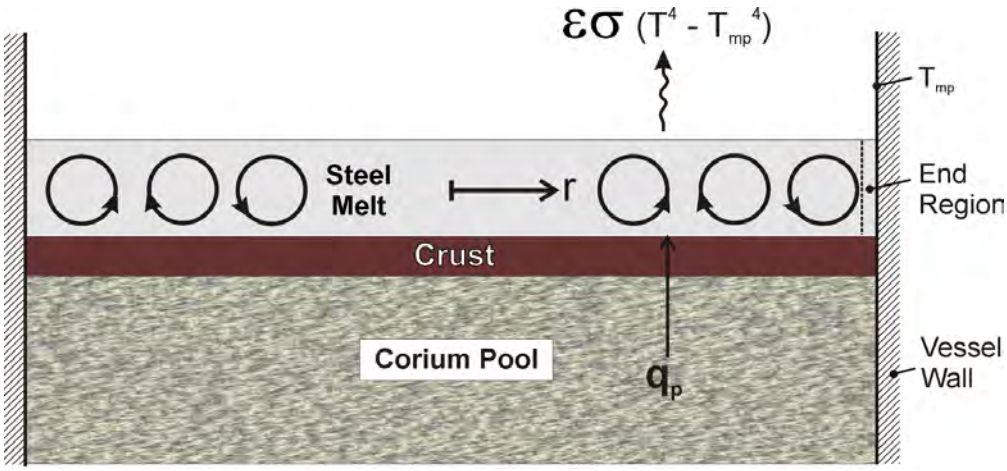


Figure 4 Microscopic Patterns in the Melting Steel Layer Heated from the Bottom

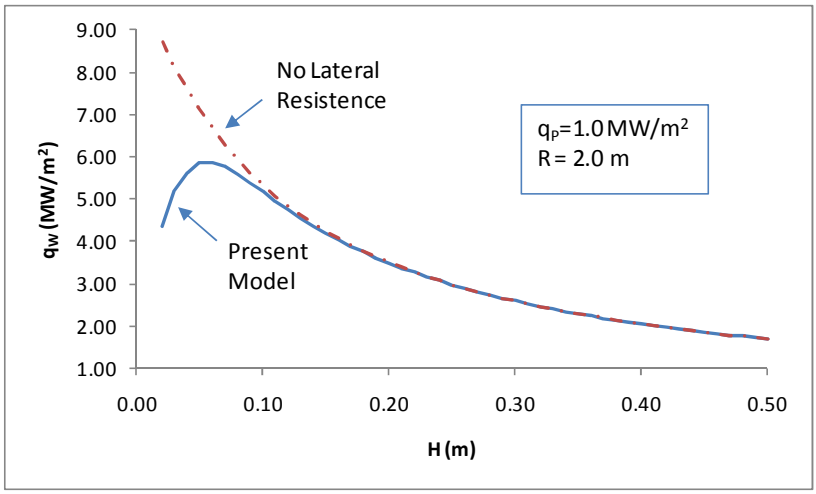


Figure 5 Comparisons of Present Model and the Model without Lateral Resistance

b) Since the corium temperature is higher than the miscibility gap initiation temperature, the corium pool is partitioned into two immiscible liquids: one metallic and one oxidic. The U-Zr-O-Fe phase diagram determines the partitioning and is assumed to be temperature invariant.
c) The U/Zr ratio is assumed to be same in the metallic and oxidic liquids.
d) The tie line that goes through the point of average constituents and links two points on the miscibility boundary in the phase diagram is determined by the intersection of the U-Zr-Fe and U-Zr-O planes. The fraction of iron at the intersection in the U-Zr-Fe plane is proportional to the fraction of Oxygen at the intersection in the U-Zr-O plane.

With these assumptions and curve-fitted miscibility boundaries, Lever's law can be applied to determine the constituents in the metallic and oxidic phases. The uranium and Zr mass fractions in the metallic phase in the MASCA experiments are calculated using this method and compared against the data in Table 1. A reasonable agreement is obtained.

In MAAP5.01, the decay heat is partitioned according to the relative amount of uranium in each phase. Once the three distinct layers are established, heat transfer rates between the layers and the vessel wall ablation rates are determined.

Test	Experiment		Calculated	
	X_U	X_{Zr}	X_U	X_{Zr}
MA-1	0.430	0.110	0.437	0.111
MA-2	0.200	0.060	0.248	0.073
MA-3	0.420	0.170	0.444	0.154
STFM-2	0.560	0.210	0.596	0.191
STFM-3	0.630	0.220	0.621	0.217
STFM-4	0.530	0.190	0.564	0.196
STFM-5	0.570	0.240	0.619	0.216
STFM-6	0.560	0.200	0.576	0.183
STFM-7	0.470	0.200	0.532	0.169
STFM-8	0.000	0.000	0.070	0.017
STFM-9	0.520	0.190	0.496	0.173
STFM-14	0.410	0.150	0.318	0.111
STFM-15	0.440	0.140	0.504	0.149

Table 1 Comparison between calculated and measured mass fractions in metallic phase

2.7 Ex-Vessel Cooling Channel Model

One key IVR design feature is the cooling channel between the reactor vessel wall and the insulation, which drives a natural circulation flow and promotes heat transfer on the vessel wall. In MAAP5.01, a new model was created for the insulation cooling channel. The model tracks the enthalpy of circulating water as it enters the channel at the bottom and rises along the vessel wall, receiving heat from the vessel wall and going through phase change until it exits through the vent at the top of the channel. Starting from the bottom of the channel, mass, momentum, and energy equations are solved for individual channel nodes assuming quasi-steady state. The key results of the model are the channel water circulation flow rate and the formation of a dryout region in the channel.

For the submerged reactor vessel the ex-vessel heat transfer correlations available in MAAP5.01 are Rohsenow correlation (Rohsenow and Choi, 1961), Yang's correlations for plain vessel and with enhanced thermal insulation (Yang et al., 2005). For the critical heat flux (CHF), Yang's correlations for plain vessel and with enhanced thermal insulation, ULPU-2000 configuration II correlation (Theofanous and Syri, 1997) for plain vessel, and UPLU-2000 configuration IV correlation (Theofanous et al., 2002) for plain vessel with curved baffle are available.

3. AP1000® passive plant test case results

The test case is a DVI line break with failure of gravity injection. This is a conservative IVR scenario because it features a very early core melt, high decay heat and minimum zirconium oxidation. The following assumptions were made:

- Passive Residual Heat Removal (PRHR) is not available.
- Only one of ADS 2/3 and 3 of ADS 4th stages are available.
- One Core Makeup Tank (CMT) is available.
- No accumulators are available.
- Passive injection squib valves fail to open for gravity injection
- Cavity flooding is available.
- PCS water cooling is available.
- In MAAP4 and previous versions of MAAP5, the metal layer consists of steel only. In MAAP5.01, a user input parameter is introduced to specify the fraction of un-reacted Zr that is included in the metal layer. In this study, it is assumed that all the zirconium mixes with the oxide and there is no Zr is in the top metal layer.
- The emissivity of the metal layer is one of the key parameters that determine the metal layer temperature and the lateral heat transfer to the vessel wall from the metal layer. In this study, the emissivity of molten stainless steel of 0.43 is assumed.
- The maximum amount of steel that can participate in forming the heavy metal layer is set to 5,000 kg. Hence, the amount of steel in the light metal layer is reduced by 5,000 kg. In the AP1000® plant design, the steel mass in the lower plenum below the thick core support plate is less than 5,000 kg. Therefore, a reduction of 5,000 kg in the light metal layer is a reasonable assumption.
- The number of axial nodes is set to 25, resulting in a node height of about 0.08 m for the AP1000® passive plant.
- Heavy metal layer is formed after the whole core has collapsed when the oxidic pool temperature exeeds 2,650 K.

The reactor scrams at 18 seconds due to the SI signal. The ADS stage 2/3 valve is opened at 385 seconds and the 4th stage ADS is opened at 473 seconds, leading to a rapid depressurization of RCS. With no injection available, the core is uncovered at 523 seconds. About 207 kg of hydrogen in generated in the core (21.5% of Zr oxidation). Core material is initially relocated to lower plenum at 2,960 seconds when the side crust of the molten core fails. The molten debris in the lower plenum

contacts the lower core support plate from below and it begins to melt. When most of the core support plate has melted, the core support plate fails, resulting in collapse of the entire core and the core shroud at around 5,100 seconds.

Figure 6 shows a snapshot of the corium pool in lower plenum at 30,000 seconds. The lighter metal layer sits on top of the heavier oxidic corium pool, with a thin upper crust between them. The lower crust is thickest at the bottom, where the wall heat flux is lowest. The vessel wall is intact on the bottom but is melted significantly on the upper part. For the vessel wall adjacent to the metal layer only about 20% of the original wall thickness remains intact and the rest has melted away. Although the corium pool is significantly hotter than the metal layer, the surrounding crust provides sufficient thermal resistance and protects the vessel wall whereas the molten metal layer is in direct contact with the vessel wall.

Figure 7 shows various corium levels and heights in the lower plenum. The initial 5,000 kg of steel goes into the oxidic pool, participating in the heavy metal formation later on. The subsequent steel delivered to the lower plenum goes into the light metal layer. During the initial relocation to the water pool in lower plenum, the molten corium jet breaks up into particulates, which are quenched and form a particulate bed. When water in the lower plenum dries out, the particulate bed heats up, melts, and rejoins the molten oxidic pool below. In this sequence the particulates join the oxidic pool when it is completely submerged in the molten steel layer, causing a sudden decease in the metal layer thickness after 6,000 seconds

At 5,470 seconds, the heavy metal layer is formed when the whole core collapses and is added to the oxidic pool, and the oxidic pool temperature exceeds the miscibility gap transition temperature of 2,650 K. Table 2 shows the composition of the heavy metal layer. Of the initial 5,000 kg of steel in the oxidic pool, a user input, 4,172 kg becomes part of the heavy metal layer. The remaining 828 kg stays in the oxidic pool.

Component	Mass (kg)
U	9,729
UO_2	992
Zr	2,616
ZrO_2	0
Steel	4,172
Total	17,510

Table 2 Composition of the Heavy Metal Layer

At 30,000 seconds, the thickness of top light metal layer is about 0.73 m while the level of bottom heavy metal layer is about 0.6 m.

Figure 8 shows the temperatures of various components in the lower plenum. At 30,000 seconds, the oxidic pool and heavy metal layer temperature is about 2,650 K and the light metal layer temperature is about 1,930 K. Figure 9 shows the radial temperature profile in the bottom vessel wall node. It spans from 400 K at the outer surface to 1,340 K at the inner surface. For the bottom node the entire wall thickness remains intact. Figure 10 shows the radial temperature profiles in the upper vessel wall node adjacent to the light metal layer. The temperature gradient in the wall becomes steeper as the wall becomes thinner due to melting. Near the light metal layer a wall thickness as thin as 2.67 cm is predicted.

Figure 11 shows heat balance in the debris bed in lower plenum. It confirms approximate energy balance between the decay heat and the downward, sideward, and upward heat loses. About the same amount of heat is removed sideward in the light metal layer as downward in the oxidic pool. Figures

12 and 13 show the heat fluxes and the heat flux to CHF ratios on the ex-vessel wall. The peak heat flux of about 1.4 MW/m^2 occurs at vessel wall nodes 23 to 25. The corresponding heat flux to CHF ratio is below 0.73. When the vessel wall is initially submerged by cavity flooding, the heat flux to CHF ratio briefly reaches 0.8.

The MAAP5.01 creep model is identical to the MAAP4 creep model, which is based on stress rupture test data. The model gives the time-to-fail for a given stress and temperature combination, and is normally correlated in terms of the Larson-Miller parameter (LMP). When the model is applied to predict creep failure of the reactor vessel lower head, where there is a significant temperature gradient along the thickness, the imposed hoop stress is distributed among individual lamina such that the creep failure time is identical for all lamina. The damage fraction, determined by dividing the time step by the time-to-fail, is accumulated until the sum exceeds one, at which point the lower head is considered to have failed by creep. The model has been validated against the hot leg and lower head failure experiments (Lee et al., 2009). In the AP1000® passive plant test case, the vessel wall creep rupture did not occur because the outer surface temperature was maintained near 400 K; the vessel wall, although thinned due to extensive melting, was able to support the load.

5. Summary

Models important to the IVR evaluation were implemented in MAAP5.01 and were successfully tested for the AP1000® passive plant. Time-dependent, sequence-specific calculations allow the user to evaluate the vessel integrity during the relocation transient as the whole core relocates to lower plenum. The key parameters affecting the IVR success are the metal layer emissivity and thickness of the top metal layer, which depends on the amount of steel in the oxidic pool and in the heavy metal layer. With best estimate inputs for debris mixing parameters in a conservative IVR scenario, the AP1000® passive plnat results show that the ex-vessel heat flux to CHF ratio reaches about 0.7, which occurs before 10,000 seconds, when the decay heat is high. The AP1000® passive plant results demonstrate that MAAP5.01 can be used to evaluate the effectiveness of IVR and to gain insight into responses of the lower head during a severe accident.

6. References

American Nuclear Society (ANS), 1979, Decay Heat Power in Light Water Reactors, ANSI/ANS-5.1-1979, La Grange Park , IL.

American Nuclear Society (ANS), 1994, Decay Heat Power in Light Water Reactors, ANSI/ANS-5.1-1994, La Grange Park , IL.

American Nuclear Society (ANS), 2005, Decay Heat Power in Light Water Reactors, ANSI/ANS-5.1-2005, La Grange Park , IL.

Bonnet, J.M., and Seiler, J.M., 1999, “Thermal-Hydraulic Phenomena in Corium Pools for Ex-Vessel Situations: the BALI Experiment,” Proceedings of the International Conference on Nuclear Engineering (ICONE 7), April 19-23, Tokyo, Japan.

Cheung, F.B. and Novas, J.B., 1980, "Heat Transfer in an Optically Thick Fluid Layer Heated from Below," Letters in Heat and Mass Transfer 7, pp. 171-181.

Churchill, S.W. and Chu, H.S., 1975, "Correlating Equations for Laminar and Turbulent Free Convection from a Vertical Plate," Int. J. Heat Mass Transfer 18, pp. 1323-1329.

Daw, J., Rempe, J., & Knudson, D. (2010). Thermal properties of structural materials used in LWR vessels, Journal of Nuclear Materials 401 , 65-70.

Jahn, M., and Reineke, H.H., 1974, “Free Convection Heat Transfer With Internal Heat Sources, Calculations and Measurements,” Proc. of the 5th Intl. Heat Transfer Conf., Tokyo, Japan, Paper NC2.8.

Lee, S.J., Henry, R.E., Paik, C.Y., Conzen, J., Luangdilok, W., 2009, “MAAP4 Hot Leg and Lower Head Failure Benchmarking”, NURETH-13, Kanazawa city, Japan, September 27-October 2.

Rohsenow, W. M., and Choi, H., 1961, Heat, Mass, and Momentum Transfer, Prentice-Hall.

Salay, M., and Fichot, F., 2004, Modeling of corium stratification in the lower plenum of a reactor vessel, OECD/CSNI Workshop on MASCA.

Theofanous, T.G., Liu, C., Additon, S., Angelini, S., Kymäläinen, O., and Salmassi, T., 1996, In-Vessel Coolability and Retention of a Core Melt, DOE/ID-10460, Volume 1, Department of Energy, October.

Theofanous, T.G., 1997, “In-Vessel Retention as a Severe Accident Management Strategy”, Plenary Lecture, Proc. NURETH-8, Kyoto, Japan, September 30 – October 4.
Theofanous, T.G., Syri, S., 1997, “The Coolability Limits of a Reactor Pressure Vessel Lower Head”, Nucl. Eng. Des., Vol. 169, pp59-76.

Theofanous, T.G., Tu, J. P., Salmassi, T., Dinh T. N., 2002, “Quantification of Limits to Coolability in ULPU-2000 Configuration IV”, Center for Risk Studies and Safety, University of California, Santa Barbara, CRSS-02.05.3, May 23.

Yang, J., Cheung, F.B., Rempe, J.L., Suh, K.Y., and Kim, S.B., 2005, Correlation of Nucleate Boiling Heat Transfer and Critical Heat Flux for External Reactor Vessel Cooling, ASME Summer Heat Transfer Conference, San Francisco, CA, 17-22 July.

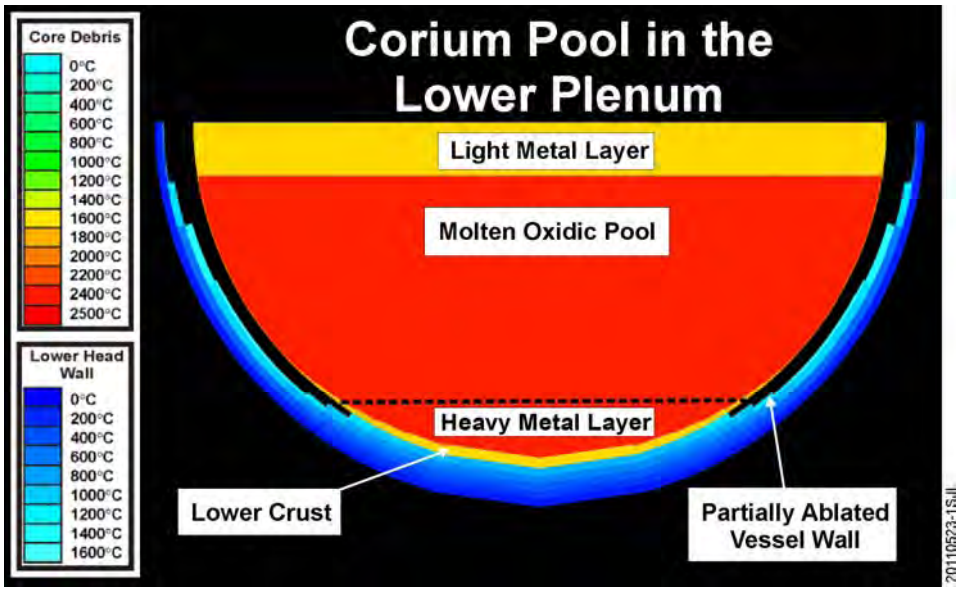


Figure 6 Temperature profile in the corium pool and vessel wall at 30,000 seconds.

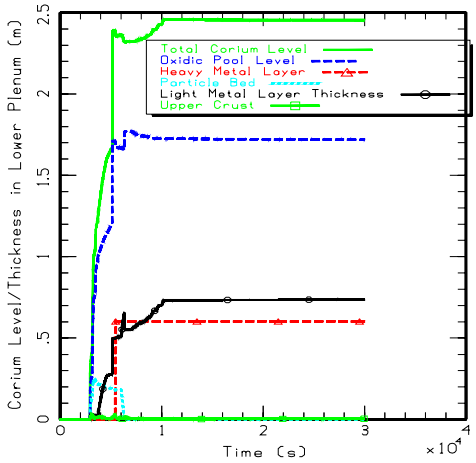


Figure 7 Corium level/thickness in lower plenum.

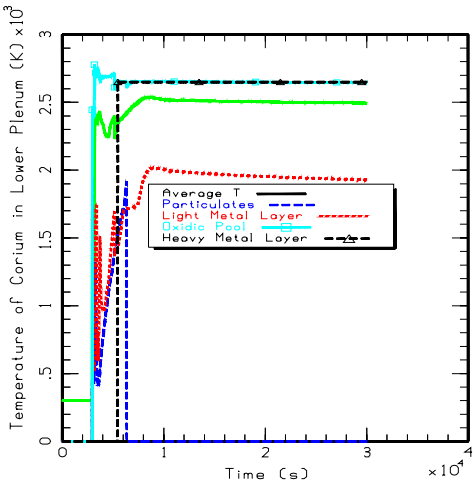


Figure 8 Temperature of corium in lower plenum.

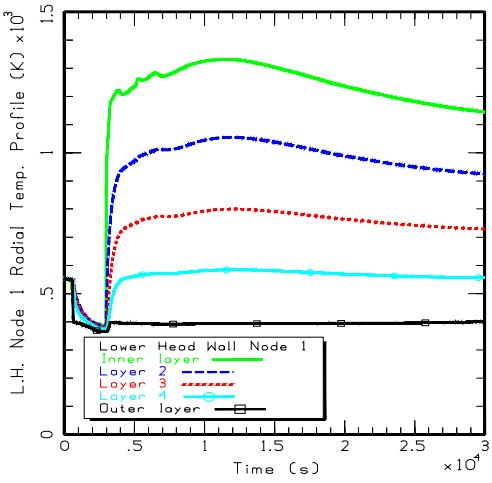


Figure 9 Temperature profile across the thickness of the lower head bottom node.

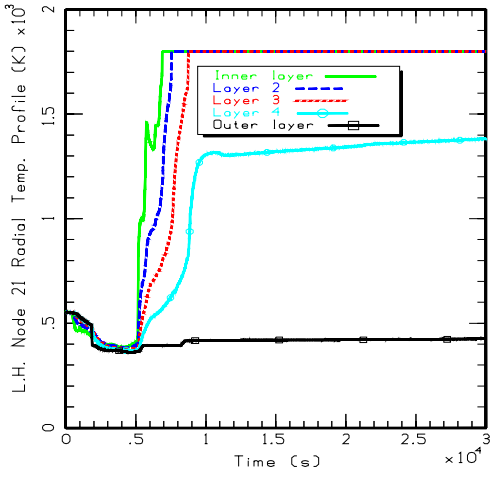


Figure 10 Temperature profile across the thickness of the upper lower head node in contact with the light metal layer.

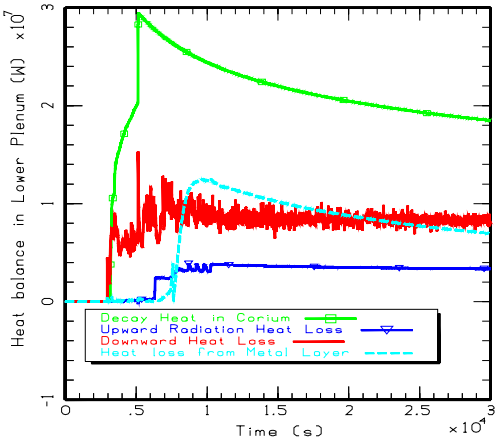


Figure 11 Heat balance in the corium pool in lower plenum.

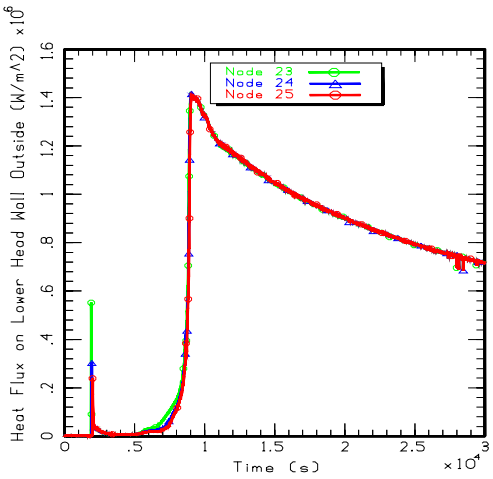


Figure 12 Heat flux on the vessel wall in contact with light metal layer.

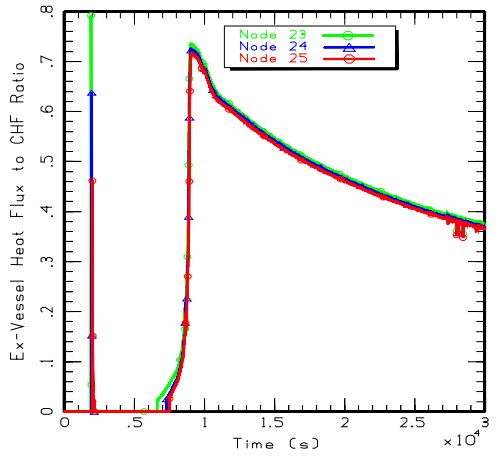


Figure 13 Ex-vessel heat flux to CHF ratio.

In-Vessel Retention Modeling Capabilities in MAAP5

FAUSKE & ASSOCIATES, LLC

Chan Y. Paik[1], Sung Jin Lee[1], James H. Scobel[2], Quan Zhou[1],
Wison Luangdilok[1],
Robert W. Reeves[1], Robert E. Henry[1], and Martin Plys[1]

[1]Fauske and Associates, LLC
Burr Ridge, Illinois

[2]Westinghouse Electric Company
Cranberry, Pennsylvania

OECD/NEA Workshop on PSA for New and Advanced Reactors

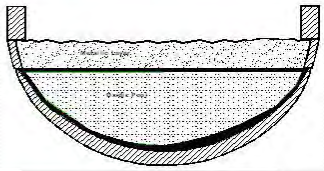
June 20-22, 2011

16W070 83rd Street • Burr Ridge, Illinois 60527
(877) Fauske1 or (630) 323-8750 • Fax: (630) 986-5481 • E-mail: info@fauske.com

1

Introduction

- IVR is a severe accident management strategy to prevent vessel failure and retain molten debris in the reactor vessel.
- The reactor vessel is externally cooled with manually injected water to remove decay heat from debris inside the lower plenum.
- If the heat transferred from the debris to the vessel walls can be removed by boiling on the external surface, the vessel will remain intact.
- Keeping the reactor vessel intact with debris retained within the reactor vessel prevents:
  - ex-vessel steam explosion
  - molten core-concrete interaction
  - ex-vessel hydrogen generation



Introduction (cont.)

- The success of IVR depends on the delicate balance between :
- the decaying heat load in the corium pool,
- highly effective nucleate boiling heat transfer on the outside,
- radiative heat removal from top of the overlying metal layer, and
- enhanced lateral heat flow in the floating steel melt to the vessel wall often referred to as the heat "focusing effect".
- Even with water available for external cooling, a high heat flux to vessel wall can threaten the integrity of the reactor vessel when the critical heat flux is exceeded or when the wall has thinned sufficiently due to melting.

Introduction (cont.)

- Here we present MAAP5.01 as the tool for integrated, sequence-specific, time-dependent evaluation of the vessel integrity under the severe core damage conditions with IVR-intended operator actions.

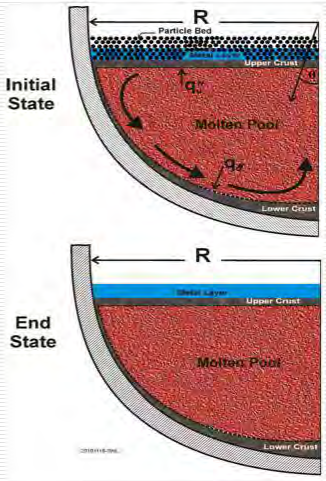
- AP1000 is used as an example for demonstration of the IVR analysis.

Severe Accident Phenomena modeled in MAAP and Evolution of MAAP versions

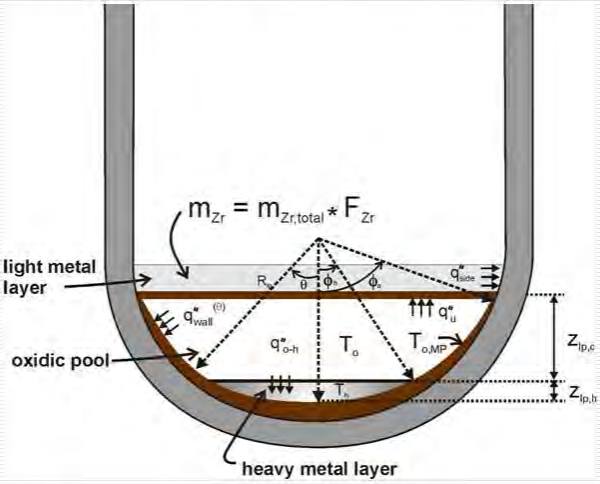
Severe Accident Phenomena	Next MAAP version(s) where significant model improvement introduced.	MAAP version(s) where minor model revision introduced.	Remarks
In-vessel hydrogen generation		4.0.2, 4.0.4, 4.0.5, 4.0.6, 4.0.7	This is also affected by core relocation.
In-vessel core relocation		4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.0.6	
In-vessel fission product release	MAAP5.01: add release of I_2, CH_3, $CsMo_2O_4$, Ru, Pu	4.0.3	Release is also affected by core relocation and H2 generation.
Hot leg creep rupture Surge line creep rupture SG tube creep rupture		4.0.5	
In-vessel molten core coolability		4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.0.6, 4.0.7	
In-vessel melt retention (IVR)	MAAP5.01	MAAP4 not recommended	
In-vessel steam explosions		Not modeled	
RPV failure		4.0.4, 4.0.5, 4.0.7, 4.0.8	
Direct containment heating		4.0.6, 4.0.7	
Hydrogen burning		4.0.4	
Ex-vessel steam explosions		4.0.4	This is modeled only as side calculation of peak pressure at given distance from center of interaction.
Ex-vessel debris coolability	MAAP4.0.8 and MAAP5.01	4.0.7	Similar results as next versions can be achieved if governing parameter FCHF=0.01 is used.
MCCI-induced concrete ablation		4.0.7	
Ex-vessel hydrogen generation		none	This is affected by concrete ablation.
Ex-vessel fission product release		4.0.4, 4.0.6	
Fuel heatup and meltdown in spent fuel pool	MAAP5.01	N/A in MAAP4	New development

MAAP4/5 Modeling of IVR

- Within the lower plenum of a reactor vessel , a molten pool of oxidic core materials is formed and is surrounded by the lower crust along the curvature of the lower head wall and the upper crust on the top surface of the pool.
- On top of the upper crust unoxidized metals are assumed to separate from the molten oxidic pool and form a separate metal layer.
- MAAP also assumes that the initially fragmented frozen debris particles remain as a particle bed on top of the metal layer until they melt.



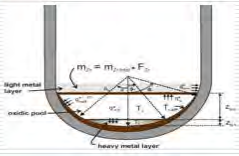
MAAP5.01 Modeling of IVR



Formation of Heavy Metal Layer in Corium Pool in MAAP5.01

- If most Zr is oxidized, heavy metal layer would not form.
- If significant amount of unoxidized Zr is present, Zr would reduce UO_2 to U, then U carries Zr and Fe to form a heavy metal layer at the bottom of the corium pool.
- The formation of heavy metal layer reduces the thickness of the light metal layer creating the focusing effect.

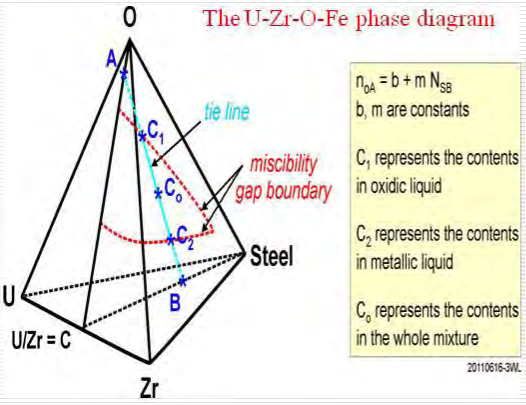
- Heavy metal layer is formed after the entire core has collapsed and relocated to the lower plenum.
- When oxidic pool temperature exceeds the miscibility gap transition temperature.
- Composition of the heavy metal layer is determined according to the Salay and Fichot (2004) approach.



The Salay and Fichot (2004) Approach for Heavy Metal Layer Formation.

- The corium pool is primarily comprised of UO_2, ZrO_2, Zr metal and stainless steel. The amount of steel in the corium pool, as oppose to in the light metal layer, is a user input parameter
- The U-Zr-O-Fe phase diagram determines the partitioning
- The U/Zr ratio is assumed to be same in the metallic and oxidic liquids

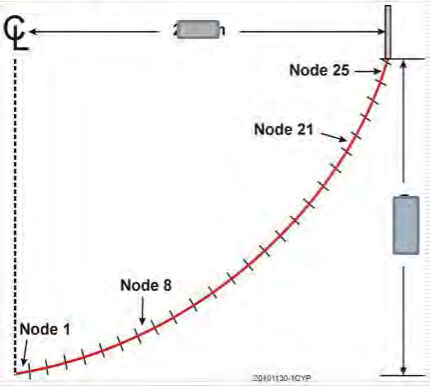
The Salay and Fichot (2004) Approach for Heavy Metal Layer Formation – (continued)



The tie line that goes through the point of average constituents and links two points on the miscibility boundary in the phase diagram is determined by the intersection of the U-Zr-Fe and U-Zr-O planes. The fraction of iron at the intersection in the U-Zr-Fe plane is proportional to the fraction of Oxygen at the intersection in the U-Zr-O plane

MAAP5.01 Lower Head Nodalization

25-node model has enough resolution to capture the thin light metal layer residing in Nodes 21 to 25.



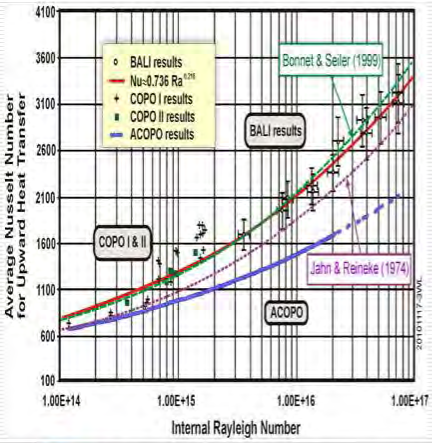
- The total number of axial nodes can be varied up to a maximum of 100 using an input parameter NNODELH.
- The radial nodes are fixed with 5 layers across the thickness of the vessel wall (same as in MAAP4).
- The external cooling channel is automatically nodalized to the same number of nodes as the axial nodes of the lower head wall.

Heat Transfer Correlations for Molten Pools

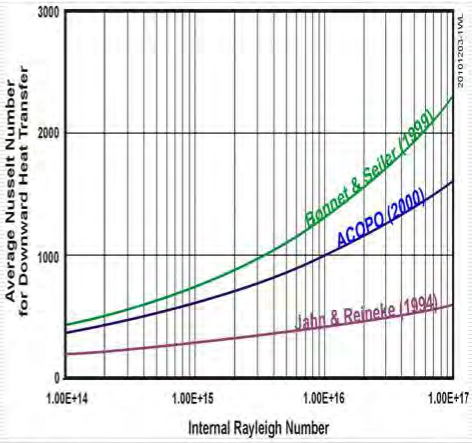
Related Experiment	COPO (Kymalainen et al.1992)	BALI	ACOPO
Authors	Jahn and Reineke (1974)	Bonnet and Seiler (1999)	Theofanous and Angilini (2000)
MAAP Control Parameter	IOXIDHT=0	IOXIDHT=1	IOXIDHT=2
Upward Heat Transfer to Upper Crust	$Nu_u = 0.345Ra^{0.233}$	$Nu_u = 0.466Ra^{0.229}$	$Nu_u = 1.95Ra^{0.18}$
Downward Heat Transfer to Curved Lower Head Wall	$Nu_d = 0.54Ra^{0.18}\left(\frac{2}{R}\right)^{0.26} f(\theta)$	$Nu_d = 0.131Ra^{0.25}\left(\frac{2a}{3R-z}\right)^{\frac{0.25}{0.25}} f(\theta)$	$Nu_d = 0.3Ra^{0.22}\ F(\theta)$
	$f(\theta) = C_\theta = \left(\frac{8(1-C_\theta)(1-\cos\phi)}{3(\phi-\cos\phi\sin\phi)-2\sin^3\phi\cos\phi}\right)\sin^3\theta$ where $C_\theta = 0.25$, $\phi = \cos^{-1}\left(\frac{R-Z}{R}\right)$		See definition of F(θ) below
Sideward Heat Transfer to Vertical wall	$Nu_s = 0.85Ra^{0.19}$		
Note	$F(\theta) = 0.1 + 1.08\left(\frac{\theta}{\phi}\right) - 4.5\left(\frac{\theta}{\phi}\right)^2 + 8.6\left(\frac{\theta}{\phi}\right)^3$ for $0.1 \le \left(\frac{\theta}{\phi}\right) \le 0.6$ And $F(\theta) = 0.41 + 0.35\left(\frac{\theta}{\phi}\right) + \left(\frac{\theta}{\phi}\right)^2$ for $0.6 < \left(\frac{\theta}{\phi}\right) \le 1.0$ $Ra = \frac{g\beta q_v L^5}{\alpha\nu k_{px}}$ Length scale L = R (lower radius) or corium pool depth		

Comparison of Molten Pool Heat Transfer Correlations used in MAAP5.01

Upward Heat Transfer

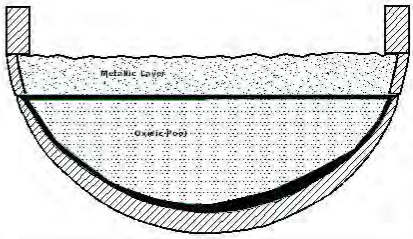


Downward Heat Transfer



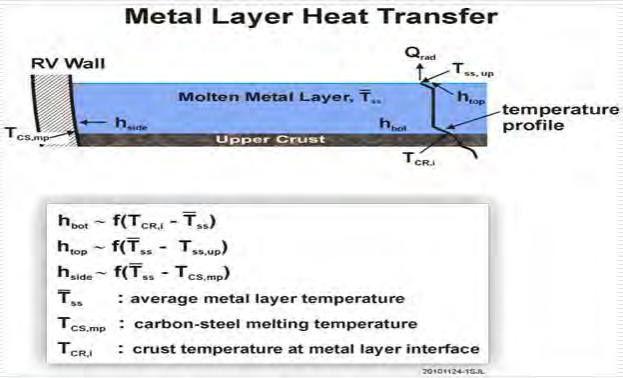
Heat Flux from Metal Layer to RPV Wall: Key Mechanism for Vessel Failure

- Metal layer is relatively thin with respect to vessel radius
- Heated from below by the molten pool
- Cooled on top by radiation to reactor internal structures
- Sidewall temperature is fixed at the melting temperature of the vessel wall



Natural Convection Heat Transfer in Light Metal Layer

Globe-Dropkin correlation for upper and lower boundary	$Nu = 0.069\ Ra^{1/3}\ Pr^{0.074}$
Churchill and Chu [1975] correlation for side boundary	$Nu = 1 + \dfrac{0.15\,(Ra \cdot \sin\theta)^{1/3}}{\left(1 + \left(\dfrac{0.492}{Pr}\right)^{9/16}\right)^{16/27}}$

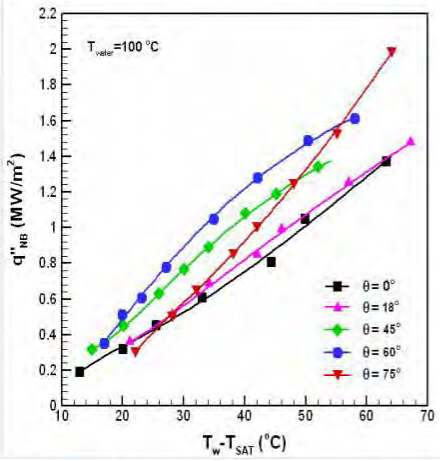


Heat Transfer Correlations for External Reactor Vessel Cooling (ERVC)

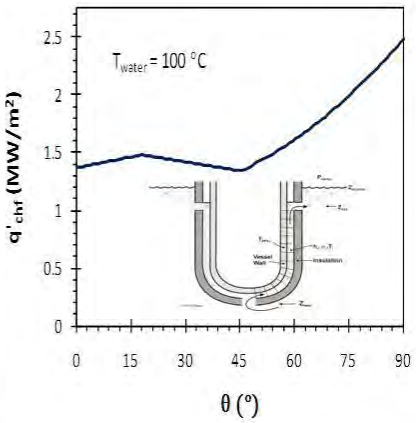
- Yang et al (2005)'s correlation for nucleate boiling heat transfer for plain vessel and with enhanced thermal insulation.
- Yang et al (2005)'s correlation for critical heat flux for plain vessel and with enhanced thermal insulation.
- ULPU-2000 configuration II correlation for ….. for plain vessel (Theofanous & Syri, 1997).
- ULPU-2000 configuration IV correlation for ….. for plain vessel with curved baffle(Theofanous et al, 2002).
- Rohsenow's correlation for……..(Rhosenow & Choi, 1961)

Yang (2005)'s Nucleate Boiling Heat Transfer Data for Channel Flow

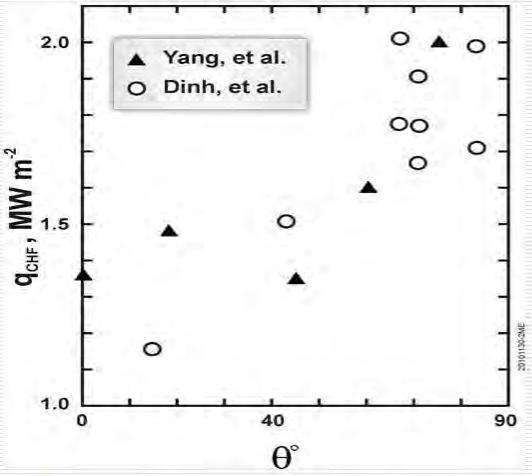
Nucleate Boiling



Critical Heat Flux

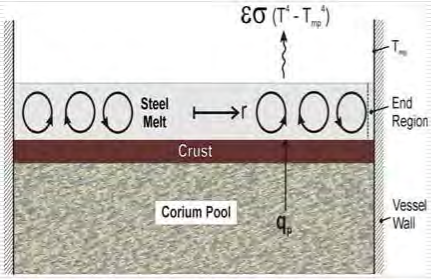


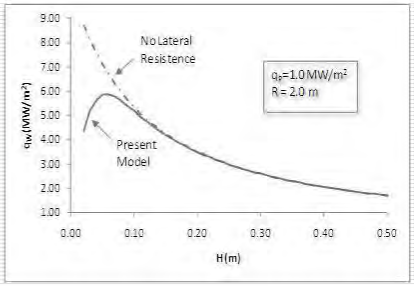
Other CHF Data for Natural Convection Boiling Channel Flow



- Comparison of data by Dinh et al. (2003) and Yang et al. (2005).
- Data are highly scattered above 1.6 MW/m^2

The Focusing Effect





Light Metal Layer Lateral Heat Transfer to Vessel Wall

- Energy equation

$$-\frac{H}{r}\frac{d}{dr}\left[r\left(k+\rho c_p\bar{\varepsilon}_H\right)\frac{dT}{dr}\right]=q_p-q$$

- Eddy diffusivity (Cheung and Novas, 1980) – assume lateral direction same as axial direction

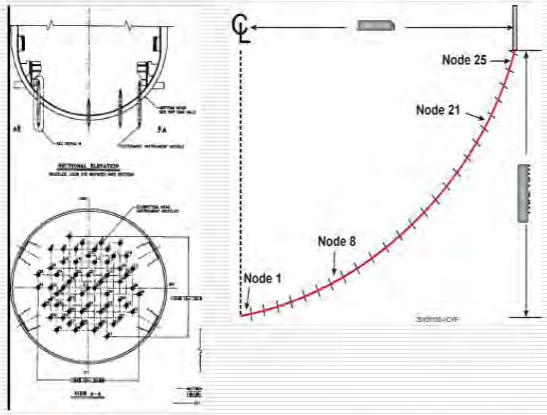
$$\bar{\varepsilon}_H=5.22\times10^{-3}\,\alpha Ra_m^{2/3}=5.22\times10^{-3}\alpha\left(\frac{gH^4\beta q}{\alpha\nu k}\right)^{2/3}$$

- B.C. at outer boundary (r=R)

$$-\left(k+\rho c_p\bar{\varepsilon}_H\right)\left.\frac{dT}{dr}\right|_{r=R}=8.68\times10^{-2}k\left(\frac{g\beta}{\alpha\nu}\right)^{1/3}\left(T(R)-T_{mp}\right)^{4/3}$$

- B.C. at center (r=0) : dT/dr=0

Impact of Instrument Penetrations on IVR



- Penetrations may be present, for example, in nodes 1 to 8.
- Penetration tube failures can be predicted even with ERVC available at node 8 due to melting of vessel wall at 1800 K.

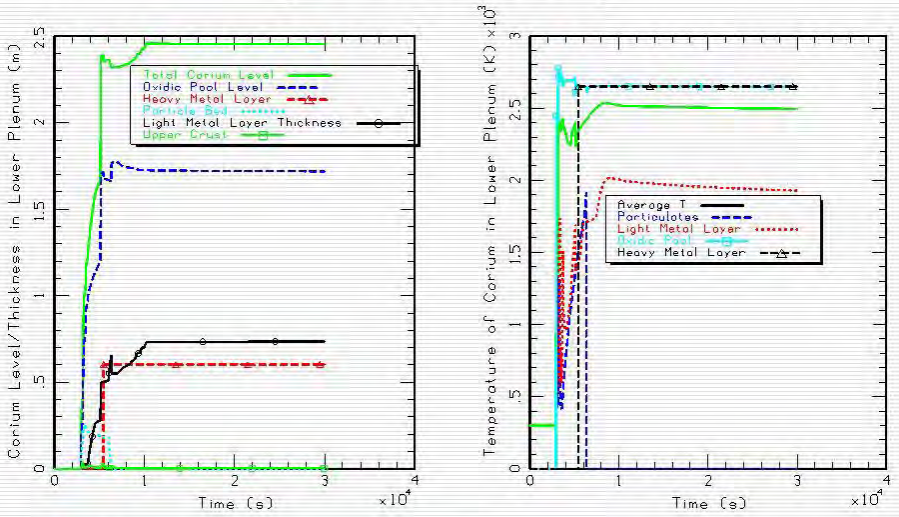
AP1000® Passive Plant Test Case

- The test case is a DVI line break with failure of gravity injection.
- The test case is a conservative IVR scenario because it features a very early core melt, high decay heat and minimum zirconium oxidation.
- AP1000® has no instrument penetrations in the lower head.
- Passive Residual Heat Removal (PRHR) is not available.
- Only one of ADS 2/3 and 3 of ADS 4th stages are available.
- One Core Makeup Tank (CMT) is available.
- No accumulators are available.
- Passive injection squib valves fail to open for gravity injection.
- Cavity flooding is available.
- PCS water cooling is available.

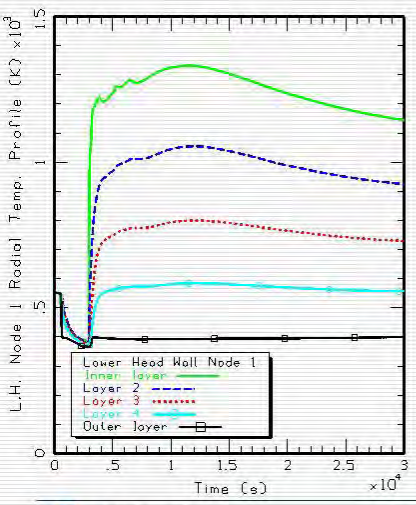
Assumptions

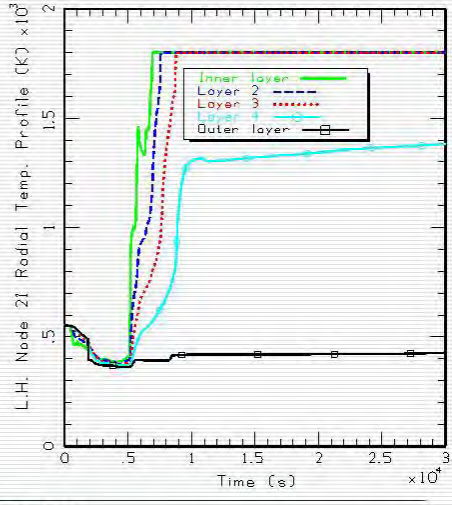
- All the zirconium mixes with the oxide and there is no Zr in the top metal layer.
- The maximum amount of steel that can participate in forming the heavy metal layer is limited to the amount of steel in the lower plenum below the thick core support plate. For AP1000® plant design, this is less than 5,000 kg. This is a reasonable assumption.
- The lower head wall is represented by 25 nodes from bottom to top, resulting in a node height of about 0.08 m for the AP1000® passive plant.
- Heavy metal layer is formed after the whole core has collapsed and the oxidic pool temperature exceeds 2,650 K.
- The emissivity of the metal layer is one of the key parameters that determine the metal layer temperature and the lateral heat transfer to the vessel wall from the metal layer. In this study, the emissivity of molten stainless steel of 0.43 is used.

AP1000® SBO



AP1000® SBO



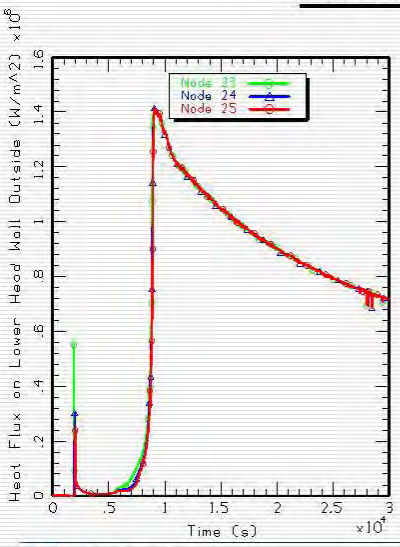


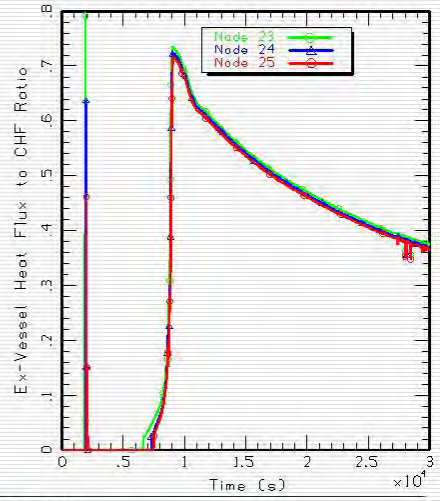
FAUSKE & ASSOCIATES, LLC

June 20-22, 2011

25

AP1000® SBO



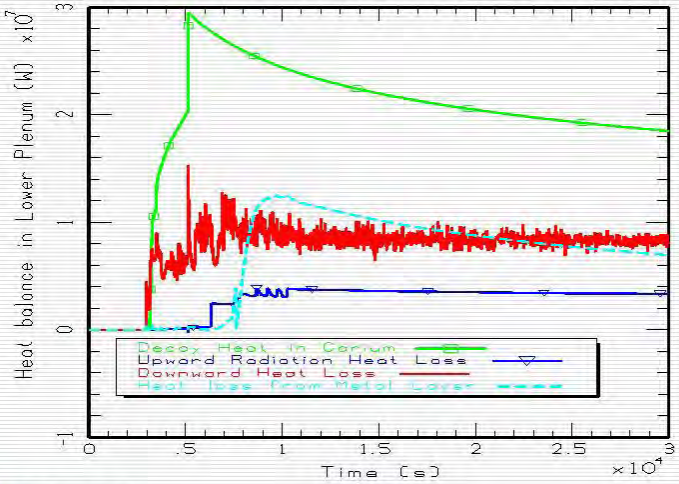


FAUSKE & ASSOCIATES, LLC

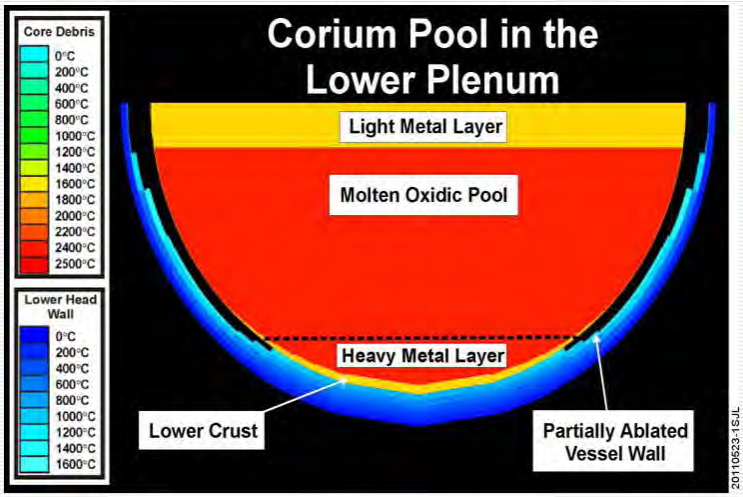
June 20-22, 2011

26

Heat balance in the corium pool in lower plenum



Temperatures of Corium Pool at 8.3 hrs



Conclusions

- MAAP5.01 is a capable tool for time-dependent, sequence-specific IVR evaluations.
- With a metal layer emissivity of 0.43 and with bounding estimate of the amount of steel that can participate in forming the heavy metal layer, the AP1000® vessel can stay intact when external vessel cooling is available.
- Because of detailed modeling of the lower head and the corium pool, MAAP5.01 is an improved tool for more realistic evaluation of RPV integrity and vessel failure timing if it is the case.

Development of Level 2 PSA Methodology for Sodium-Cooled Fast Reactors

- Overview of Evaluation Technology Development -

Tohru Suzuki [1], Ryodai Nakai [1], Kenji Kamiyama [1], Hiroshi Seino [1],

Kazuya Koyama [2] and Koji Morita [3]

[1] Japan Atomic Energy Agency, 4002 Narita-cho, O-arai, Ibaraki, 311-1393, Japan
suzuki.tohru54@jaea.go.jp

[2] Mitsubishi FBR Systems, Inc., 2-34-17, Jingumae, Shibuya-ku, Tokyo, 150-0001, Japan

[3] Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan

Abstract

A Probabilistic Safety Assessment (Level 2 PSA) is indispensable to the comprehensive safety assessment of Sodium-cooled Fast Reactors (SFRs). For this purpose, Japan Atomic Energy Agency (JAEA) consolidated the analytical methodologies and technical basis for all phases/sequences to be evaluated in the Level 2 PSA. In addition to the existing computational codes such as SAS4A, SIMMER-III, DEBNET, ARGO and APPLOHS, JAEA newly developed MUTRAN and SIMMER-LT codes in order to evaluate the long term behaviors of the material-relocation in the degraded core. These tools enabled the systematic assessment for the in-vessel accident sequences. For the ex-vessel accident sequences, JAEA also improved CONTAIN/LMR code taking into account the feature of SFRs and verified the analytical models in CONTAIN/LMR by utilizing the new experiments such as sodium-concrete reaction test. In addition, the technical basis for constructing phenomenological event trees was compiled, in which the dominant factors having significant effects on the event progression were corresponded to the related experiments and analytical results.

Keywords: Sodium-cooled Fast Reactors (SFRs), Core Disruptive Accident (CDA), Material-relocation phase, Ex-vessel accident sequence

1. Introduction

A Probabilistic Safety Assessment (Level 2 PSA) is indispensable to the comprehensive safety assessment of Sodium-cooled Fast Reactors (SFRs). For this purpose, the analytical methodologies for all phases/sequences to be evaluated in the Level 2 PSA should be established, and the technical basis for constructing the phenomenological event trees should also be developed.

The sequences to be evaluated in Level 2 PSA for SFRs are schematically shown in **Fig. 1**. With regard to the safety analyses of SFRs, computational tools such as SAS4A (Tentner 1985), SIMMER-III (Kondo 1992; Tobita 2006), DEBNET (Koyama 2009), ARGO (Horie 2006) and APPLOHS (Niwa 1991) have already been developed. These tools, however, are not sufficient for systematically assessing the whole sequence of Core Disruptive Accident (CDA) because the evaluation technologies for the material-relocation phase and the ex-vessel accident sequences are lacking. Concerning the technical basis, in addition, the dominant factors in all phases/sequences should be identified through parametric analyses, and the information obtained from these analyses and related past experiments should be compiled so as to quantify the branch probabilities in the phenomeno-logical event trees. Therefore, the following issues can be addressed in order to consolidate the methodology of Level 2 PSA for SFRs:

1) Development of evaluation technology for material-relocation phase
2) Development of evaluation technology for ex-vessel accident sequence

3) Development of technical basis to construct event trees

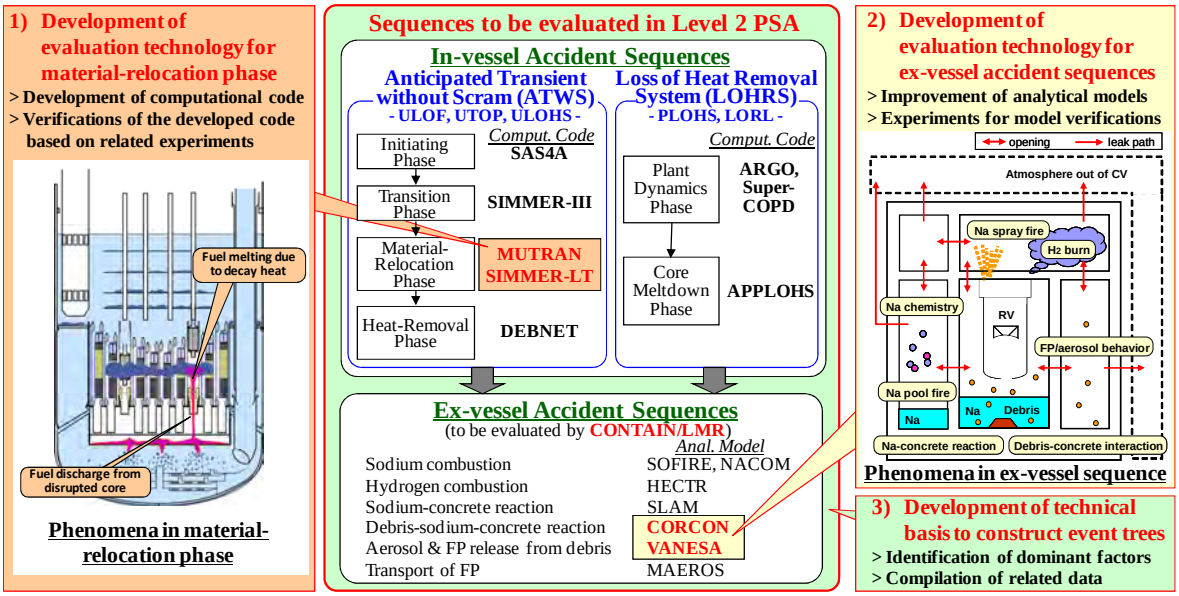


Fig. 1 Sequences to be evaluated in Level 2 PSA for SFRs.

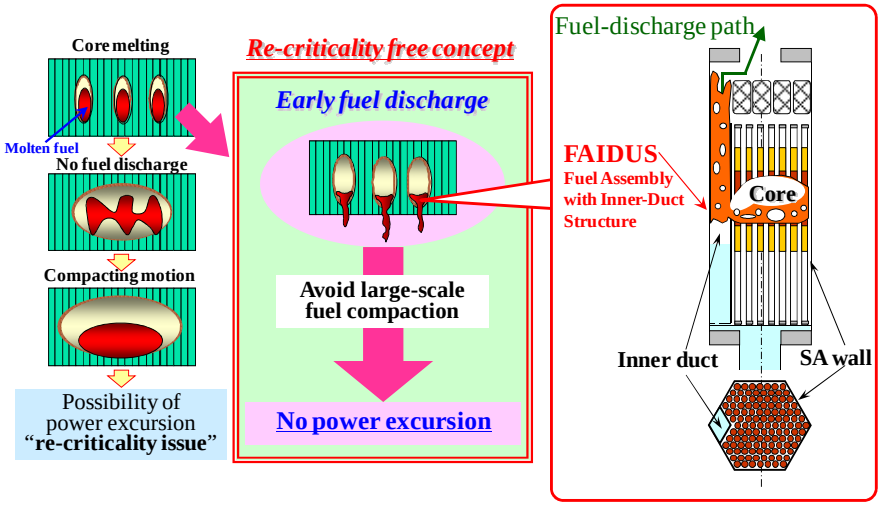


Fig. 2 Re-criticality free concept.

On the other hand, the safety evaluation of Japan Sodium-cooled Fast Reactor (JSFR) is required in the Fast Reactor Cycle Technology Development (FaCT) project (Sagayama 2007). In the design of JSFR, the Fuel Assembly with Inner-Duct Structure (FAIDUS) (Niwa 2003) based on the so-called re-criticality free concept is introduced in order to avoid large-scale molten-fuel compaction and severe power excursion in the disrupted core (see **Fig. 2**). The development of Level 2 PSA methodology is also very important from the view point of future licensing of JSFR.

In the present study, the development of the evaluation technology for the Level 2 PSA of SFRs with a focus on JSFR is described, scoping the computational tools MUTRAN and SIMMER-LT for the material-relocation phase and CONTAIN/LMR for the ex-vessel accident sequence. In addition, the compilation of the technical basis to be utilized in the Level 2 PSA of SFRs is overviewed. The particular development of the technical basis and the construction of event tree for ATWS (Anticipated Transient without Scram), LOHRS (Loss of Heat Removal System) and ex-vessel accident sequences are presented in the relevant papers (Sato 2010; Yamano 2010; Koyama 2010; Tobita 2010; Ohno 2010).

2. Evaluation technology for material-relocation phase

The event progression in Unprotected Loss of Flow (ULOF), which is a typical accident categorized into ATWS, is schematically shown in **Fig. 3**. This figure is illustrated for the JSFR adapting FAIDUS.

In the initiating phase (Fig. 3-(a)), fuel pin disruption caused by coolant boiling due to ULOF would result in axial fuel dispersion in the subassembly (SA). During the transition phase (Fig. 3-(b)), the inner duct structure of FAIDUS would breakup before the failure of the SA wall. The molten fuel would be discharged in the upward direction through the inner ducts with the driving force enhanced by fission-gas pressure. After the pressure reduction due to fission-gas escape with fuel discharge, the failure of the SA would result in the collapse of the upper core structure. Since the molten fuel has already been discharged, the materials remaining in the core region would consist of solid fuel and steel. Because of the low mobility of solid fuel in the core region, the subsequent events would progress gradually. In the material-relocation phase (Fig. 3-(c)), the control rod guide tube (CRGT) would breakup according to the gradual fuel melting due to decay power, and the fuel remaining in the core region would be discharged in the downward direction through CRGT. The molten fuel discharged through CRGT would be quenched and fragmented into fuel debris in the lower plenum region. The fuel debris would be accumulated on a multi-layer debris tray installed in the bottom region of reactor vessel. In the heat-removal phase (Fig. 3-(d)), the decay heat generated in the debris bed on the debris tray would be stably removed by the natural convection of sodium coolant in JSFR design.

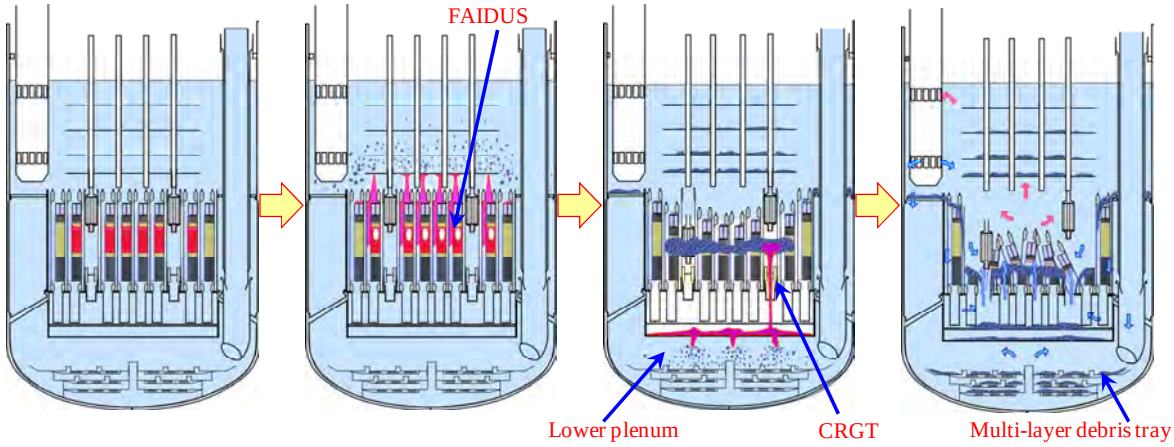


Fig. 3 Expected event progression of ULOF.

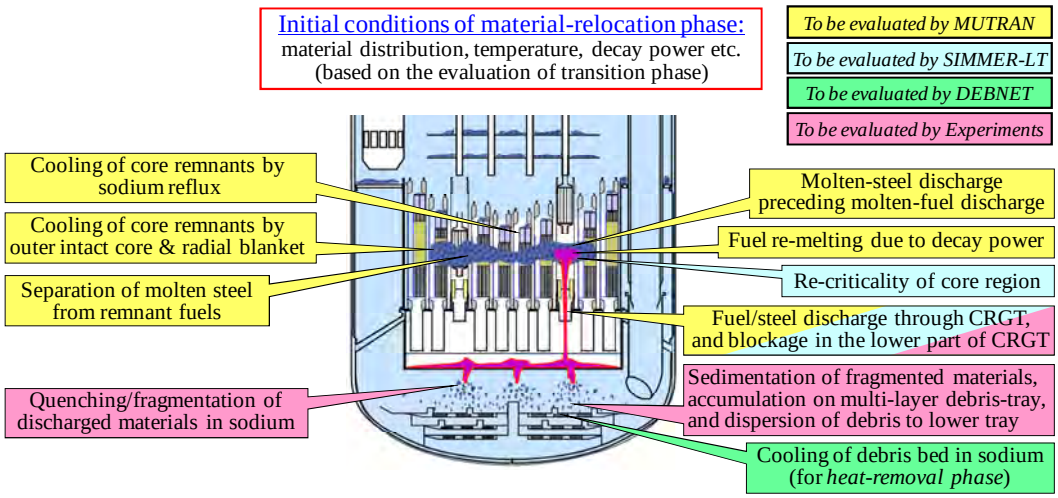


Fig. 4 Phenomena to be evaluated in material-relocation phase.

Among these phases, the material-relocation phase will consist of a long term event progression and complicated phenomena. The phenomena to be evaluated in this phase and the evaluation approach are schematically summarized in **Fig. 4**. In general, the initial condition of the material-relocation phase would be determined by the evaluation of the transition phase. In order to systematically investigate material-relocation behavior, the analytical tools MUTRAN and SIMMER-LT were newly developed and verified as described in the following sections.

2.1 Development and Verification of MUTRAN Code

MUTRAN has been developed in order to evaluate the long term behavior of the materials remaining in the core. The time range to be simulated by MUTRAN is from several hours to several dozen hours. Since the molten-fuel discharge during the transition phase would bring the core to a typical subcritical state, the heat source to be considered in MUTRAN would be the decay power generated by the core remnants. In analyses with MUTRAN, therefore, the heat source is given as input data based on the decay-heat curve, and neutronics calculations are not incorporated. The long term behavior in the material-relocation phase is basically governed by the heat transfer among the core materials and the heat removal to the core outside as shown in **Fig. 4**.

In the development of MUTRAN, the pilot code was extended so as to execute the whole core calculation, in which the inner/outer core, blanket and CRGT regions were adequately represented. In addition, several models were newly introduced in which the molten fuel discharge due to CRGT failure and the cooling of core remnants by sodium reflux could be appropriately reproduced. The verification of these models was also performed using the experimental data obtained in EAGLE project (Koyama 2010).

With the model developments and basic verifications, MUTRAN is now available for whole-core analysis. A sample result of the whole-core calculation is displayed in **Fig. 5**. In this calculation, the material relocation was simulated taking into account the decay power, cooling conditions, fuel re-melting, CRGT failure, and discharge through CRGT. The calculation result shows that the material distribution in the core region which depends on the material-discharge behavior and the blockage formation in CRGT can be reproduced. The material distribution simulated by MUTRAN will be connected to SIMMER-LT in the case of approaching re-criticality, as described in **2.3**.

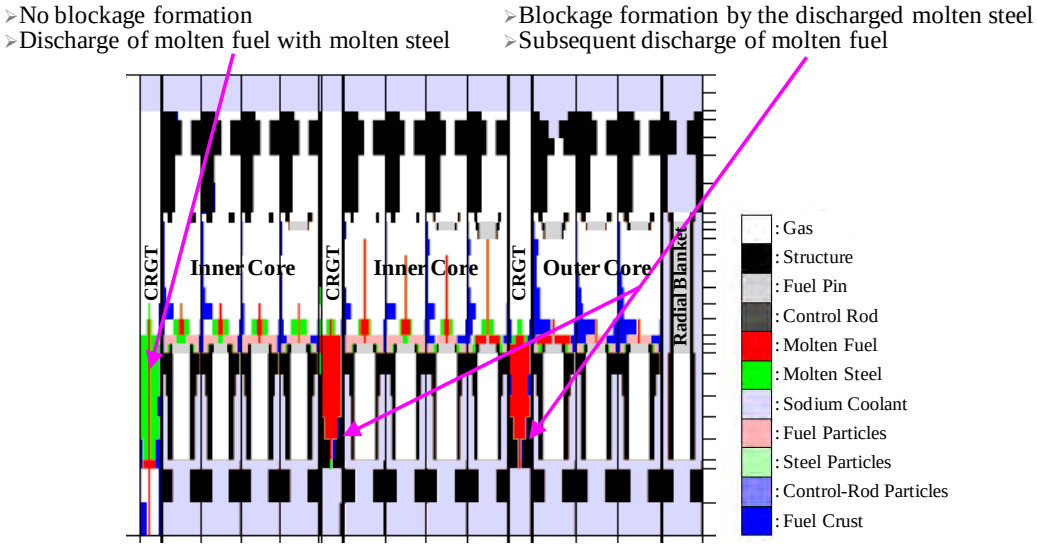


Fig. 5 Whole-core calculation by MUTRAN.

2.2 Development and Verification of SIMMER-LT Code

SIMMER-LT has been also developed to evaluate the material-relocation phase. The time range to be simulated by SIMMER-LT is from several minutes to several dozen minutes. Since SIMMER-LT was

based on the framework of SIMMER-III (Kondo 1992), neutronics calculations according to the material distribution in the core region can be performed. To apply SIMMER-LT to the material-relocation phase, however, computational efficiency should be enhanced for analyses of rather long-term transients.

To achieve overall speed-up of the calculations, code parallelization was implemented and tested first. As a result of this parallelization, an increase in speed by a factor of more than 6 was obtained with 32 processing elements. Next, a multi-time step integration algorithm was introduced to optimize the time-step size for fluid-dynamics calculations. We confirmed that this improvement could accelerate the code by a factor of about three (Nakai 2009). In addition, the original vaporization/condensation (V/C) model of SIMMER-III was simplified to reduce the computational load in heat and mass transfer calculations. In the simplified V/C model, energy transfers between vapor and liquid phases were represented by a departure from saturation conditions, and mass transfers associated with the energy transfers were modeled as an equilibrium process without representing phase changes at interfaces. This simplification is possible under the assumption that thermodynamically non-equilibrium states between vapor and liquid phases are mitigated within the order of a time-step size used for fluid-dynamics calculations. This simplification resulted in a twofold increase in speed in the V/C calculation portion. The verification of the simplified V/C model was performed through the comparison between SIMMER-LT and SIMMER-III with regard to the long-term sodium vaporization under the decay-power condition. The calculation result of SIMMER-LT using the equilibrium V/C model was consistent with that of SIMMER-III using non-equilibrium V/C model. The present results demonstrate that SIMMER-LT could be applied to long term transients of the material-relocation phase up with computing time within reasonable bounds.

2.3 Sample Calculation performed by MUTRAN and SIMMER-LT

In order to demonstrate the technology developed for the material-relocation phase, the whole reactivity transient according to the material distribution in the core region was evaluated. In this calculation, MUTRAN and SIMMER-LT were switched in the following procedures:

[1] simulate the long-term material relocation by MUTRAN
[2] evaluate the snapshot reactivity/power by static neutronics calculations, based on the material distribution simulated by MUTRAN
[3] switch the simulation from MUTRAN to SIMMER-LT before super-critical state
[4] evaluate the continuous reactivity/power transient by SIMMER-LT

The calculation result obtained from the procedure above is displayed in **Fig. 6**. This figure demonstrates that the systematic methodology for evaluating the whole sequence of the material-relocation phase has been sufficiently developed.

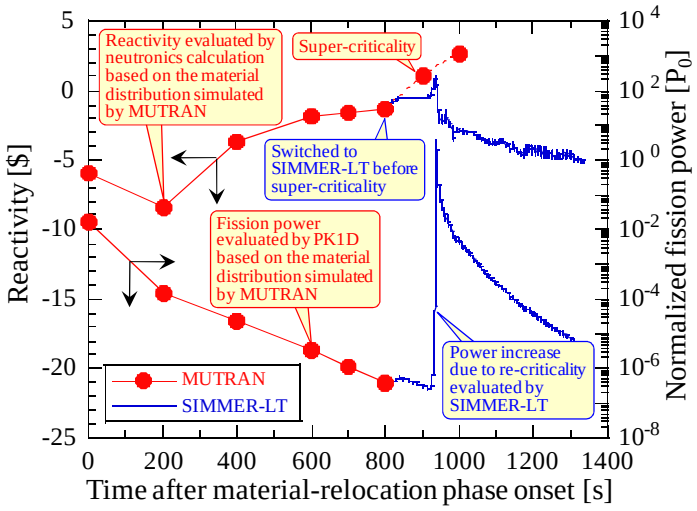


Fig. 6 Reactivity/power in material-relocation phase evaluated by MUTRAN and SIMMER-LT.

3. Evaluation technology for ex-vessel accident sequence

Assuming that CDA was not retained in the reactor vessel, the interaction among sodium, debris and concrete of the containment structure may cause the ablation of concrete, the generation of combustible gas, and the release of aerosols including fission products (FPs). Since the accident progression out of reactor vessel and the subsequent transfer behavior of radioactive materials are important issues to be estimated in Level 2 PSA, an evaluation technology for the ex-vessel accident sequence of SFRs should be developed.

For the evaluation of the ex-vessel accident sequence, the analytical models CORCON and VANESA, installed in CONTAIN/LMR, should be improved taking into account the features of SFRs because these models were originally developed for light water reactors. In these model improvements, the phenomena expressed in blue in **Fig. 7** have been investigated and the experiments expressed in red in the figure have been performed to clarify them. In parallel with the model improvements, their verification should also be done based on the newly performed experiments (Nakai 2009). In the present paper, the experimental results of a sodium-concrete reaction test are summarized and a verification of CONTAIN/LMR based on this test will be described.

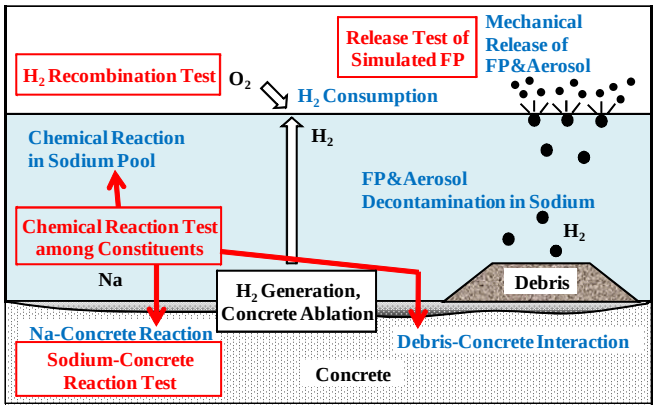


Fig. 7 Experiments to clarify the phenomena in ex-vessel accident sequence.

3.1 Sodium-Concrete Reaction Test

In order to clarify the effect of high-temperature debris on the sodium-concrete reaction including concrete erosion and hydrogen generation, a series of experimental tests as shown in **Fig. 8** was performed, in which the heater power representing high-temperature debris was parametrically changed in the sodium pool. In the experiments, the molten sodium heated in the sodium-supply tank (0.4 kg and 600 ^{o}C) was poured onto the concrete test piece installed in the test apparatus. During the pouring of molten sodium, the heater power was adjusted so as to keep the sodium pool at the prescribed temperature (600 - 800 ^{o}C). Under these experimental conditions, the temperature transients in the sodium pool, the erosion of concrete and the generation of hydrogen were measured as the experimental values. During the measurements, argon gas was supplied (250*l*/min) into the cover gas region of the apparatus so as to avoid the accumulation of generated hydrogen there. The erosion status was observed by retrieving the concrete test pieces after the experiments and reaction products were sampled for analyses.

The typical results of concrete erosion are displayed in **Fig. 9**, where the sodium-pool temperatures were kept at 600 ^{o}C and 800 ^{o}C by adjusting the heater power as the experimental parameter. The main observations obtained from these pictures are summarized below:

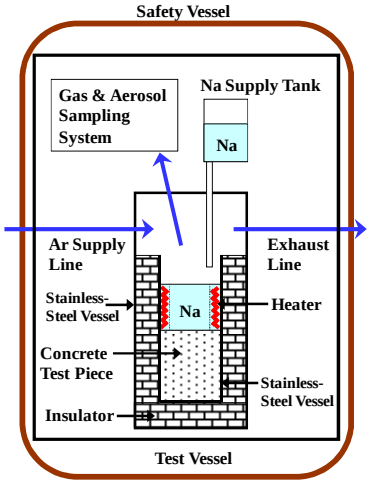
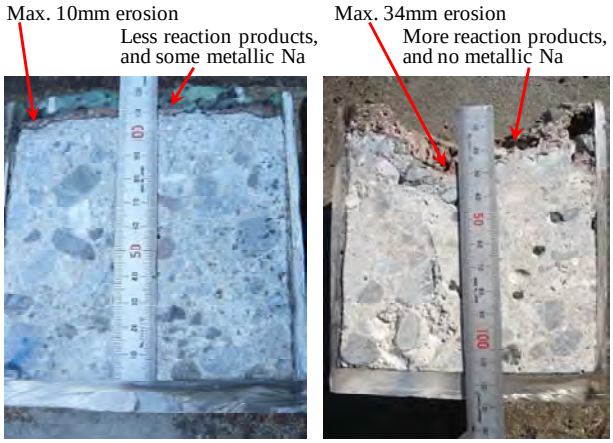


Fig. 8 Sodium-concrete reaction test.



(i) Na Temperature: about 600 °C (ii) Na Temperature: about 800 °C

Fig. 9 Concrete pieces observed after sodium-concrete reaction test.

a) The concrete erosion and hydrogen generation due to sodium-concrete reaction would be enhanced with the increase of sodium-pool temperature i.e. the increase of heater power.
b) The sodium-concrete reaction at a sodium-pool temperature of 800 °C would be terminated due to the dissipation of sodium. The reaction at 600 °C, on the other hand, would be terminated due to other reasons as described in the following section. These observations were obtained from an investigation of the amount of sodium remaining in the test section after the experiments.

3.2 Verification of CONTAIN/LMR based on Sodium-Concrete Reaction Test

Based on the chemical reaction test among constitutions as shown in **Fig. 7**, the following reactions related to CORCON and VANESA were newly introduced into CONTAIN/LMR:

$$4Na+3SiO_2 \rightarrow 2Na_2SiO_3+Si \quad (1)$$
$$3Na+2Al_2O_3 \rightarrow 3NaAlO_2+Al \quad (2)$$
$$2NaOH+ Al_2O_3 \rightarrow 2\ NaAlO_2+H_2O \quad (3)$$

In order to verify the improvement above, especially focusing on Eq. (1), experimental analyses of the sodium-concrete (siliceous concrete) reaction test described in the previous section were performed. In the present analyses, two types of test were simulated, in which the sodium-pool temperatures were kept at 600 °C and 800 °C. The calculation results for the case of 600 °C are displayed in **Fig. 10**. The main remarks obtained from these analyses are as follows:

A) The transient of sodium-pool temperature obtained in the experiment could be appropriately reproduced by CONTAIN/LMR through the improvement above.
B) The overall trend of the hydrogen-generation rate could be qualitatively represented by CONTAIN/LMR. The generation rate, however, would be overestimated in the beginning stage, and be underestimated in the late stage. The overestimation in the beginning stage might be caused by overestimating the excretion of free water from concrete, and the underestimation in the late stage might be caused by excluding the accumulation effect of chemical products in the model.
C) By comparing the two simulation results for sodium-pool temperatures of 600 and 800 °C, the general trend observed in the experiments could be reproduced where the sodium-concrete reaction would be enhanced with the increase of sodium-pool temperature. In addition, the simulation results for 600 °C suggested that the sodium-concrete reaction would be terminated due to the reduction of water contributing to the reaction.

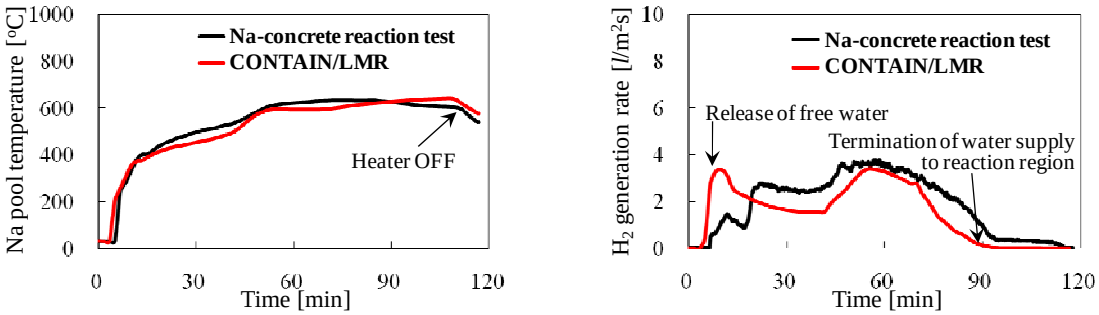


Fig. 10Verification of developed models in CONTAIN/LMR (600 °C of sodium pool).

As described above, the model improvements for CORCON and VANESA in CONTAIN/LMR made it possible to suitably represent the experimental results of the sodium-concrete reaction test. In particular, it was confirmed that the phenomena important for Level 2 PSA of SFRs, such as the characteristics of sodium-concrete reaction and hydrogen generation, could be appropriately represented. Through the present study, the chemical-reaction models introduced into CONTAIN/LMR were verified, and their applicability to the ex-vessel accident sequence in SFRs was also confirmed.

4. Technical basis for Level 2 PSA

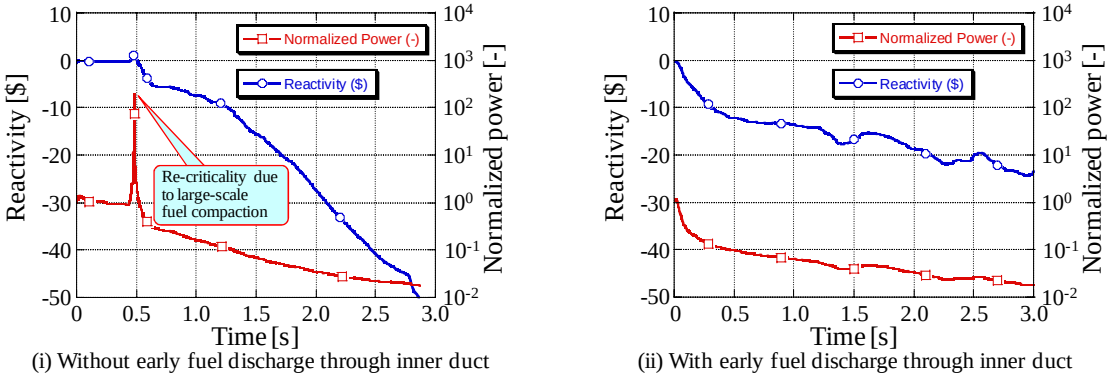
In order to build up the technical basis for Level 2 PSA, the dominant factors, which have significant effects on the event progression, should be identified for all phases/sequences. In the identification of the dominant factors, a series of sensitivity analyses was executed by utilizing the corresponding computational tools displayed in **Fig. 1**. The dominant factors identified through the sensitivity analyses should be reflected on the setting of branch headings in phenomenological event trees. For the evaluation of event progression and branch probabilities, related analytical result and experimental data should be compiled as the technical data basis corresponding to the dominant factors.

4.1 Identification of Dominant Factors

In the identification of dominant factors, a series of sensitivity analyses using the adequate computational tools should be executed for all of the phases/sequences to be investigated in Level 2 PSA. As examples of these sensitivity analyses, the early fuel discharge through the inner duct during the transition phase (Yamano 2010) and the debris-bed cooling in the containment vessel during the ex-vessel accident sequence (Ohno 2010) are briefly presented here.

The sensitivity analyses for the transition phase were executed by SIMMER-III code. The effect of FAIDUS on the reactivity transient is displayed in **Fig. 11**, where the early fuel discharge through the inner duct as shown in **Fig. 2** was artificially suppressed in the calculation (i) and not suppressed in (ii). Since the early fuel discharge could affect the possibility of re-criticality as shown in **Fig. 11**, it would be set as a branch heading of event tree. The dominant factors composing the early fuel discharge should be associated with the analytical result and experimental data as described in **4.2**.

The sensitivity analyses for the ex-vessel accident sequences were also performed by using a debris-bed cooling calculation model in CONTAIN/LMR. The effects of dominant factors on debris-bed cooling in the containment vessel are displayed in **Fig. 12**, where the sensitivity of particle diameter, porosity, debris-bed height, and contact angle were investigated against the dryout heat flux. As shown in **Fig. 12**, the particle diameter and porosity would have significant effects on the debris-bed cooling.



(i) Without early fuel discharge through inner duct (ii) With early fuel discharge through inner duct

Fig. 11 Sensitivity analysis for early fuel discharge in transition phase.

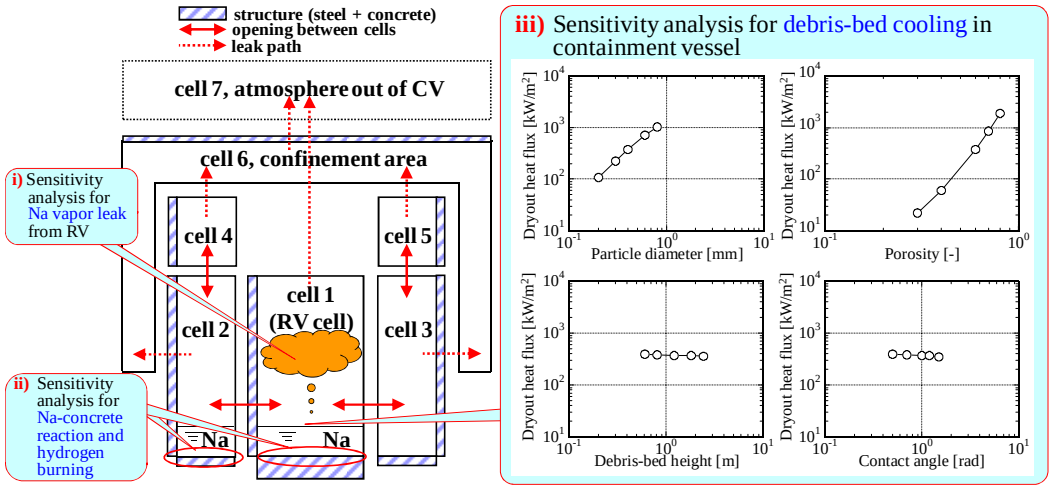


Fig. 12 Sensitivity analyses for ex-vessel accident sequences.

4.2 Construction of Phenomenological Event Trees and Compilation of Related Data

After the identification of dominant factors based on the sensitivity analyses for all of the phases/sequences to be evaluated in Level 2 PSA, a series of phenomenological event trees was constructed in which the identified dominant factors should be reflected on branch headings. As an example, the phenomenological event tree for the transition phase is displayed in **Fig. 13**. In addition to the early fuel discharge through the inner duct, the neutronic termination and reactivity insertions were also put as the branch headings based on the identification of dominant factors.

The technical information on the related phenomena, analytical results, and experimental data were then collected and compiled as the technical data basis in order to evaluate the event progression and branch probability within the phenomenological event trees. Such information can be associated with the branch headings. As shown in **Fig. 13**, "Inner-duct failure timing" evaluated by using the EAGLE experiments (Konishi 2006; Konishi 2007) and "Driving force for fuel discharge" based on the CABRI (Nonaka 1992) and TREAT experiments (Bauer 1986) would be corresponded to the dominant factors in the technical basis. The adequacy of the present approach and the sufficiency of the developed methodology have already been reviewed among Japanese CDA experts including university professors.

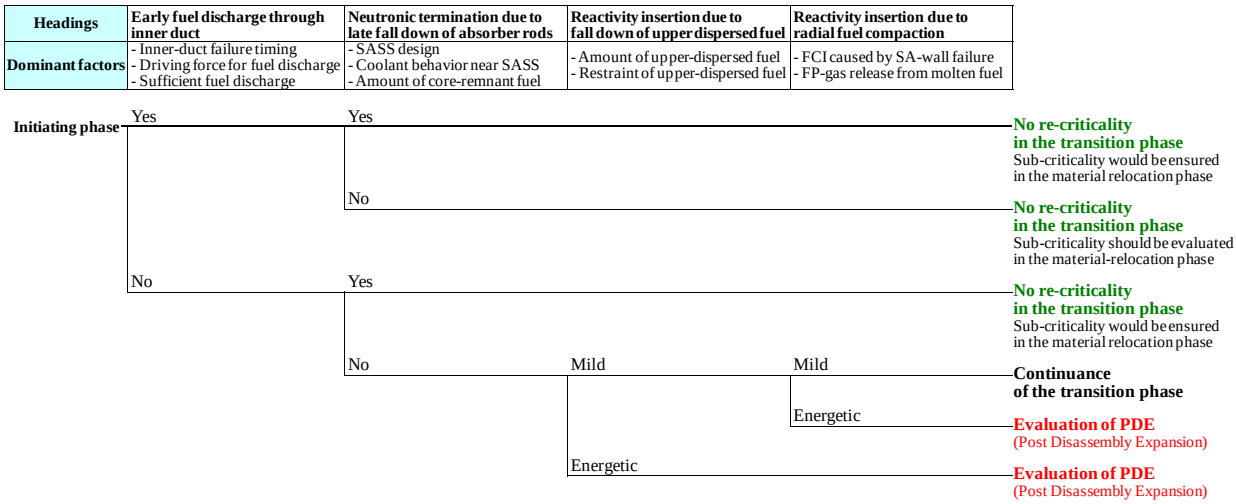


Fig. 13 Construction of phenomenological event tree for transition phase.

5. Conclusions

The evaluation-technology development of Level 2 PSA for SFRs was overviewed. In order to systematically assess the phases/sequences to be evaluated in Level 2 PSA, computational tools for the material-relocation phase and the ex-vessel accident sequence were developed and verified. In addition, the technical basis for constructing phenomenological event trees was consolidated, in which the information on the related analyses/experiments were compiled so as to determine the event progression and branch probabilities within the event trees. The conclusions of the paper are summarized as follows:

1) The computational tools, MUTRAN and SIMMER-LT, were developed. These tools enabled systematic simulations of the material-relocation phase.
2) The analytical models, CORCON and VANESA, were improved based on newly performed experiments. The CONTAIN/LMR code with the improved models enabled appropriate simulations of the ex-vessel accident sequence taking into account the feature of SFRs.
3) The information to be efficiently utilized in the construction of event trees was compiled as a technical data basis, in which the dominant factors having significant effects on the event progression were corresponded to the related analytical/experimental results.

The particular development of the technical basis and the details of event-tree constructions for ATWS, LOHRS and ex-vessel accident sequences are presented in the relevant papers (Sato 2010; Yamano 2010; Koyama 2010; Tobita 2010; Ohno 2010). By assembling the technical data provided in these papers, the general information needed in Level 2 PSA for SFRs can be completed.

6. References

Bauer, T. H., et al., (1986), Post-Failure Material Movement in the PFR/TREAT Experiments, *Proc. Int. Mtg. on Fast Reactor Safety and Related Physics*, p.1647, Guernsey, UK.

Horie, H., et al., (2006), Sensitivity and Uncertainty Analysis of ARGO-3 Code on the ULOF Event of 4S Reactor, *Proc. ICAPP'06*, Reno, USA.

Kondo, Sa., et al., (1992), SIMMER-III: An Advanced Computer Program for LMFBR Severe Accident Analysis, *Proc. ANP'92*, Vol. IV, p. 40.5-1, Tokyo, Japan.

Konishi, K., et al., (2006), The Eagle Project to eliminate the Recriticality Issue of Fast Reactors –Progress and Results of In-Pile Tests, *Proc. NTHAS5-F001*, Nov. 26-29, Jeju, Korea.

Konishi, K., et al., (2007), The Results of a wall failure in-pile experiment under the EAGLE project, *Nuclear Engineering and Design*, **237**, pp. 2165 – 2174.

Koyama, K., et al., (2009), Development of Severe Accident Evaluation Technology (Level 2 PSA) for Sodium-cooled Fast Reactors (4) Identification of Dominant Factors in Core Material Relocation and Heat Removal Phases, *Proc. ICAPP'09*, Tokyo, Japan.

Koyama, K., et al., (2010), Development of Level 2 PSA Methodology for Sodium-Cooled Fast Reactors (4) Development of Technical Basis in the Material-Relocation and Decay-Heat Removal Phases of Unprotected Events, *Proc. NUTHOS-8*, Shanghai, China.

Nakai, R., et al., (2009), Development of Severe Accident Evaluation Technology (Level 2 PSA) for Sodium-cooled Fast Reactors (1) Overview of Evaluation Methodology Development, *Proc. ICAPP'09*, Tokyo, Japan.

Niwa, H., (1991), A Study on the In-Vessel Processes of LOHRS Type Accidents, PNC TN9410 91-304.

Niwa, H., et al., (2003), LMFBR Design and its Evolution: (3) Safety System Design of LMFBR, *Proc. GNES4/ANP2003*, No. 1154, Kyoto, Japan.

Nonaka, N., et al., (1992), Improvement of Evaluation Method for Initiating-Phase Energetics Based on CABRI-1 In-Pile Experiments, *Nuclear Technology*, **98**, p.54.

Sagayama, Y., et al., (2007), Launch of Fast Reactor Cycle Technology Development Project in Japan, *Proc. Global 2007*, Boise, Idaho, USA.

Sato, I., et al., (2010), Development of Level 2 PSA Methodology for Sodium-Cooled Fast Reactors (2) Development of Technical Basis in the Initiating Phase of Unprotected Events," *Proc. NUTHOS-8*, Shanghai, China.

Tentner, A. M., et al., (1985), The SAS4A LMFBR Whole Core Accident Analysis Code, *Proc. Int. Mtg. Fast Reactor Safety*, Vol. 2, pp. 989-998, Knoxville, USA.

Tobita, Y., et al., (2006), The Development of SIMMER-III, an Advanced Computer Program for LMFR Safety Analysis and Its Application to Sodium Experiments, *Nuclear Technology*, **153**, 3, pp. 245-255.

Tobita, Y., et al., (2010), Development of Level 2 PSA Methodology for Sodium-Cooled Fast Reactors (5) Development of Technical Basis for the Protected Loss of Heat Sink, *Proc. NUTHOS-8*, Shanghai, China.

Ohno, S., et al., (2010), Development of Level 2 PSA Methodology for Sodium-Cooled Fast Reactors (6) Development of Technical Basis in Ex-vessel Accident Sequences, *Proc. NUTHOS-8*, Shanghai, China.

Yamano, H., et al., (2010), Development of Level 2 PSA Methodology for Sodium-Cooled Fast Reactors (3) Development of Technical Basis in the Transition Phase of Unprotected Events, *Proc. NUTHOS-8*, Shanghai, China.

Development of Level 2 PSA Methodology for Sodium-Cooled Fast Reactors
- Overview of Evaluation Technology Development -

T. Suzuki, R. Nakai, K. Kamiyama, H. Seino
Japan Atomic Energy Agency
K. Koyama
Mitsubishi FBR Systems, Inc.
K. Morita
Kyushu University

OECD/NEA Workshop on PSA for New and Advanced Reactors, June 20-22, 2011

Contents

OECD/NEA Workshop on PSA for New and Advanced Reactors, June 20-22, 2011

Fast Reactor Cycle Technology Development Project

1. Introduction
Backgrounds

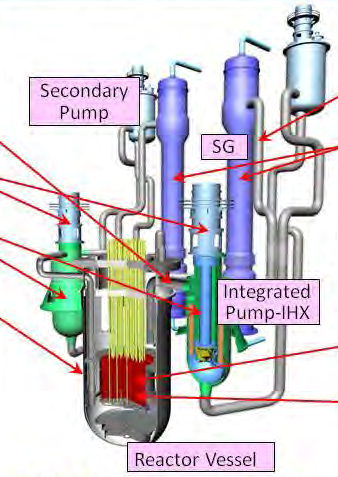
Economic Competitiveness

Reduction of Mass & Volume

1) Shortened piping with high chromium steel
2) Two-loop cooling system
3) Integrated pump-IHX component
4) Compact reactor vessel
5) Simplified fuel handling system
6) CV with steel plate reinforced concrete building

Long Operation by High Burn-up Fuel

7) Advanced fuel material



1500 MWe Large Scale SFR

Higher Reliability

Sodium Technology

1) Sodium leak tightness with double wall piping
2) Higher reliable SG with double wall tube
3) Higher maintenance ability inside of sodium boundary

Higher Safety

Core Safety

1) Passive shutdown and decay heat removal
2) Re-criticality free core

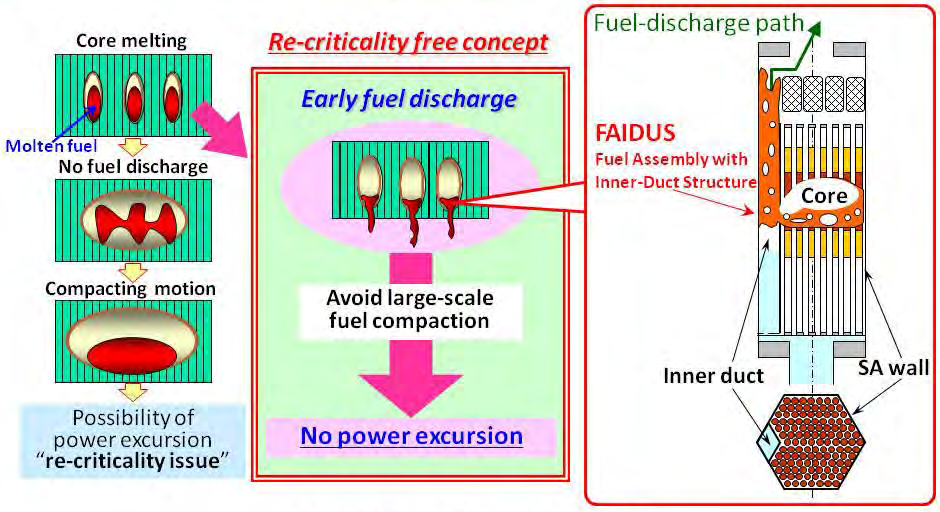
Seismic Reliability

3) Seismic reliability in core assemblies

Innovative technologies incorporated in JSFR

Fast Reactor Cycle Technology Development Project

1. Introduction
Backgrounds



Concept of re-criticality free core

Fast Reactor Cycle Technology Development Project

1. Introduction
Objectives

- Re-criticality free and In-Vessel Retention (IVR) against Core Disruptive Accidents (CDAs);
  - Feasibility of sub-criticality & achievement of IVR based on the innovative technologies
- Probabilistic Safety Assessment (Level 2 PSA);
  - Complementary approach to the deterministic safety assessment
  - Consideration of the uncertainties in event progression
  - Assessment of the sequences leading to a large release of radioactive materials from containment
- Insufficiency of evaluation technology for systematic assessments;
  - Undeveloped methodology for material-relocation phase
  - Feature of sodium-cooled fast reactors (SFRs) in ex-vessel accident sequence
  - Compilation of related information for constructing phenomenological event trees

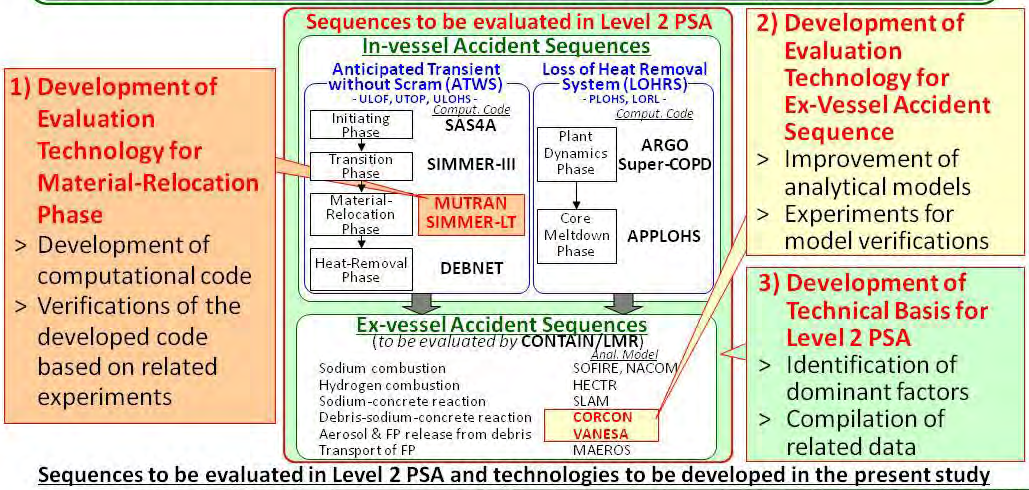
Objectives of the present study:

To develop the evaluation technologies & technical basis in order to perform Level 2 PSA for Sodium-cooled Fast Reactors (SFRs)

Fast Reactor Cycle Technology Development Project

1. Introduction
Objectives

To develop the evaluation technologies & technical basis in order to perform Level 2 PSA for Sodium-cooled Fast Reactors (SFRs)



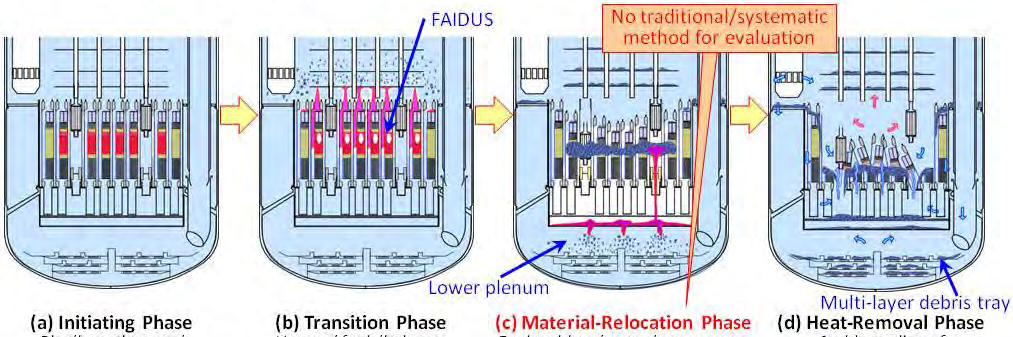
Sequences to be evaluated in Level 2 PSA and technologies to be developed in the present study

Fast Reactor Cycle Technology Development Project

2. Evaluation Technology for Material-Relocation Phase

1) Development and verification of MUTRAN code
- Long-term (– several dozen hours) & overall behavior *without* neutronics

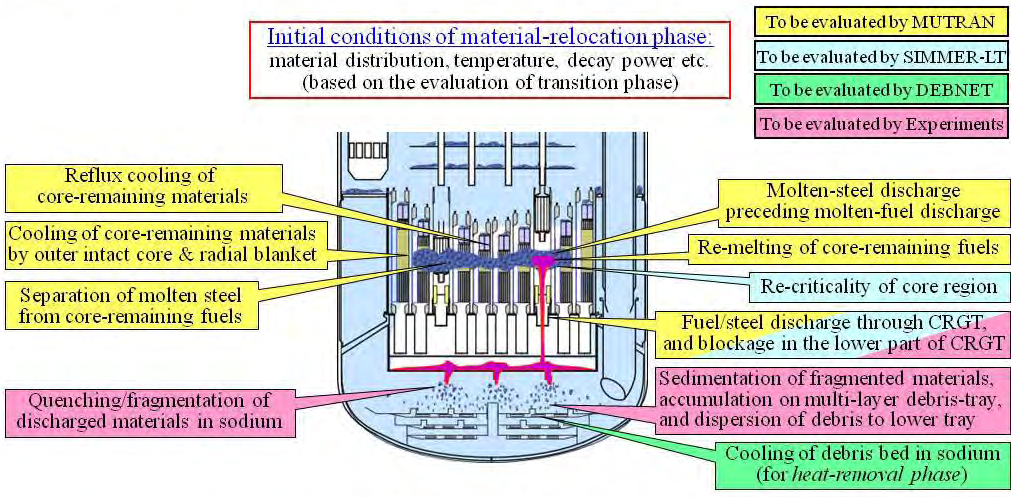
2) Development and verification of SIMMER-LT code
- Comparatively long-term (– several dozen minutes) behavior *with* neutronics



Expected event progression of ULOF

Fast Reactor Cycle Technology Development Project

2. Evaluation Technology for Material-Relocation Phase



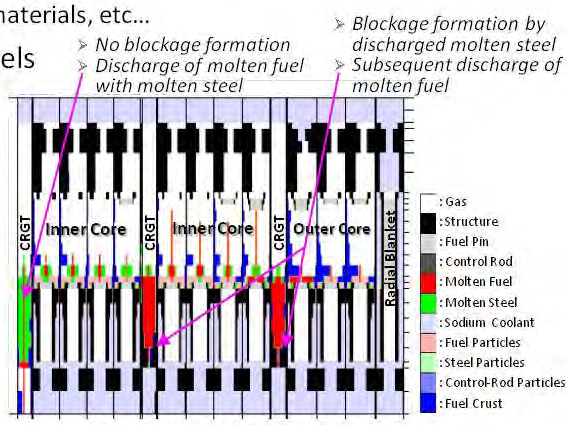
Phenomena to be evaluated in material-relocation phase

Fast Reactor Cycle Technology Development Project

2. Evaluation Technology for Material-Relocation Phase

Development and verification of MUTRAN code

- Code extension and new models
  - Modeling of inner/outer core, blanket, and control-rod guide tube (CRGT)
  - Molten fuel discharge due to CRGT failure
  - Reflux cooling of core-remaining materials, etc…
- Verification of introduced models
  - Experimental analysis based on EAGLE experiments etc.
    #) To be presented in relevant paper
- Whole-core calculation
  - Overall material-relocation can be demonstrated considering heat generation (decay power), cooling condition, fuel re-melting, CRGT failure and fuel discharge.
    #) See right figure



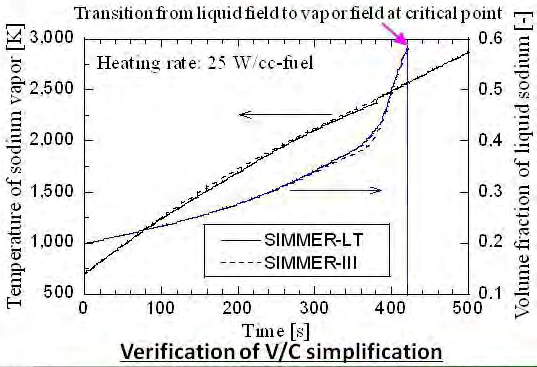
Whole-core calculation by MUTRAN

Fast Reactor Cycle Technology Development Project

2. Evaluation Technology for Material-Relocation Phase

Development and verification of SIMMER-LT code

- Code development based on SIMMER-III framework with neutronics
- Key issues in code development to reduce computational loads
  - Speed-up by code parallelization → *factor of 6 with 32 processing elements*
  - Optimization of time-step size in fluid-dynamics portion → *factor of 3*
  - Simplification of vaporization/condensation (V/C) model → *factor of 2*
- Verification of V/C simplification
  - Comparison between SIMMER-LT & SIMMER-III for long-term sodium vaporization under decay power condition
  - SIMMER-LT using equilibrium V/C was consistent with SIMMER-III using non-equilibrium V/C model
    #) See right figure
- Applicability to long-term cal.
  - Computing within reasonable time



Verification of V/C simplification

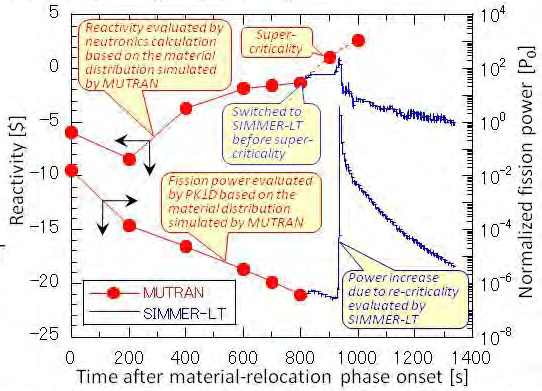
Fast Reactor Cycle Technology Development Project

2. Evaluation Technology for Material-Relocation Phase

Demonstration by MUTRAN and SIMMER-LT

- Demonstration of developed technology for material-relocation phase
  - Connection from MUTRAN to SIMMER-LT
  - Whole transient of reactivity according to the material distribution
  - Systematic evaluation of whole sequence including re-criticality
- Combination of the codes
  1) Calculate the long-term material relocation by MUTRAN
  2) Evaluate the snapshot reactivity/ power by static neutronics cals., based on the material distribution simulated by MUTRAN
  3) Switch from MUTRAN to SIMMER-LT before super-critical state
  4) Evaluate the continuous reactivity/ power transient by SIMMER-LT

  #) See right figure

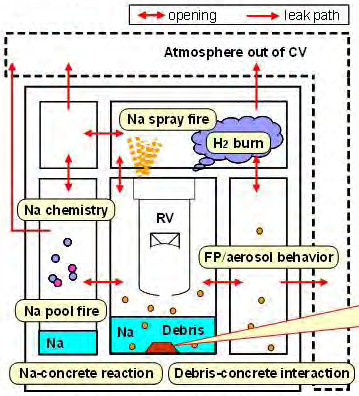


Reactivity/power transient in material-relocation phase

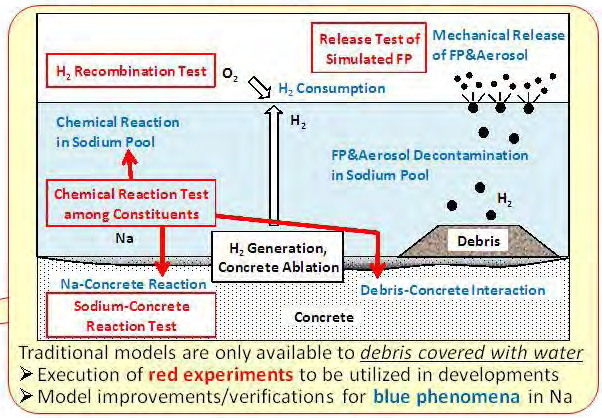
Fast Reactor Cycle Technology Development Project

3. Evaluation Technology for Ex-Vessel Accident Sequence

1) New experiments for model improvement and verification
   - Clarification of phenomena in ex-vessel sequence for SFRs
2) Model improvement and verification in CONTAIN/LMR code
   - Application of CORCON & VANESA to SFR-condition utilizing the new experiments



Phenomena in ex-vessel sequence



Traditional models are only available to *debris covered with water*

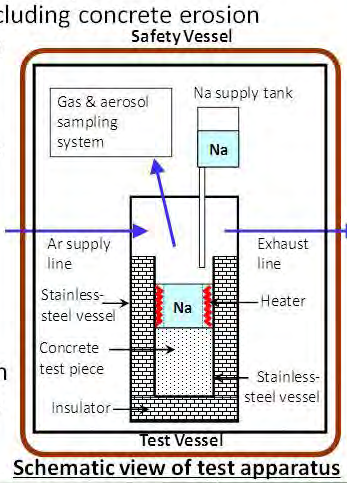
- Execution of **red experiments** to be utilized in developments
- Model improvements/verifications for **blue phenomena** in Na

Fast Reactor Cycle Technology Development Project

3. Evaluation Technology for Ex-Vessel Accident Sequence

New experiments for model improvement and verification

- Sodium-Concrete Reaction Test
  - To clarify the effect of high-temperature debris on Na-concrete reactions including concrete erosion and hydrogen generation
  - Molten sodium poured onto concrete test piece
  - Experimental parameter:
    - Na pool temperature
  - Measured values:
    - transient of Na-pool temperature
    - concrete erosion
    - hydrogen generation
  - Sodium-concrete reaction activated by the increase of Na-pool temperature



Schematic view of test apparatus

(i) Na Temperature: about **600 °C**

(ii) Na Temperature: about **800 °C**

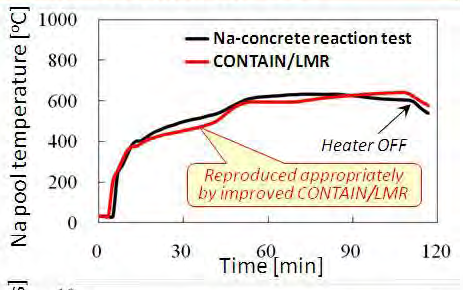
Fast Reactor Cycle Technology Development Project

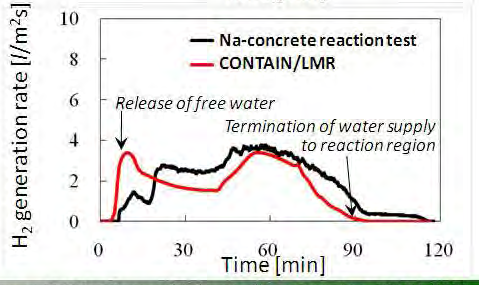
3. Evaluation Technology for Ex-Vessel Accident Sequence

Model improvement and verification in CONTAIN/LMR code

- Analysis of Sodium-Concrete Reaction Test by CONTAIN/LMR with improved models
  - Important phenomena for Level 2 PSA of SFRs can be appropriately represented:
    - characteristics of Na-concrete reaction
    - hydrogen generation etc...
  - Chemical reaction models were verified.
  - Applicability to the ex-vessel sequence of SFRs was confirmed.

  #) See right figure



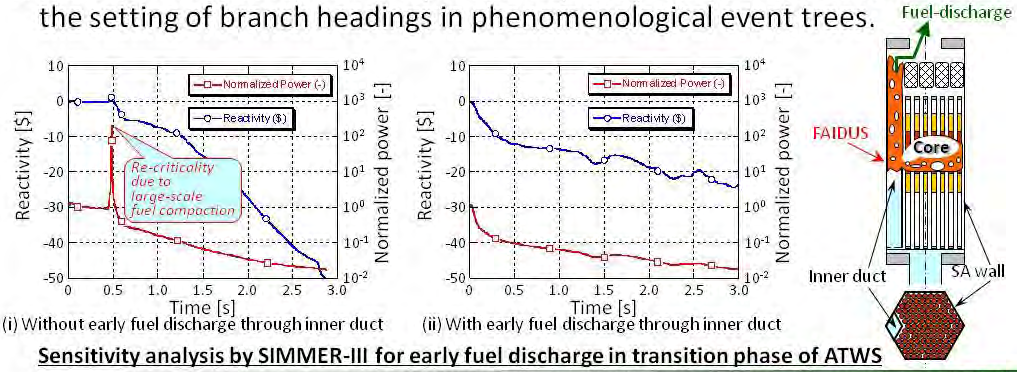


Fast Reactor Cycle Technology Development Project

4. Technical Basis for Level 2 PSA

Identification of dominant factors

- Identification of dominant factors in all phases/sequences by various sensitivity analyses:
  - ATWS: SAS4A, SIMMER-III, MUTRAN & SIMMER-LT, and DEBNET
  - LOHRS: ARGO, Super-COPD, and APPLOHS
  - Ex-vessel accident sequence: CONTAIN/LMR
- Dominant factors identified by sensitivity analyses would be reflected on the setting of branch headings in phenomenological event trees.



Sensitivity analysis by SIMMER-III for early fuel discharge in transition phase of ATWS

Fast Reactor Cycle Technology Development Project

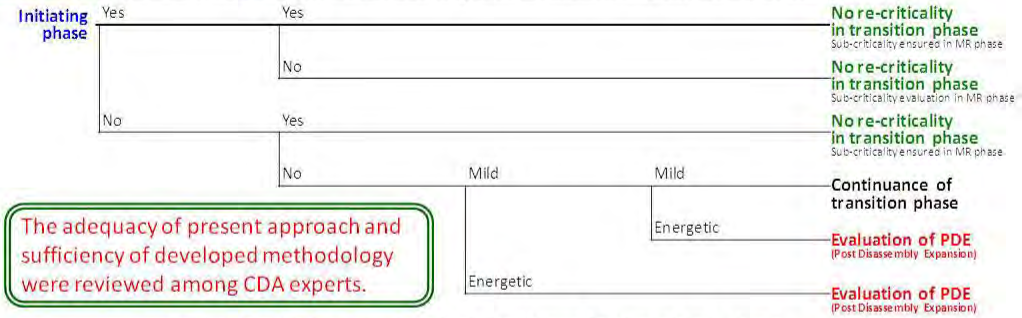
4. Technical Basis for Level 2 PSA

Compilation of related data to construct phenomenological event trees

Identified by a series of sensitivity analyses

Corresponded to related analytical/experimental data in the compiled database:
- Inner-duct failure timing → Evaluation based on EAGLE experiments
- Driving force for discharge → Demonstrated by CABRI & TREAT experiments

Headings	Early fuel discharge through inner duct	Neutronic termination due to late falling down of absorber rods	Reactivity insertion due to falling down of upper dispersed fuel	Reactivity insertion due to radial fuel compaction
Factors	- Inner-duct failure timing - Driving force for discharge	- Coolant behavior near SASS - Amount of core-remnant fuel	- Amount of dispersed fuel - Restraint of dispersed fuel	- FCI caused by SA failure - FP-gas from molten fuel



The adequacy of present approach and sufficiency of developed methodology were reviewed among CDA experts.

A sample of phenomenological event tree for transition phase

Fast Reactor Cycle Technology Development Project

5. Conclusions

- The evaluation-technology development of Level 2 PSA for SFRs was overviewed:
  1) MUTRAN and SIMMER-LT were developed. These tools enabled systematic simulations of the material-relocation phase.
  2) CORCON and VANESA were improved based on new experiments. These models enabled CONTAIN/LMR to simulate ex-vessel accident sequence considering the feature of SFRs.
  3) Technical basis for constructing event trees was compiled, in which the dominant factors for event progressions were identified and the related analytical/experimental data were corresponded.

The particular developments of technical basis and the details of event-tree construction are discussed in the relevant publications.

6. Relevant Papers

- Relevant publications:
  - *Overview of Evaluation Technology (present)*
  - *Technical Basis in Initiating Phase (NUTHOS-8, Shanghai)*
  - *Technical Basis in Transition Phase (ditto)*
  - *Technical Basis in Material-Relocation/Heat-Removal Phases*
  - *Technical Basis for Protected Loss of Heat Sink (ditto)* → *LOHRS*
  - *Technical Basis for Ex-Vessel Accident Sequence (ditto)* → *Ex-Vessel*

ATWS and *LOHRS* → *In-Vessel*; *In-Vessel* and *Ex-Vessel* → *Level 2 PSA*

- By assembling the technical data provided in these papers, the general information needed in Level 2 PSA for SFRs can be completed.

PSA Level 2 as Element of an Integral Safety Assessment before Plant Commissioning

Horst Löffler, Dr. Oliver Mildenberger, Dr. Martin Sonnenkalb, Dr. Thomas Steinrötter

GRS mbH, Schwertnergasse 1, 50667 Köln, Germany - Horst.Loeffler@grs.de

Abstract

In Argentina the Central Nuclear Atucha II is near to completion. This is a pressurized heavy water reactor (PHWR with many similarities to typical German PWRs. Although it is not a recent design, it has some partly uncommon features, so that there is a certain resemblance to performing a PSA for a new design. In addition, Argentinean rules require a PSA level 3 before commissioning, and frequency limits for accident consequences in terms of doses to the public are imposed. This is an advanced PSA requirement and constitutes a significant challenge.

PSA level 1, level 2 and level 3 have to be performed in order to show compliance with the Argentinean dose limit. Such studies have been done first by the former KWU in the 1980s to get the construction license (FABIAN 1985). Nowadays the plant owner NA-SA performs PSA level 1 and provides information about the core damage states to GRS, who does the subsequent PSA level 2 part. GRS delivers source terms to the environment and the associated frequencies to the Argentinean research institute CNEA, which performs level 3 together with NA-SA. Since GRS is situated in the middle of the chain, interface definition with both ends has been a significant task of the GRS activities. Experience gained during this process will be highlighted in the presentation.

The analysis of PSA level 2 proper follows a traditional approach:

- *Deterministic accident simulation with integral code MELCOR*
- *Analyses of specific issues which are not covered by MELCOR*
- *Probabilistic accident progression analysis with EVNTRE event tree methodology.*

Methodology and results of PSA level 2 applied to CNA II will be presented. Particular emphasis will be given to the issues of performing PSA for plants with partly uncommon properties, which are still under construction. This is comparable to the challenge of performing a PSA for a novel design. The focus is as well on the definition of the two interfaces to PSA level 1 and level 3.

Keywords: PSA level 2, PHWR, Argentina, severe accidents

1. Introduction

The Argentinean plant Central Nuclear Atucha II (CNA II, 745 MWe) together with its largely similar “sister unit” of lower power level (CNA I, 357 MWe) is located at the same site. While CNA I went into operation in 1974, the construction of CNA II has started 1981. Buildings and large components have been built until the mid-1980s. Construction has been interrupted from 1994 until 2004. Now this plant is nearing completion. CNA II has to fulfil the Argentinean risk criterion. It requires that the consequences of accidents respectively severe accidents must not exceed a certain frequency-dependent limit. Therefore, it is necessary to identify and analyse the different accident sequences and to determine their respective frequencies in a PSA level 2 as a basis for plant external analyses in PSA level 3.

PSA level 2 analyses apply PSA level 1 results as initial conditions, and the outcome of PSA level 2 is transferred to PSA level 3 which finally generates those doses to the public which can be compared to the risk criterion. Consequently, PSA level 2 has an interface with PSA level 1, and an interface with PSA level 3.

The basic approach for the probabilistic accident progression analysis is an event tree analysis. In addition, the PSA of CNA II relies on a limited number of deterministic computer simulations using the integral code MELCOR 1.8.6. MELCOR is one of the most advanced computer codes for severe accident analyses and is applied worldwide for PSA level 2. A large effort has been devoted within the PSA level 2 for CNA II to produce a set of MELCOR runs according to the state of the art on a best-estimate basis starting with initial and boundary conditions as close as possible to real plant specific data. Issues that are not sufficiently covered by MELCOR, or that are plant specific, have been treated and described separately.

Although CNA II is not a novel design, the plant has some uncommon features. In addition, the Argentinean radiological risk criterion is an advanced requirement. Therefore, it is justified to submit the present contribution to the OECD workshop on new and advanced reactors.

2. Particular challenges of the PSA

As stated in the introduction, CNA II is not a novel design; nevertheless there are several issues which are comparable to the challenge when performing a PSA for a new plant. The following list provides those items:

- The PSA has to be performed before the plant is in operation There is very little experience from similar plants. Worldwide, there is just one smaller plant CNA I which is comparable to CNA II.

- The scope of the PSA includes PSA level 3, i.e. radiological consequences.

- The levels 1, 2, and 3 of the PSA to get the operation license are performed by different specialised teams.

- Accident progression is very slow for many sequences and especially after core degradation has started due to low specific power, large amount of coolant and moderator water in the reactor circuit and large steel mass of filler pieces inside RPV bottom.

- The primary system has some unique features (four moderator loops connected to the moderator tank inside the RPV, almost all free volume in the RPV bottom head occupied by steel filler pieces, use of natural or lightly enriched uranium fuel elements inside zircaloy coolant channels [like BWR canisters], arranged in the large moderator tank of the RPV with a very large pitch between the channels)

- The containment is of the typical German large dry type; but there are specific design differences like the online refuelling and the external spent fuel pool, space occupied by the moderator systems and its heat exchangers located below the steam generators, flow paths connecting the cavity and the sump at the bottom, enabling core melt after RPV failure to challenge the containment function.

Figure 1 shows the moderator loops and sections of the main coolant loops. Figure 2 is an overall picture of the whole plant, where the containment, the auxiliary building and the spent fuel pool building can be seen in particular.

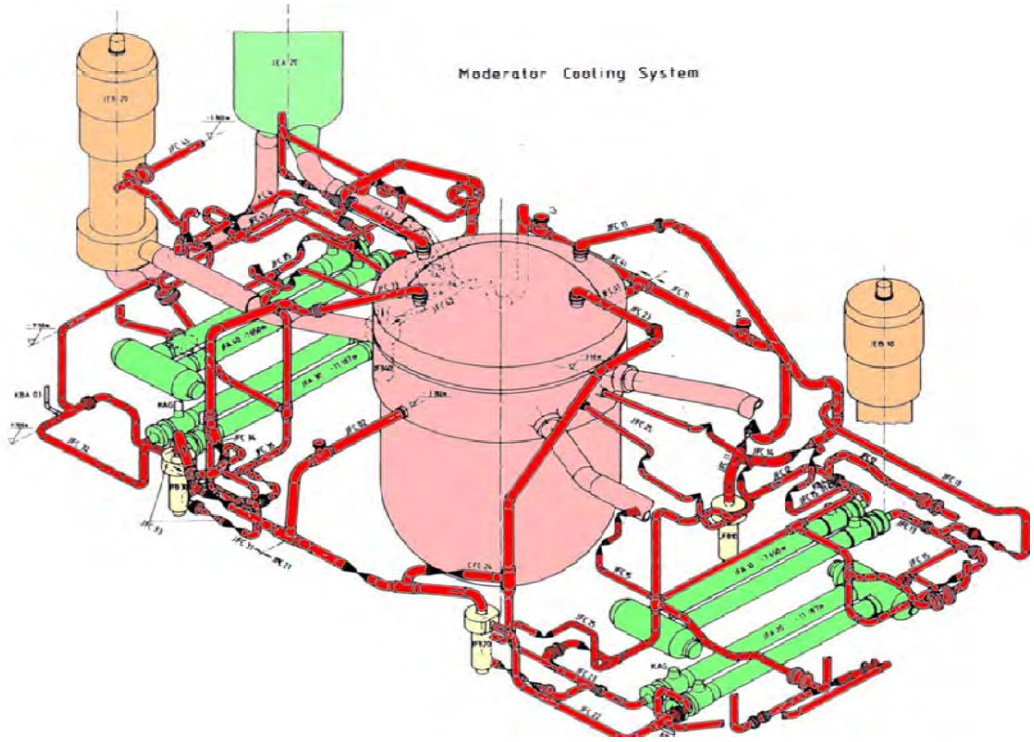


Fig. 1: Primary and moderator cooling system of CNA II

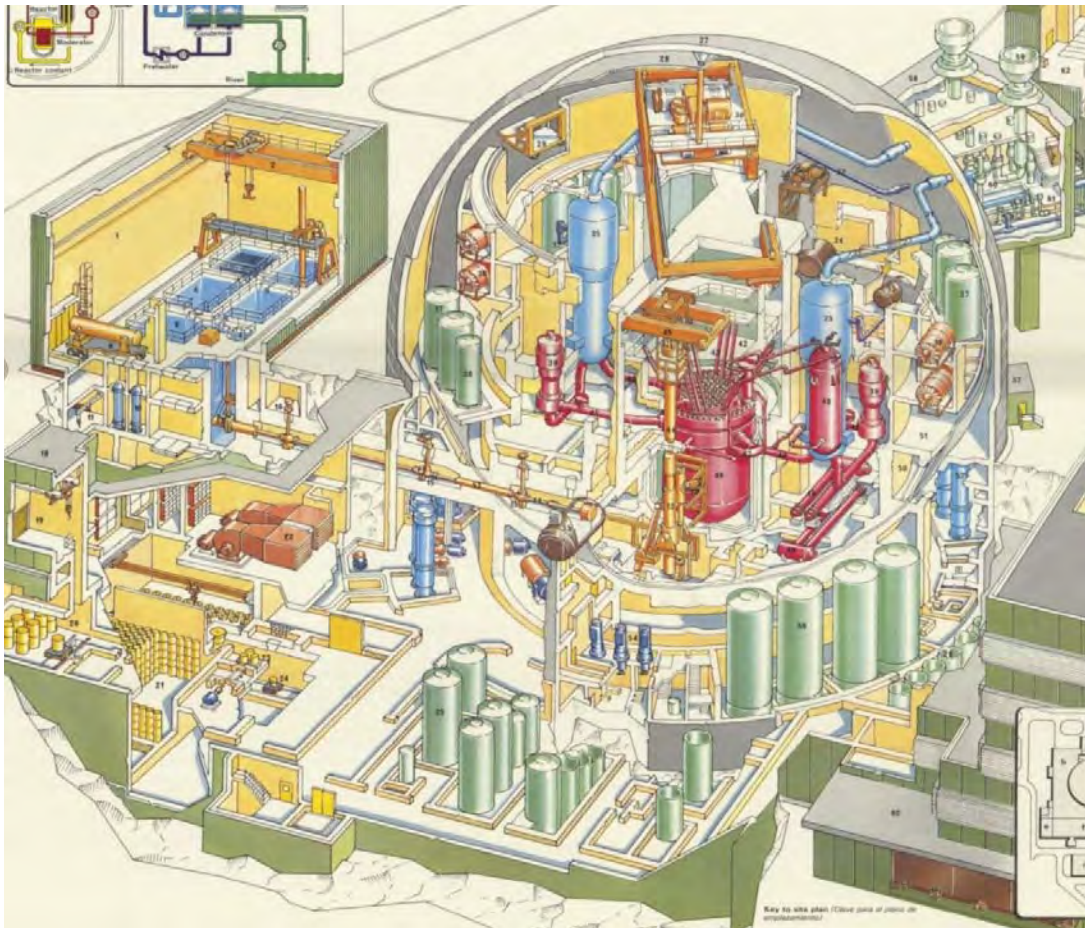


Fig. 2: General view of CNA II plant

3. The argentinean dose limit

The Argentinean dose limit (AUTORIDAD REGULATORIA NUCLEAR, 2002) requires that the accident related risk to an individual must not be higher than the risk due to normal operation. The risk is defined as product of the frequency for a certain exposition and the conditional probability for death caused by the exposition (see fig. 3).

The conditional probability for death is derived from ICRP data. It is separated into a stochastic region (<1 Sv) and into a non-stochastic region (>6 Sv). Between these two regimes there is a transitory regime. The risk due to normal operation is derived from an admissible exposition of 0.001 Sv / a.

Applying some additional pessimistic assumptions in order to cover uncertainties, the line shown in fig. 3 is defined. The criterion is valid for a single individual; it does not represent considerations for a group. Since 6 Sv is assumed to be lethal for the individual, an increase of the dose beyond 6 Sv could not produce more effect. Therefore the line does not further decrease beyond 6 Sv and 1.E-7/a. The criterion is valid for all operating regimes and for all initiating events. If more than 10 different groups have to be considered, the y-axis of the graph has to be adapted accordingly.

Fig. 3: The Argentinean dose limit

When applying the criterion, accident sequences have to be combined into groups and for each of the groups a pessimistic sequence should be selected, representing the whole group. Per definition, the sequences within a group are not very different, although they are not identical. In practice, difficulties occurred in the process of selecting a pessimistic sequence as follows:

- If the groups are defined adequately, the consequences of the group members do not differ very much, so that it is questionable whether the effort to identify the most pessimistic one is justified.

- In order to identify the most pessimistic sequence in a group, it is (at least in principle) necessary to completely analyse many of the sequences within a group - including source term determination and the off-site consequences.

- It may turn out, that the most pessimistic sequence has a very small probability, far below the more frequent members of the group.

Lessons learned:

The criterion defines a certain dose limit to the public. It does not provide guidance with respect to other characteristic results, e.g. to core damage frequencies or to frequencies of large releases. This is straightforward and logical, but it means that the traditional grouping of sequences into core damage states or release categories is not helpful. In principle all sequences have to be analysed until the final dose calculation. Since this is not practical with the present methodology, grouping at intermediate levels is still needed, but it is required that within a group the most pessimistic sequence is selected as representative.

4. Interface between PSA Level 1 AND Level 2

The plant owner NA-SA performs PSA level 1 (for initiating events from full power operation only) and provides information about the core damage states to GRS, who does the subsequent PSA level 2. NA-SA applies the code RiskSpectrum, and GRS applies EVNTRE (GRIESMEYER 1989). Therefore, an interface had to be defined, linking both levels of the PSA. In principle, the traditional approach with a set of about 15 different attributes as described in general in the German PSA guideline (BUNDESAMT FÜR STRAHLENSCHUTZ 2005) defining the core damage states has been followed. Those attributes cover usual features (such as RPV pressure, or containment isolation) but also plant specific issues (such as loss of heat removal through the moderator loops, or leaks in the moderator loops). Since PSA level 2 work could not wait until PSA level 1 was finished, both teams had to work in parallel, and the interface had to be defined early in the project. This required considerable effort and iteration because the impact of some accident related plant properties had not been quite clear in the beginning, and because the different teams had to become familiar with the way of thinking and modelling of the other team.

Lessons learned:

PSA level 1 tends to apply pessimistic success criteria based on design basis accidents. PSA level 2 provide more realistic criteria for core damage states. In the present PSA for CNA II, the more realistic criteria identified by level 2 have mostly been adopted by level 1.

PSA level 1 / 2 interface uses about 15 core damage state attributes as recommended in the German PSA guide. Only minor modifications have been necessary to include the plant specific status of the moderator loops and its heat exchangers.

Once the interface is defined and agreed, the transfer of core damage states runs smoothly, including Monte Carlo uncertainty data.

PSA level 1 for CNA II identified that there are only few representative sequences leading to core damage. The final number of relevant core damage states is small (about 10). Many accident sequences, which can be imagined in principle (e.g. containment bypass, large break LOCA, high pressure sequences) have negligible frequencies.

5. Selection of representative MELCOR runs as basis for Level 2 analyses and for the interface to Level 3

GRS delivers source terms to the environment and the associated frequencies to the Argentinean research institute CNEA, which performs level 3. GRS applies the integral code MELCOR 1.8.6

(GAUNTT 2005) for severe accident analysis, and CNEA uses MACCS (BIXLER 2009) for the level 3 purposes. MELCOR source term output can easily be converted to a MACCS input file, so that from a technical point of view, the interface is no challenge.

However, this leads to the question, which MELCOR runs should be regarded as representative for source terms and which cases are needed to allow the event tree quantification. The following issues have to be considered:

- MELCOR is regarded as a state-of-the-art tool for severe accident analysis, providing realistic results. In probabilistic terms this means that MELCOR typically will represent the more likely sequences and source terms. However, in a PSA also very unlikely sequences at the edge of the spectrum need to be considered. As an example, there is a remote probability for containment failure due to hydrogen combustion, but in order to assess the related source term, combustion with subsequent containment failure had to be defined in a MELCOR run. Therefore, the user has to force MELCOR to calculate extreme sequences. It is important that nevertheless the selected parameters and assumptions are not unreasonable and physical phenomena are considered appropriately.

- Secondly, as required by the risk criterion, the source term representing a group of sequences should be pessimistic in a sense of causing highest consequences. Since several different sequences from PSA level 1 end up in the same CDS group, it is not trivial to select the most pessimistic one without detailed analyses. This difficulty has led to a more practical approach in the project, selecting the most frequent scenario to represent a group of CDS.

Lessons learned

It is difficult to define “pessimistic” scenarios without detailed analyses within a group of sequences which are not very different, in order to fulfil the Argentinean risk criterion.

The selection of the boundary conditions for the MELCOR runs related to systems status is done based on PSA level 1 fault trees. “Best estimate” conditions without particular conservative assumptions are always used.

Forcing MELCOR to calculate sequences beyond the usually expected accident progression requires care in order to avoid unphysical results. One example is an analysis with a local hydrogen combustion causing a small defined local containment failure.

6. Modelling the plant with MELCOR

CNA II is similar to typical German PWRs for many aspects but it differs in several other aspects from those reactors, so that modelling it with MELCOR is a real challenge. The following issues are particularly important:

- The coolant and moderator in CNA II is heavy water, not light water. Light water is used only in the emergency core cooling system. MELCOR does not have sufficient models for heavy water thermal properties. A survey of heavy water thermal properties and a comparison of the early accident phase between MELCOR and RELAP (which has an adequate model) confirmed that the light water models and the developed reactor/moderator circuit model are adequate.

- CNA II has individual zircaloy fuel channels around each fuel element. Therefore, although it is a pressurized water reactor, the MELCOR core model for BWRs with zircaloy canister structures around fuel elements has been applied. It allows an adequate modelling of the core melting process including zircaloy oxidation and hydrogen production and the opening of

flow paths between the coolant channels and the moderator tank. Not much adjustment was needed to get reasonable results.

- CNA II has four moderator loops including a moderator pump and a heat exchanger in each of it. An individual model of each loop was needed as the systems are used during normal operation for heating the steam generators feed water and during accidents for emergency core cooling and residual heat transfer in addition to the steam generators.

- CNA II has large steel filler pieces in the lower and upper plenum of the RPV, reducing the required volume of heavy water. A fine axial lower plenum model was needed. In combination with the low power, this leads to very long lasting core melt sequences with large liquid steel fractions before the RPV bottom fails mainly at a lateral position. Not all of the steel filler pieces get molten.

- After RPV bottom failure, corium spreads into the cavity and can move through ducts from the cavity to the containment sump, where it is covered by the sump water. There it will probably fail one to four of the sump suction lines or their penetrations at the bottom of the sump. So the containment function is lost and connection(s) into one to four different rooms inside the reactor building annulus at its lowest level are opened. Several related assumptions about up to six different “cavities” had to be entered by the user. “Cavity models” of the reactor pit, the sump and the four rooms inside the reactor building annulus are needed. The melt transfer between the cavities is controlled by the code user.

- The MELCOR analyses performed in the project have been used in addition for the determination of the passive autocatalytic recombiner (PAR) concept. This requires an adequate modelling of the containment volume and of the PARs.

- As the most probable radionuclide release paths lead through the annulus and parts of the connected auxiliary building, both had to be modelled in large detail as well. This applies also to ventilation systems inside the containment and as well the annulus.

Lessons learned

MELCOR is flexible enough to model several plant features of CNA II which are different from ordinary reactors – PWRs or BWRs. Therefore, there may also be good prospects for applying or adapting MELCOR to new reactor designs.

Adequate detail in the plant modelling, together with the often slow accident evolution and requirements from PSA level 3 related to the duration of analysed sequences, lead to large computing times (sometimes in the order of months on a PC).

Critical evaluation of MELCOR results is needed in order to ensure a realistic assessment of non-common features. Code to code comparison with a detailed RELAP model used by NA-SA for PSA level 1 provided confidence in the MELCOR models. Having large experience in applying MELCOR to PWR and BWR plants was very helpful.

Some MELCOR deficiencies could be identified and fixed or circumvented (e.g. by a separate source term estimation within the event tree analysis related to gaseous iodine source terms).

7. Probabilistic assessment

The probabilistic accident progression analysis is based on an event tree analysis performed with the EVNTRE code. In early stages of the project, before it was known that the spectrum of core damage states is rather limited, and before some plant specific features had been fully evaluated, a general event tree had been developed within this PSA. Due to the particular design of CNA II and according to the set of core damage states provided by PSA level 1, several issues normally addressed in PSA level 2 are irrelevant or trivial in this plant.

The final event tree consists of approximately 100 branching points. They are mostly arranged in a logical way so that causes are followed by consequences. This is practically equivalent to a chronological ordering of the branching points. About half of the branching points are needed to evaluate source terms and other results.

Since high pressure scenarios and containment bypass scenarios are not relevant in CNA II according to the present set of CDS, only the following uncertain issues remained with potential high influence on the source terms, needing refined probabilistic assessment:

- Hydrogen combustion in the containment and potential containment challenge, if the PAR system foreseen to be installed does not prevent them.

- Loss of containment function by melt-through of sump suction lines / penetrations due to core melt attack.

- After sump suction line melt-through: Pressure build up and failure of doors from the reactor building and / or from the auxiliary building, leading to the environment.

Explicit source terms from MELCOR calculations are available only for a relatively small number of representative accident sequences. But at least one MELCOR calculation exists for each CDS group and for each of the defined release categories. Often sensitivity calculations of the base cases have been performed to support the event tree quantification. In order to have some estimate of the source term for each sequence described by the event tree a so-called release factor model has been implemented into the event tree analysis for iodine in its most likely chemical form CsI and for noble gases. Gaseous iodine is considered additionally in the event tree models.

Lessons learned

Plant-specific features can be important for the overall result (like the potential for containment failure via sump suction lines in case of CNA II). Their probabilistic assessment often requires expert judgement in addition to results and boundary conditions obtained from deterministic analyses.

The EVNTRE code has proven its value for complex probabilistic analyses, especially because user-defined subroutines for obtaining branching probabilities can be implemented. For example, this feature has been used in the present PSA for a source term estimate on the basis of a release factor model which is directly linked to the event tree model.

8. Definition of release categories and source terms as interface to Level 3

During the course of the project, several iterations with staff from PSA level 3 took place to develop an agreed PSA level 2 – level 3 interface. The following key issues are taken into account in defining release categories (considering that the present CNA II analysis does not contain containment bypass sequences):

- Status of containment ventilation isolation (isolated – not isolated)
- Containment leak before RPV failure (leak develops – does not develop)
- Core relocation to lower plenum leading to RPV failure (no RPV failure – RPV failure more than 48 h after initiating event – RPV failure less than 48 hours after initiating event)
- Containment failure via sump suction line (failure occurs – does not occur)
- Status of doors to environment in annulus and auxiliary building after containment failure (doors are forced open – doors remain closed)

The selection of these attributes is based on the source terms calculated by various MELCOR runs. It could be shown that this set of attributes sufficiently defines the source term. The precise definition of the release categories needs information about similarities of releases and therefore depends on the MELCOR accident analyses.

In principle, with those five sorting criteria mentioned above a maximum of $2 \cdot 2 \cdot 3 \cdot 2 \cdot 2 = 48$ release categories could be defined. In the practical definition of the release categories, however, some of the possible combinations are grouped together if their release characteristics are similar or if a finer distinction would lead to release categories with vanishing frequency. Further, it is not reasonable to combine all attributes, because some of them are overriding others. For example, if the containment ventilation is open, there is always the possibility for an early and large release of radionuclides into the environment, whatever is the status of the other parameters. Finally, the analysis showed that seven different release categories are sufficient.

As mentioned above, the frequency of each release category has been calculated with the event tree, and the source term for each release category has been taken from an appropriate representative MELCOR run. Uncertainties of frequencies are identified by a Monte Carlo analysis of the event tree, and uncertainties of the source term magnitude are covered by the specific release model in the event tree, taking into account also gaseous iodine.

8. Summary and results

With respect to PSA level 2 for new and advanced reactors, the experience with CNA II shows:

- Existing deterministic (MELCOR) and probabilistic (EVNTRE) methods and PSA guidelines in general are flexible enough to analyse new or especially uncommon reactor designs.
- Plant specific design details may require specific analyses or estimates beyond present code capabilities, and they can largely determine the PSA results.
- If PSA level 3 is required, significant uncertainty exists regarding the definition of source terms and the selection of representative or most “challenging” cases.
- In particular the behaviour of Iodine is still not covered satisfactorily by state-of-the-art models in MELCOR. Additional effort was needed in the event tree to represent gaseous iodine.
- A precise definition of interfaces between the PSA levels supports understanding among different PSA teams and enables parallel work on the different levels. A direct transfer of MELCOR results to the PSA level 3 team is a simple and useful approach.

The unique feature of CNA II in contrast to most other operational reactors is a direct path from the cavity to the sump at its bottom level: ore melt easily can reach the sump and the sump suction lines after RPV failure. This causes likely damage to sump suction lines and their penetrations due to core melt attack after RPV failure, which means that the containment function is lost. The failure of doors to the environment is rather likely after sump suction line melt-through, leading to considerable source terms through the annulus and/or parts of the auxiliary building into the environment at ground level.

As a consequence, one release category characterized by RPV melt-through, sump suction line melt-through and doors to the environment pushed open clearly dominates. Nevertheless, the release fraction of Iodine in the form of CsI aerosol is only of the order of 2 % of the core inventory even in this case because Iodine is mostly contained within sump water, not in the atmosphere. Sump water is released from the containment, but it remains in the lower rooms of the reactor building. Because of the low CsI release fraction, the relative contribution of gaseous iodine becomes important. The additional fraction of gaseous iodine reaching the environment can be of the same order as the iodine in aerosol form.

The hydrogen issue is almost irrelevant, demonstrating the beneficial effect of the PARs foreseen to be installed.

The duct between cavity and sump which is detrimental for core melt progression, could on the other side allow the implementation of an accident management measure to cool the RPV from outside to avoid its failure. Since the RPV is big and the specific power is low, there are good chances for success. This measure is under consideration at present, but not yet decided.

10. References

AUTORIDAD REGULATORIA NUCLEAR (2002), Criterios radiologicos relativos a accidentes en reactores nucleares de potencia, AR 3.1.1, Revision 2, 2002

BIXLER, N., K. McFadden, L. Eubanks, and R. Haaker, Overview and Status of WinMACCS/MACCS2, Paper presented at CSARP Meeting, September 15-17, 2009, Residence Inn Bethesda, Bethesda, Maryland

BUNDESAMT FÜR STRAHLENSCHUTZ, Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, BfS-SCHR-37/05, August 2005

FABIAN, H.; Frischengruber, K. Safety concept and evaluation for the pressurized heavy water reactor Atucha II, Atomkernenergie Kerntechnik Vol 46 (1985) No1

GAUNTT, R. O., J.E. Cash, R. K. Cole, C. M. Erickson, L.L. Humphries, S. B. Rodriguez, and M. F. Young, MELCOR Computer Code Manuals, Vol. 1: Primer and Users' Guide, Version 1.8.6 September 2005, Sandia National Laboratories Albuquerque, NM 87185-0739, NUREG/CR-6119, Vol. 1, Rev. 3, SAND 2005-5713

GRIESMEYER, J. M., Smith, L.N, A Reference Manual for the Event Progression Analysis Code (EVNTRE), NUREG/CR-5174, September 1989

PSA Level 2 as Element of an Integral Safety Assessment before Plant Commissioning

Horst Löffler, Dr. Oliver Mildenberger,
Dr. Martin Sonnenkalb, Dr. Thomas Steinrötter

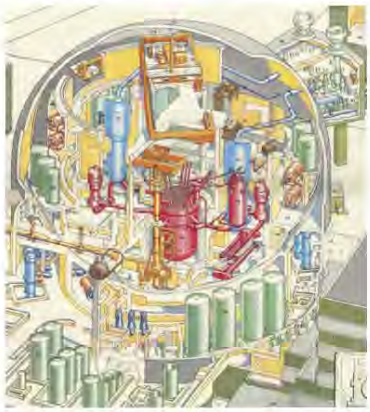
OECD/NEA workshop on PSA for New and Advanced Reactors
Paris, June 20-24, 2011

Why this presentation in a workshop on PSA for New and Advanced Reactors?

- Licensing requirement is very advanced: quantitative dose limit to be demonstrated by PSA level 3
  - **Principal requirement on PSA is probably even higher than for many new projects**
- Several uncommon properties of reactor under consideration call for adaptation of existing methodology
  - **Problems and approaches for solution of uncommon reactor properties may be similar in principle for new designs**

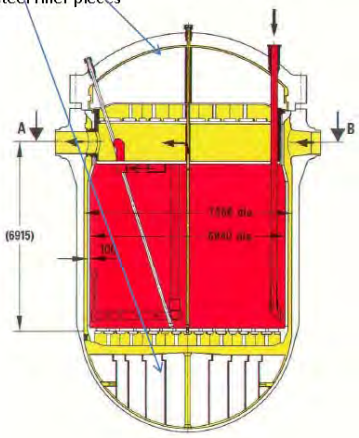
Atucha II (CNA II, 745 MWe)

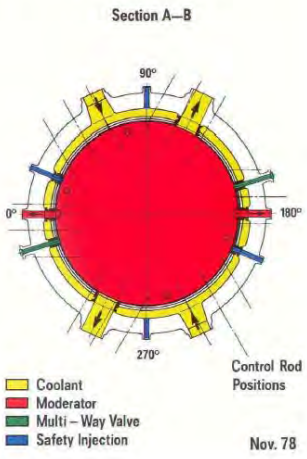
- KWU-Design: PWR with heavy water and RPV and large dry containment
  - Two independent core cooling systems continuously operating:
    a) reactor cooling loop (fuel elements inside channels , 2 SG)
    b) moderator cooling loops (moderator between fuel channels, 4 loops with heat exchangers)
    → low core melt frequency by transients (except SBO)
    → leaks at moderator loop are relevant
  - Low specific power and large steel mass in lower plenum
    → slow core melt progression
    → external RPV cooling could be successful
  - Connection between reactor cavity and sump promotes local containment failure at sump suction lines after RPV meltthrough
- Long delay in construction after completion of buildings and large components
- Construction almost completed now
- PSA Level 1 – 3 performed by KWU in mid 1980's
- Actual PSA Level 3 is precondition for licensing (→ argentinian dose limit)
  - Level 1 from plant owner NA-SA
  - Level 2 from GRS (full power only)
  - Level 3 from argentinian research center CNEA + NA-SA



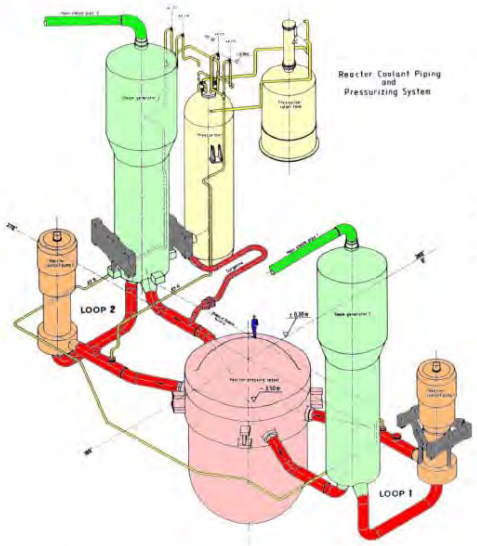
CNA II: reactor pressure vessel

- Fuel elements exchanged during power operation → inclined control rods
- Lower and upper RPV head filled with steel filler pieces
- coolant temp. max. 314°C
- moderator temp. max. 239°C
- many RPV nozzles





CNA II: reactor coolant loops (RCL)

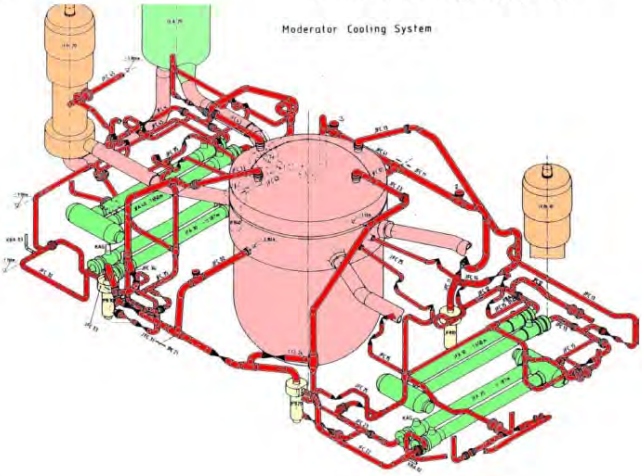


- common 2-loop PWR
- in case of incident normal heat removal by steam generators
- operating pressure 11.5 MPa
- heavy water
- pressurized accumulators and low-pressure injection pumps available

H. Löffler, 2011-06-21 5

CNA II: moderator loops (ML)

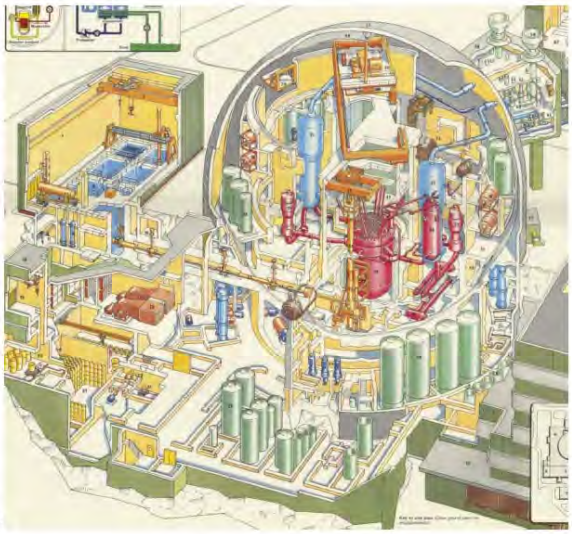
- four ML with lower temperature than main coolant loops
- extracted heat is used for preheating the feedwater
- ML are operating continuously → backup in case of loss of main coolant loops
- Valve switching needed when changing ML from normal to emergency operation



H. Löffler, 2011-06-21 6

CNA II: Containment and buildings

- Typical German containment
- Plant specific: Reactor cavity has connection to sump
  - cavity may be wet
  - RPV external cooling possible in principle
- Suction of LP injection pumps always and only from sump
- Moderator-HX below SG and above sump
- Modifications for online-refueling:
  - Spent fuel storage outside containment
  - Refueling machine always located above RPV
  - Fuel element transport below surface
  - Building bottom located ca. 20m below surface
- Release paths lead through reactor building and auxiliary building
- Passive Autocatalytic Recombiners against Hydrogen



H. Löffler, 2011-06-21 7

Argentinian Dose Limit

- „Risk" is defined as the probability for an individual to die from radioactive releases leaving the plant.
- The risk due to accidents must not exceed the maximum admissible risk due to normal operation (corresponds to 0,001 Sv/a)
- Stochastic region < 1 Sv; non stochastic > 6 Sv

- Together with several pessimistic assumptions the graph shown at right evolves
- The criterion is valid for a single individual, not for a group
  → no decrease beyond 6 Sv.
- The y-axis has to be renormalized if more than 10 different release categories have to be considered.
- The criterion is valid for all initiating events and all operating states.

H. Löffler, 2011-06-21 8

Transition from PSA Level 1 to Level 2

- Level 1: Performed by NA-SA with RiskSpectrum
- Level 2: Performed by GRS with EVNTRE
- Teams of Level 1 and 2 have been working in parallel
  → Definition of a set of core damage states (CDS) as interface early in the project

- **Lessons learned:**
- Approaches and assumptions in Level 1 not always consistent to Level 2
  → Iteration and common understanding needs time
- CDS characterization had to be adapted to plant specific properties
  → about 15 different core damage state attributes, each with at least 2 values
- Once the interface had been defined, data transfer level 1 → 2 runs smoothly , including CDS frequency distribution

- Results of Level 1:
  - 10 CDS with >10E-9/a each
  - Station black out is dominant (potential recovery of electric power ignored)
  - No CDS with: high pressure in RCL, or containment bypass, or energetic power excursion

H. Löffler, 2011-06-21 9

Deterministic Accident Progression Analysis: Approach

- MELCOR 1.8.6 has been selected as flexible state-of-the-art tool
- All accident sequences are calculated up to 24 h after large release begins (which is typically meltthrough of sump suction lines)
- MELCOR data files containing source terms are directly transferred to PSA level 3
- Challenges:
  - Core design (fuel elements with individual cooling channels) is uncommon for PWR and requires application of the MELCOR BWR core model
  - 4 additional moderator loops need additional complex modeling
  - Providing precise source terms for Level 3 requires detailed modeling of release paths including buildings
  - Demonstrate that H_2O data from MELCOR can be applied to D_2O (comparison to results from RELAP code)
  - The system status for the MELCOR runs is based on PSA level 1 fault trees. "Best estimate" success criteria without particular conservative assumptions are used.
  - Run times for a sequence can be extremely long, partly because of long real times (typically 1 d to 3 d until RPV meltthrough)

H. Löffler, 2011-06-21 10

Typical times for accident sequences

	core melting	core slumping	RPV failure	containment failure
0.1A LOCAs in ML with loss of LP injection	from 2-3 h	from 5-6 h	from 20 h	short after RPV Failure (sump suction line meltthrough)
SBO	4-8 h	~11 h	~1 d	
200-400 cm² LOCAs in RCL with loss of LP injection	from 2h	from 2d	from 3 d	
90 cm² LOCAs in RCL with loss of LP injection	~34 h	~4 d	~4.5 d	
complete loss of feedwater	~60 h (after cavitation of LP pumps)	~77 h	~4 d	n/a

H. Löffler, 2011-06-21 11

Lessons learned in deterministic accident progression analysis

- **MELCOR is flexible enough** to model several plant features of CNA II which are different from ordinary reactors – PWRs or BWRs. Therefore, there may also be good prospects for applying or adapting MELCOR to new reactor designs.
- Adequate detail in the plant modelling, together with the often slow accident evolution and requirements for a long duration of analysed sequences, lead to **large computing times** (sometimes in the order of months on a PC).
- **Critical evaluation of MELCOR analysis is needed** in order to ensure a realistic assessment of non-common features. Code to code comparison with a detailed RELAP model used by NA-SA for PSA level 1 provided confidence in many of the MELCOR models

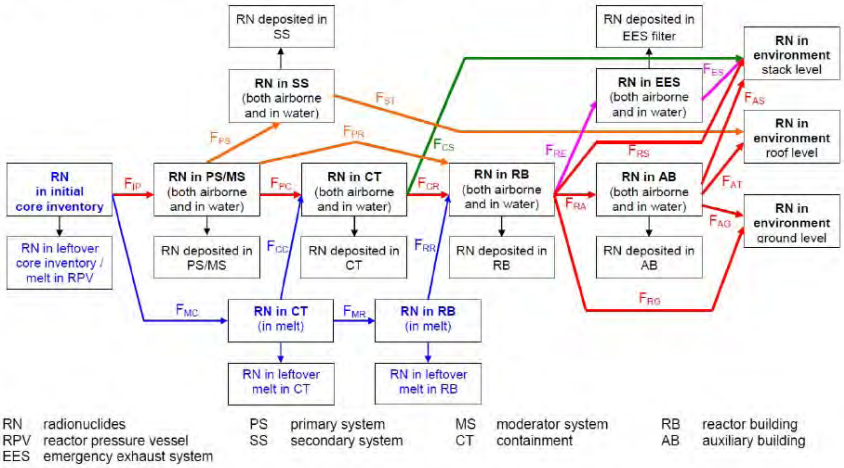
H. Löffler, 2011-06-21 12

Event tree analysis

- Event tree for CNA II is simple in principle because:
  - Small number of CDS
  - Rather small variability of accident progression inside containment
- However: high requirement with respect to source terms as basis for PSA Level 3
  - MELCOR source terms alone not sufficient
  - Simple release model implemented into event tree (see next page)
  - Additional consideration of gaseous iodine
  - Source term determined for each single sequence in the event tree
  - Source terms are grouped according to release categories
- Approach provides:
  - Range of source term magnitude within a release category
  - The relative position of MELCOR source term within a release category

H. Löffler, 2011-06-21 13

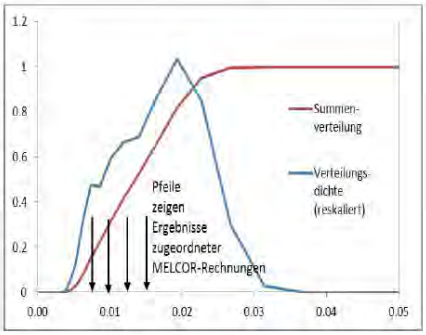
Simple release factor model inside the event tree analysis



Transitions between volumes are derived from MELCOR results and completed by uncertainty assessments

H. Löffler, 2011-06-21 14

Source terms within a release category



X-axis: Fraction of the Iodine core inventory which is released into the atmosphere in the most frequent release category in CNA II
Y-axis: relative frequency

Summary:
(not valid for other release categories !) :

- The aerosol Iodine source term is between 0.005 and 0.03 of the core inventory
- The MELCOR source terms are located in the lower range of the release magnitude
- Gaseous Iodine is not taken into account in this figure.

H. Löffler, 2011-06-21 15

Lessons learned for event tree analysis

- **Plant-specific features can be important** for the overall result (like the potential for containment failure via sump suction lines in case of CNA II).
  Their probabilistic assessment often requires expert judgement in addition to results and boundary conditions obtained from deterministic analyses.
- The EVNTRE feature of implementing **user-defined subroutines directly into the analysis is extremely valuable.**
- User defined subroutine has been used to define **a release factor model** for probabilistically evaluating source terms and assessing deterministic source terms

H. Löffler, 2011-06-21 16

Release Categories an Source Terms

- Accident sequences are grouped into release categories.
  - Five sorting criteria (e.g. status of containement isolation)
  - Seven release categories (RC)
  - For each RC a source term from a representative MELCOR run
  - Argentinian regulation requires „pessimistic“ sequence within a RC. However, this is hardly achievable → instead „representative “ sequence
- MELCOR-source term does not consider gaseous iodine → event tree provides additional contribution of gaseous iodine.
- Typical accident sequence with late containment failure at sump suction lines and subsequent pushing open of building doors is as follows:
  - The radionuclides are mostly contained within the (sump-)water which is located at the bottom of buildings and cannot reach the environment.
  - About 2 % of the core inventory of iodine are released into the environment through building doors immediately after containment failure.
  - Additionally 2 % of the iodine inventory are released in gaseous form
  - 40 % to 50 % of the noble gas inventory are released into the environment until the end of the calculation (24 h after containment failure)

Lessons learned for interface to Level 3

Interface consists of a **source term calculated by MELCOR** for each release category together with its frequency distribution **and an indication of the spread of source term magnitude** within the release category. Gaseous Iodine has to be taken into account.

It is difficult to define “pessimistic” scenarios within a release category, in order to fulfil the Argentinean risk criterion.

Forcing MELCOR to **calculate deviating sequences** beyond the usually expected accident progression in order to quantify specific source terms requires care in order to avoid unphysical results. One example is seeking a source term for an unlikely local hydrogen combustion causing a limited local containment failure.

Summary

Existing deterministic (MELCOR) and probabilistic (EVNTRE) **methods and PSA guidelines in general are flexible enough** to analyse new or uncommon reactor designs.

Plant specific design **details may require specific analyses or estimates beyond present code capabilities**, calling for expert judgement; and they can largely determine the PSA results.

If PSA level 3 is required, significant **uncertainty exists regarding** the definition of source terms and the **selection of representative or most "challenging" cases**.

In particular **the behaviour of Iodine is still not covered satisfactorily by state-of-the-art models** in MELCOR. Additional effort was needed in the event tree to represent gaseous iodine.

Accident analysis tools identified **risk reducing plant improvements**:

- Passive autocatalytic recombiners (installation has been decided)
- RPV external cooling (implementation under consideration)

H. Löffler, 2011-06-21 19

MAAP5 Modeling Capabilities for Initial Plant Transients and Shut-down State, and Application to Shutdown PSA and Full Scope SAMG Covering All Plant States for Operating and New Plants

Chan Y. Paik[1], Oleg Solovjanov[2], Quan Zhou[1], Sung Jin Lee[1], Robert W. Reeves[1], Robert E. Henry[1], and Wison Luangdilok[1]

[1]Fauske and Associates, LLC
16W070 83rd Street
Burr Ridge, Illinois 60527
Paik@Fauske.com

[2]Westinghouse Electric Belgium
Rue de I'Industrie 43,
1400 Nivelles, Belgium
Solovjo@westinghouse.com

Abstract

The Modular Accident Analysis Program (MAAP) is a computer code that is used for integrated severe accident analysis in both light water and heavy water moderated reactors. The MAAP code was developed and is maintained by Fauske and Associates, LLC under the sponsorship of Electric Power Research Institute (EPRI). MAAP5 is the latest generation of MAAP, which has new models to calculate forced and natural circulation inside a reactor coolant system (RCS) with more detailed nodalization. It also has a point kinetics and 1-D neutronics model, features to address new advanced reactor designs such as AP1000 and EPR, and improved containment models. Improvements were also made to calculate ANS-3-5 transients required for simulators, and shutdown and low power conditions, including mid-loop operations and conditions such as the reactor head open and the vessel submerged under the refueling water pool with the nozzle dams in place. This paper describes the new models in MAAP5 and presents example calculations of reactor transients such as a trip of one RCP, manual reactor scram, and maximum power ramp case. It also describes the development of the full scope SAMGs covering all plant operating states. Westinghouse has developed Shutdown SAMG (SSAMG) that is integrated into at-power Westinghouse Owners Group (WOG) SAMG to form a complete symptom-based SAMG package applicable to all Plant Operational States (POS). The development of the SSAMG is based on the shutdown and low power MAAP5 analyses and PSA studies performed for the European plants. The principal changes required in the entry conditions, diagnostic parameters, diagnostic prioritization, as well as specific severe accident guidelines and development of new guideline for Spent Fuel Pools. The SSAMG methodology based on this approach is matured and has been implemented at several operating plants with different reactor types: Westinghouse PWR, AREVA PWR, and VVER. The Westinghouse methodology to extend the applicability of the WOG SAMG to shutdown and low power conditions and the basis derived from the low power and shutdown MAAP5 analyses and PSA studies is described.

Keywords MAAP, AP1000, Initial Transient, Shutdown SAMG

1. Introduction

Modular Accident Analysis Program (MAAP) is a computer code that has been used by nuclear industry for integrated severe accident analysis for almost three decades. The MAAP code has been proven a powerful tool to simulate severe accident scenarios in generation II PWR and BWR plants, CANDU plants, and generation III plants such as AP1000, EPR and ESBWR. The latest revision, MAAP5.0.1, includes many new models and improvements over previous MAAP4, which have greatly extended the capability of the code. The new improvements not only make MAAP5 more powerful for conventional severe accident applications and Level II studies, but also make it suitable for long-term design-based transient analyses and Level I success criteria calculations.

For RCS model improvements, it now allows users to employ more sophisticated nodalization schemes in the RCS, evaluate the individual response of each coolant loop and steam generator, and consider coupling of secondary side of multiple steam generators through the steam header. One of the key improvements in MAAP5 is to accommodate the independent coolant loop response for PWR designs (MAAP4 can only have one “broken” and one “unbroken” loop). In addition to individual loops, MAAP5 models RCS designs with two reactor coolant pumps (RCPs) per steam generator (i.e., those designs with two cold legs for each hot leg). This enables an analyst to evaluate the system response including back flow in the idle loop, when one pump is shut down with the other RCPs in operation. The MAAP5 RCS model was benchmarked against the TMI-2 accident, Prairie Island steam generator tube rupture (SGTR) incident, Davis-Besse loss of feed water (LOFW) incident, and the BETHSY experiments.

MAAP5.0.1 code is the latest revision which can simulate the passive features of the AP1000 design with improved Core Makeup Tank (CMT) and Passive Residual Heat Removal (PRHR) models. Figure 1 show the RCS nodalization for AP1000. The surge line is modeled as a separate RCS node. In each node, mass and energy of water and gases (steam, N2, O2, H2, CO, and CO2) are tracked and pressure and temperature are calculated. Core makeup tank(s) and passive residual heat removal (PRHR) systems are AP1000- specific engineered safety systems. The CMT is modeled as a RCS region (or a node) in MAAP5 and the two CMTs are individually modeled. An improvement was made in MAAP5.0.1 to calculate the break flow (water and gas) during a double-ended DVI line break transient. Also, fission product transport from RCS to containment through the core makeup tank is modeled. The PRHR system is modeled as a heat sink in MAAP5. The volume associated with the piping and heat exchanger tubes is neglected. The calculation of heat transfer between the primary system coolant and the containment side of the PRHR tubes submerged in the IRWST water pool is similar to the heat transfer calculated in the steam generator. To simplify the heat transfer calculations, the heat capacity of the heat exchanger tubes is assumed to be negligible and gas heat transfer through the un-wetted heat exchanger in the IRWST side is neglected. The MAAP 5.0.1 AP1000 models were benchmarked against the Oregon State University’s (OSUs) passive vessel injection experiments (OSU, 1994).

The MAAP5 steam generator model was benchmarked against the MB-2 experiments (Mendler, 1986). The main steam header model in MAAP5 considers the common volume shared by all main steam lines. It is located from downstream of the MSIVs to upstream of high pressure turbine. This model is important when studying steam generator (SG) interactions during main steam line breaks. For AP1000 design, if the reactor is tripped or turbine load is reduced, the turbine bypass valves will open to extract a certain amount of steam from the steam header. The reactor control systems automatically open (or close) these valves in a regular way to control RCS temperature and SG pressures within safety limits. A new steam dump system model was added in MAAP5.0.1 to simulate the specific design of AP1000.

In addition to the RCS model, MAAP5 has a new containment model that can be used for Design Basis Accident (DBA) analyses as either a single node or multi-node model. Since a severe accident may result in release of fission products from the reactor core to the RCS and containment, and to the environment, MAAP5 is integrated with MAAP5-DOSE to calculate the in-plant and ex-plant

radiation dose. Radiation dose rates and integral doses resulting from the fission product releases can be calculated for any containment and auxiliary building nodes including the control room. Dose rates and doses at off-site can be specified by using an atmospheric dispersion factor (X/Q) from the various release points. The code has features to specify following time-dependent parameters: 1) off-site and on-site breathing rates of people in the affected areas, 2) the occupancy factor within in-plant nodes, such as a control room and technical support center building, and 3) the atmospheric dispersion factor. The code can also calculate Alternate Source Term radiation doses in compliance with NRC Reg. Guide 1.183.

Core model improvements in MAAP5 include a one-dimensional neutronics model and the addition of new models for oxidation of B4C and hybrid control rods. For the PWR version of MAAP5, a point-kinetics model has also been added. Lower head model improvements include detailed metal layer heat transfer modeling, improved oxidic pool convection model, maximum 100 nodes for lower plenum wall and lower crusts, and an improved ex-vessel cooling (outside surface) heat transfer model (i.e., various nucleate boiling heat transfer correlations and CHF as a function of inclination angle with and without thermal insulation effects). The code can also calculate heat transfer and natural circulation inside the gap between the reactor vessel wall and insulation for plants like AP1000 and APR1400.

For the PWR code, plant shutdown conditions can be modeled including mid-loop conditions and reactor head open cases with water in the refueling pool. Air or nitrogen injection into the pressurizer during initial shutdown conditions can also be modeled. Additionally, nozzle dams can be placed in each loop.

This paper illustrates the capabilities of the latest revision MAAP5.0.1 to simulate and validate initial transients and severe accidents from shutdown conditions for AP1000 design. Section 2 discusses three AP1000 initial transients simulated with MAAP5 code, manual reactor trip, maximum power ramp and trip of one feed water pump. Section 3 discusses results of operator actions during a severe accident from shutdown conditions and describes the Westinghouse methodology to extend the applicability of the WOG SAMG to shutdown and low power conditions and the basis derived from the low power and shutdown MAAP5 analyses and PSA studies. The last section concludes the paper.

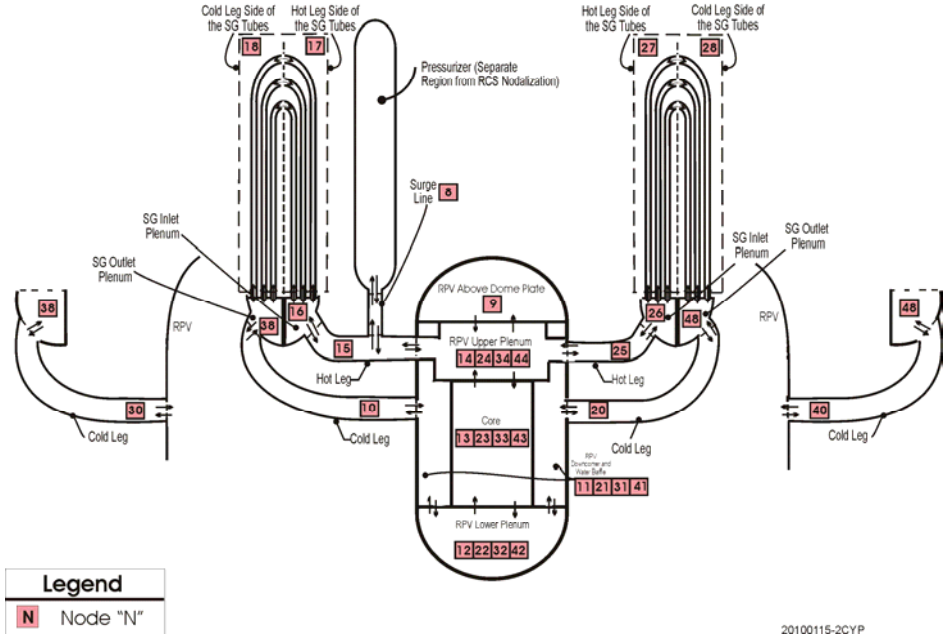


Figure 1, RCS Nodalization for AP1000 Type Plant

2. AP1000 initial transient simulations

Three selected AP1000 initial transients were analyzed (manual reactor trip, maximum power ramp and trip of single RCP) and are discussed in this section to demonstrate capabilities of MAAP5.0.1. For the AP1000 initial transient calculations, the point kinetics model is used.

2.1 Manual Reactor Trip

A reactor trip signal is initiated after a period of steady-state operation. Once the signal is received, all shut-down (SD) bank control rods are automatically dropped into the core to trip the reactor. The turbine stop valve is closed a few seconds after the reactor trip signal is received to isolate the main steam line. Main feed water (MFW) is shut off abruptly after receipt of a reactor trip signal and start-up feed water (SFW) is assumed to start immediately when MFW is terminated. Once the reactor is tripped, a reference no-load temperature is set, and the steam dump system automatically opens the turbine bypass valves to control SG pressures and allow the RCS temperature to match the no-load temperature.

For this transient, MAAP5 calculations are benchmarked against previous studies with RELAP5 (Barbensi, 2005). Figures 2 thru 4 show comparisons of average RCS temperature, SG pressure and SG level (narrow range) between MAAP5.0.1 and RELAP5. RCS temperature rapidly decreases in the first several seconds after the trip, due to power reduction and opening of the turbine stop valve. As the turbine stop valve is closed, RCS temperature and SG pressure start to increase. The temperature keeps increasing until it exceeds the no-load temperature, at which time the turbine bypass valves are automatically opened by the steam dump system. Eventually, dumping steam from the secondary side of the SG stabilizes the SG pressure and lets the RCS temperature match the no-load temperature. Comparisons between MAAP5 and RELAP5 show good agreement in RCS temperature and SG pressure. The water level in the SG secondary side is slightly lower for MAAP5, which may be caused by different nodalization scheme between the two codes. This transient shows that the RCS model, SG model and steam header model in MAAP5 can reproduce important thermal hydraulics processes in the early phase of a non-LOCA transient with satisfactory accuracy.

2.2 Maximum Power Ramp

The transient starts with a reduction of turbine load at a rate of 5% per minute to 75% of the nominal value. The load then starts to increase at a rate of 5% per minute from 75% to 95%, and the reactor operates at the 95% flow rate for 1 hour. As the turbine load changes, reactor power is expected to follow the load change through a nuclear feedback without actuating reactor trip or protection systems. Control rods are assumed to be inoperable during the entire power ramp transient and reactor power responds to the load change only through reactivity feedback mechanisms (Doppler and moderator temperature coefficients).

Figure 5 shows the comparison between the reactor power and the flow rate through the turbine stop valve. The power follows the flow rate change as expected with a slight delay time when the flow rate goes up or down. Peak values of the RCS temperature and pressure are both lower than the respective set-points to trip the reactor. The SG pressures are also less than those required to trip the reactor or actuate the safety systems. This sequence demonstrates MAAP5 capability to successfully model a transient requiring nuclear feedback in AP1000 design.

2.3 Trip of Single Reactor Coolant Pump (RCP)

There are total of four RCPs (pumps 1A and 1B for SG loop 1; pumps 2A and 2B for SG loop 2) in the AP1000. The initiating event for this transient is a trip of reactor coolant pump 1A.

Figure 6 shows that once RCP 1A trips, flow through this pump follows a pump-coast down curve in the first several seconds, then quickly drops to about -40%. A negative flow fraction indicates reverse flow from the cold leg back into the SG outlet plenum. In the mean time, the flow fraction through pump 1B increases from 100% to 121%, and the flow fractions through pumps 2A and 2B also increase slightly from 100% to 103.5%. Since pumps 1A and 1B share one SG outlet plenum, the trip of pump 1A creates a path for the water to flow through pump 1B, to the reactor downcomer, laterally through downcomer quadrants, then back to the SG outlet through the cold leg associated with the tripped pump. As a result, the flow rate through pump 1A is reversed and the flow through pump 1B increases to compensate for the reverse flow. The slight increase in pump flow through 2A and 2B is caused by density and thermal-hydraulic changes following the reactor trip. Figure 7 shows that the water level (wide range) in loop 2 SG is lower than that in loop 1 SG because more decay power is directed to the SG2 due to higher flows.

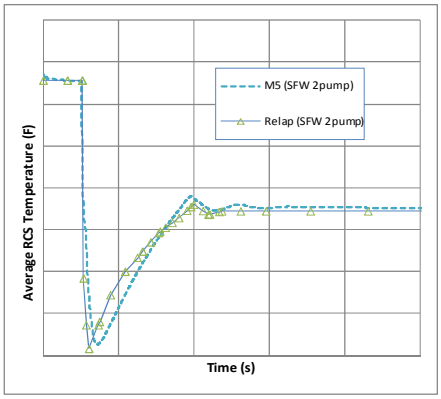


Figure 2, Comparison of RCS Average Temperature between MAAP5.0.01 and RELAP5

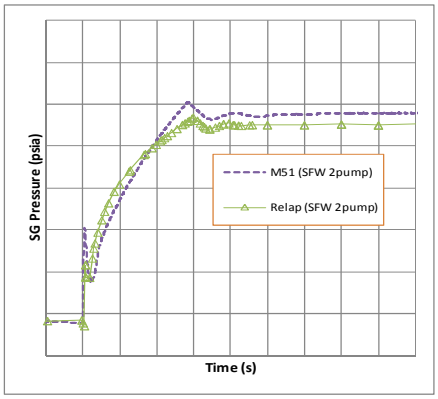


Figure 3, Comparison of SG Pressure between MAAP5.0.1 and RELAP5.

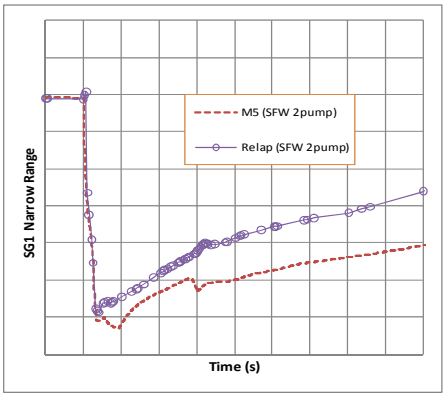


Figure 4, Comparison of SG Water Levels between MAAP5.0.1 and RELAP5.

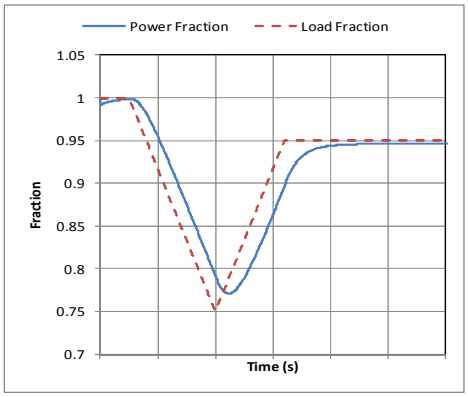


Figure 5, Turbine Load and Reactor Power Fraction for the Maximum Power Ramp Transient

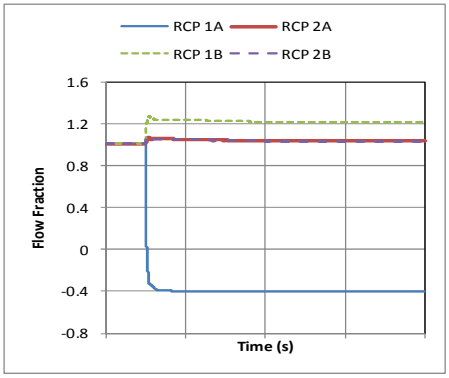


Figure 6, Flow Fraction through RCPs for the Single RCP Trip Transient

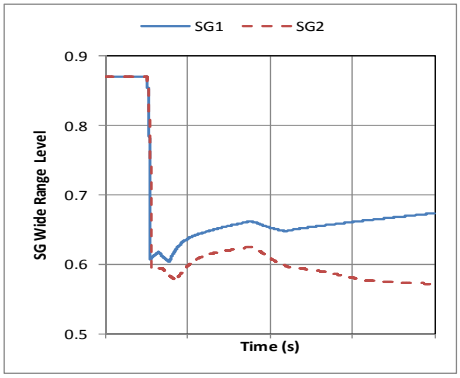


Figure 7, Comparison of SG Water Levels for the Single RCP Trip Transient

3. Application of MAAP5 for shutdown SAMG development

The MAAP5 code has capabilities to model mid-loop operations and shut down conditions with the reactor head open and the vessel submerged under the refueling water pool with nozzle dams in place. The following examples were performed for a Zion-like Westinghouse 4-loop plant to demonstrate the effectiveness of operator actions during the severe accident from shut-down conditions:

Case 1 (base case):

- 120 hours since the reactor scram.
- Reactor head open and the vessel submerged with 2 m of water above it.
- Nozzle dams in place in all loops.
- Nozzle dam failure (large LOCA) in loop 1.
- No injections, no containment sprays, and no RHR cooling available.
- Containment is isolated with a leakage area of 3.35E-6 m^2.

Case2:

- Same conditions as base case.
- LPI (suction from containment sump) start at 20,000 seconds.

Case 3:

- Same conditions as base case.
- Containment spray (suction from containment sump) is started at 20,000 seconds.

In all cases, the core is uncovered at 13,040 seconds. Figure 8 shows the two-phase level in the core within the core boundary. Because of low decay heat, the two-phase level decreases very slowly. When the spray is on, the containment spray water is collected in the refueling pool floor and spilled into the reactor vessel because the reactor head is open. The hottest core node temperature and the mass of hydrogen generated are shown in Figures 9 and 10. In these cases, the Zr oxidation with steam and air are both modeled. To see the effect of the operator actions, the dose rate at the exclusion area boundary (EAB) is compared and shown in Figure 11. As shown in this figure, the dose rate at the EAB is reduced when containment sprays or LPI are started.

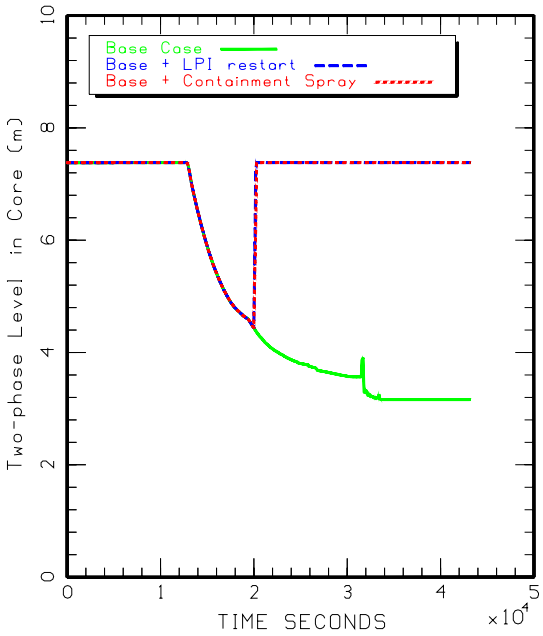


Figure 8, Comparison of two-phase level in the core region

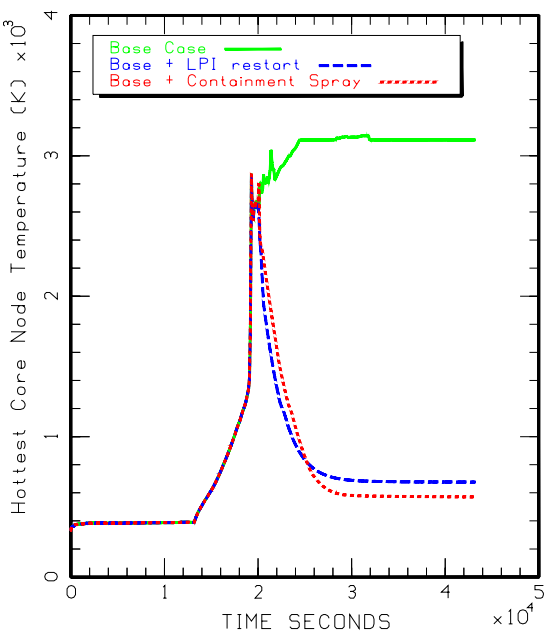


Figure 9, Comparison of hottest core node temperature

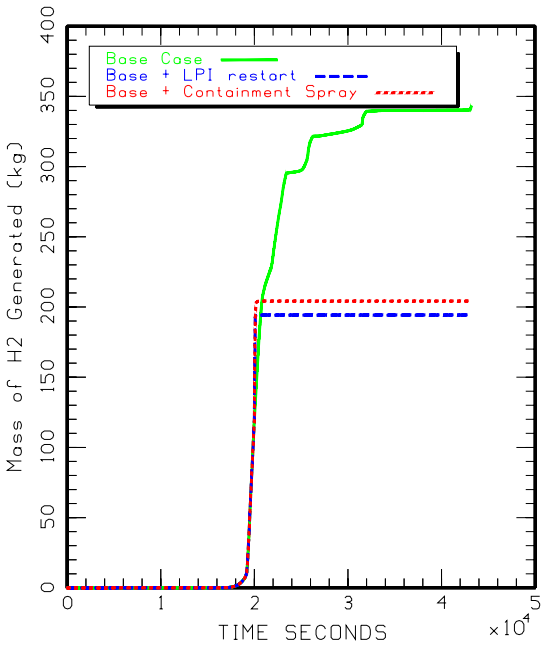


Figure 10, Comparison mass of hydrogen generated

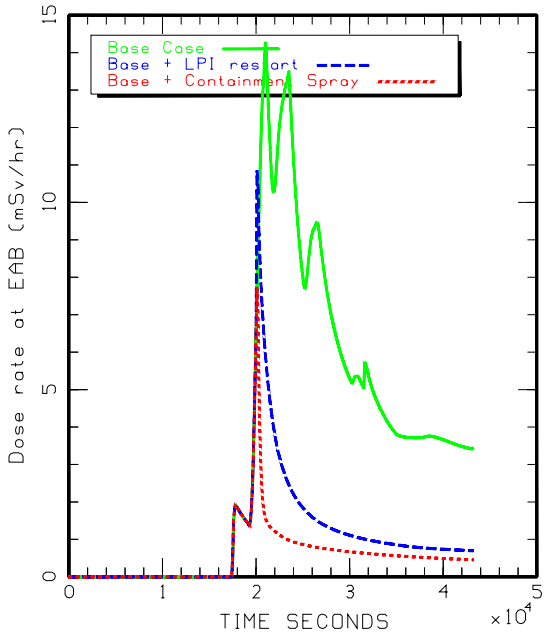


Figure 11, Comparison of dose rate at exclusion area boundary (EAB)

4. Applications of shutdown MAAP5 analyses and pra insights to development and implementation of full scope SAMG covering all plant operating states

4.1 Risks during Low Power and Shutdown States

Why be concerned about shutdown states? The first MAAP analyses and probabilistic safety assessments (PSAs) performed on nuclear power plants (NPPs) considered only accident sequences which could occur when the NPP is operating at full power, with the implicit assumption that during shutdown the risk is much lower. The focus of formal safety assessments of NPPs is a selection of representative incidents and accidents, analyzed under conservative assumptions, in order to justify design features like automatic safety systems. One of these conservative assumptions is that operators must have at least a 10 minute (after the recognition of an incident/accident) "grace period" before any manual control will be required. Within this period of time, all modifications of plant status – if needed – must be automatic. This philosophy explains why several plant states during shutdown were not formally assessed, based on the much slower dynamics, as only decay heat is present (no nuclear power). However, due to several incidents experienced in NPPs during shutdown in many countries, the first Probabilistic Safety Assessments (PSAs) were carried out in USA and France to investigate the risk of core melt when the reactor is in a shutdown condition. Later on, these results were confirmed by similar studies carried out in other countries.

The results of the MAAP5 analyses and shutdown PSAs are largely identical and can be summarized in a few words as follows. Any increased risks during low-power and shutdown (LP&S) states mainly result from:

- the reduced availability of systems;
- the comparatively small amount of coolant during certain phases;
- the lack of automatic measures to control abnormal events;
- the lower quality of Emergency Operating Procedures (EOP) and lack of Severe Accident Management Guidelines (SAMG);
- the considerably increased difficulty – compared with power operation – of monitoring and keeping track of plant states;
- the fact that many maintenance and inspection activities take place at the same time.

The PSA investigations have demonstrated that the original idea of negligible risk during shutdown because of a large grace time is not valid for all states. Practically all shutdown PSAs have shown that the shutdown risk always lies within the same order of magnitude as that of power operation and often even clearly exceeds the latter: the core damage frequency (CDF) per reactor-year while at shutdown or low power is approximately 1/4 of the total CDF for PWR and goes up to 3/4 for VVERs.

These findings could be explained by several reasons. In many accidental situations, operator intervention is necessary, in cases where alarms, indicators and operating procedures are poor or absent. The greatest challenge comes from the possibility of simultaneous unavailability of equipment causing the loss of a given safety function. During an outage, the role of the operations staff changes considerably when compared with full power operation. The operating circumstances are more demanding, the work more intensive, and shift turnovers more difficult. More reduced coolant inventory operations were identified as presenting the greatest challenge to the operator.

The applicability of existing severe accident management guidance to shutdown states was evaluated and found to be inadequate. Accident Management Procedure/Guidelines improvements were required to achieve a balance between the risks resulting from power operation and low power & shutdown states.

In addition to the findings related to plant safety, the PSAs have underlined that in many cases, the knowledge of the plant behaviour during an accident sequence was insufficient.

4.2 Westinghouse SSAMG Development Process

In order to attempt to resolve this issue, Westinghouse has developed the Shutdown Severe Accident Management Guidance (SSAMG) (WENX-97-06) which gives guidance for both control room and TSC personnel to mitigate a severe accident under shutdown or low power conditions.

The general approach that was chosen consists in extending the existing SAMGs (At-power) for use during low power or shutdown conditions. Therefore the current SAMG package has been reviewed and the necessary changes and additions were identified. The following ground rules were set and robustly maintained:

- The SSAMGs are an extension of the existing SAMGs. Thus, the approach is to extend the range of applicability of the SAMGs,
- The WOG SAMGs are symptom based, primarily because in a severe accident it is difficult to identify which events caused the severe accident. For shutdown conditions, the number of possible plant configurations is larger, therefore it is even more important that the SSAMGs are symptom based;
- The SSAMGs should as far as possible be applicable to all Plant Operational States (POS). Severe accidents could occur and may be more likely to occur during the transition from one POS to another.
- The potential damage of spent fuel in the spent fuel pool/storage is considered in the SSAMGs.
- As large scale maintenance is frequently carried out during planned shutdown states, the first concern of SSAMGs is the safety of the workforce.
- Shutdown severe accident management covers also external events, such as fires, floods, seismic events and extreme weather conditions that could damage large parts of the plant, as well as specific challenges posed by external events, such as higher probability of loss of the power supply, loss of the control room and reduced accessibility to systems and components.

The development of SSAMG is multi-step process. The first step reviews the Plant Operating Technical Specifications (OTS) and Shutdown Level 1 and Level 2 PSAs with the objective of defining the characteristics of different Plant Operational States. This includes:

- the different plant thermal-hydraulic states,
- different instrumentation and control configurations,
- the status of containment isolation,
- the location of the fuel,
- the level and volume of water in the primary system,

- availability of vent paths in the primary system,
- available safety and other systems,
- whether the vessel head is in place or not, and
- the conditions during changes from one state to another.

The starting point of this investigation is the definition of the POSs and comparison to the OTS modes of operation. To ensure the validity of the SSAMGs, the POSs are used during the development process, but the final presentation is according to the OTS operating modes.

The second step involves the review of the MAAP5 accident analyses and Shutdown PSAs to gain insights with regard to:

- dominant accident sequences and initiators,
- vulnerable plant states,
- time to boiling, time to core damage, and time to containment failure,
- consequences of core damage, and
- the symptoms of severe accident phenomena.

The third step involves reviewing the existing emergency operating procedures. The objective of this review is to identify:

- changes required to OTS and the Shutdown Emergency Operating Procedures (Shutdown EOPs) to accommodate the SSAMGs,
- identify conditions for entry into SSAMG for accident sequences not covered by Shutdown EOPs, and
- identify appropriate kick-outs from Shutdown EOPs to the SSAMGs.

In step 4, the SAMG diagnostic flow charts (DFC) and SCSTs are evaluated for shutdown conditions. The following issues are investigated for each of the POSs defined in Step 1:

- identify relevant phenomena and available or relevant diagnostic parameters (e.g. induced SGTR cannot occur when the vessel head is removed),
- identify the available instrumentation to measure the diagnostic parameters (e.g. are the core exit thermocouples available),
- determine the priority of diagnostics for each POS,
- define structure of DFC and SCST applicable to all POSs,
- verify the parameters and measurement for the definition of a controlled stable containment and core state.

In Step 5, this step involves an assessment of the existing SACRGs, SAEGs, SAGs and SCGs for shutdown conditions:

- identify applicable SAGs and SCGs,

- for each of these identify additional systems, negative impacts, limitations and long term concerns,
- define any new guidelines that may be required.

In Step 6, the applicability of computational aids (CA) is assessed.

- check which computational aids are applicable,
- identify any required modifications (such as the extension of duration for decay heat estimation),
- identify any new computational aids.

In Step 7, identify in a concise way the essential changes to the SAMGs and document the elements of the complete package.

Over the past few years Westinghouse applied these principles and generic guidelines to develop plant-specific SSAMGs for several utilities with different reactor types.

Severe accident management consists of mitigative actions after core damage has occurred. However, a comparison of the operating states of the different reactor types indicates some common points of distinction:

- The first common OTS distinction is based on whether the SGs or RHR is being used for decay heat removal during hot shutdown. Some plants do not have “primary” RHR system and use steam generators for decay heat removal in different modes (like “water-steam” or “water – water”).
- The second common distinction is based on whether the primary system is full or partially drained during RHR operation. The level at the onset of the accident leading to core damage is not significant with regard to severe accident mitigation except with regard to time to core damage.
- The third common distinction is based on containment status. Whether or not the containment is open able to be isolated is important for SSAMGs. An open containment during shutdown states involves all the plant configurations (with the core inside the reactor vessel) for which the confinement function of the containment cannot be guaranteed in connection with maintenance work inside the containment.
- The fourth common cut-off considers whether the vessel head is in place or not. Whether or not the primary system contains large openings is significant for SSAMGs.
- The fifth considers whether the fuel is in the vessel or not. The location of the fuel is significant for SSAMGs. If the fuel is in the spent fuel pool rather than in the reactor, different actions are required.

Transition criterion from EOP to SAM is one significant challenge for Shutdown States (WCAP-14696). The most suitable criterion for transition from EOPs to SAMs is the “onset of core damage”. A suitable, unambiguous and easily used symptom which indicates that core damage is imminent or occurring is therefore required.

Over the years, different plant parameters and conditions have been considered for performing this function of recognizing the onset of core damage. Candidates include core (fuel assembly) coolant outlet temperature (referred to here as core exit temperature or CET), containment radiation levels, and containment hydrogen concentration and/or reactor vessel level.

Some of these (especially those using containment parameters) are very sensitive to the specific accident scenario (i.e., the value at the onset of core damage for one scenario may vary significantly from that for another, for example due to the influence of sprays and fission product deposition phenomena). Also, all have some range of uncertainty that must somehow be considered. On the other hand, for applications in emergency response, clear, easy to use tools and symptoms are preferred as they do not require lengthy and complex evaluations to be performed as a pre-requisite to decision making. In addition, assessments should not involve undue conservatisms (for example, it is inappropriate to transition from EOPs to SAMGs either too early or too late by including conservatism in the evaluation and definition of a symptom's setpoint).

Different accident management approaches may define "core damage" somewhat differently, but the fundamental concerns are overheating of the fuel and clad, and the onset of significant Zr oxidation in the steam or steam-air environment of the uncovered fuel. The most direct parameter to use to detect this condition would be fuel or cladding temperature. Since it is not possible to directly measure the cladding temperature, a suitable alternative, as directly related to clad temperature as possible, must be used.

PWR/VVER plants use thermocouple instrumentation to measure the temperature in the coolant channel at the exit of the fuel assemblies. They provide a direct measurement of coolant temperature, and are rugged, qualified instruments, with a large range and suitable accuracy. Many approaches to accident management use the CETs as a key input to detecting the onset of core damage. Since core exit temperature is not a direct measure of clad temperature, its use does suffer to some extent from the disadvantage that a given fuel/clad temperature limit may be reached at a range of different CET readings, depending on the accident scenario. However, the effect is less important than would be the case with the use of alternatives to the CETs. This is for two reasons:

- thermal hydraulic behaviour of the core and core exit region is reasonably well understood, and MAAP5 models are good,
- though fuel and clad temperatures may vary depending on the accident scenario once a certain value of core exit temperature is reached, such variation is reasonably limited, and is also well understood. In particular, there is a relatively strong dependence on system pressure, therefore, the option always exists to make the setpoint a function of pressure, or to select "high" and "low" pressure values to address this, rather than using a single value.

Whether this is done is a decision based on a balance between increased complexities in usage, and increased precision.

Different approaches use a combination of methods and parameters, although core exit temperature is usually a key input. In most PWR/VVER designs, the core exit thermocouple passes through the primary system pressure boundary at the reactor vessel head. When the head is removed for refuelling operations, the thermocouples must be disconnected. Some plants re-connect a limited number of thermocouples following reactor vessel head removal, but this is by no means common practice, and when it is done, functionality is usually very limited. It is common for the plant to have no CETs available between the time of removal and replacement of the head during the refuelling cycle.

In case of an accident occurring when the CETs are unavailable, an alternative indication of onset of core damage is therefore required.

Given that the core exit temperature is not available, various alternative plant parameters have been considered (and in some cases used) in the past. All suffer from disadvantages of various types. Examples include:

Containment radiation: the method consists of calculating the expected radiation instrumentation response to a severe accident at the time when the core exit temperature reaches the (no longer measurable) value used for the at-power transition. This has been done for several plants (PWR and VVER).

However, it should be noted that such a calculation is expected to be sensitive to numerous event specific characteristics, including:

- whether the RV head has been removed or not (even if short, there must be a time window after removal of thermocouples but before head removal),
- accident initiator (especially openings or not in the RCS, for example LOCAs versus transients),
- the status of the RCS injection system,
- the status of the containment spray system,
- shielding effects at the detector and detector location,
- deposition of fission products.

In addition, the calculation of the expected response is not straightforward.

In spite of these disadvantages, this is the parameter that has always been chosen for SAM packages which do address shutdown.

An example of containment radiation criteria used for VVER plants is shown in Figure 12.

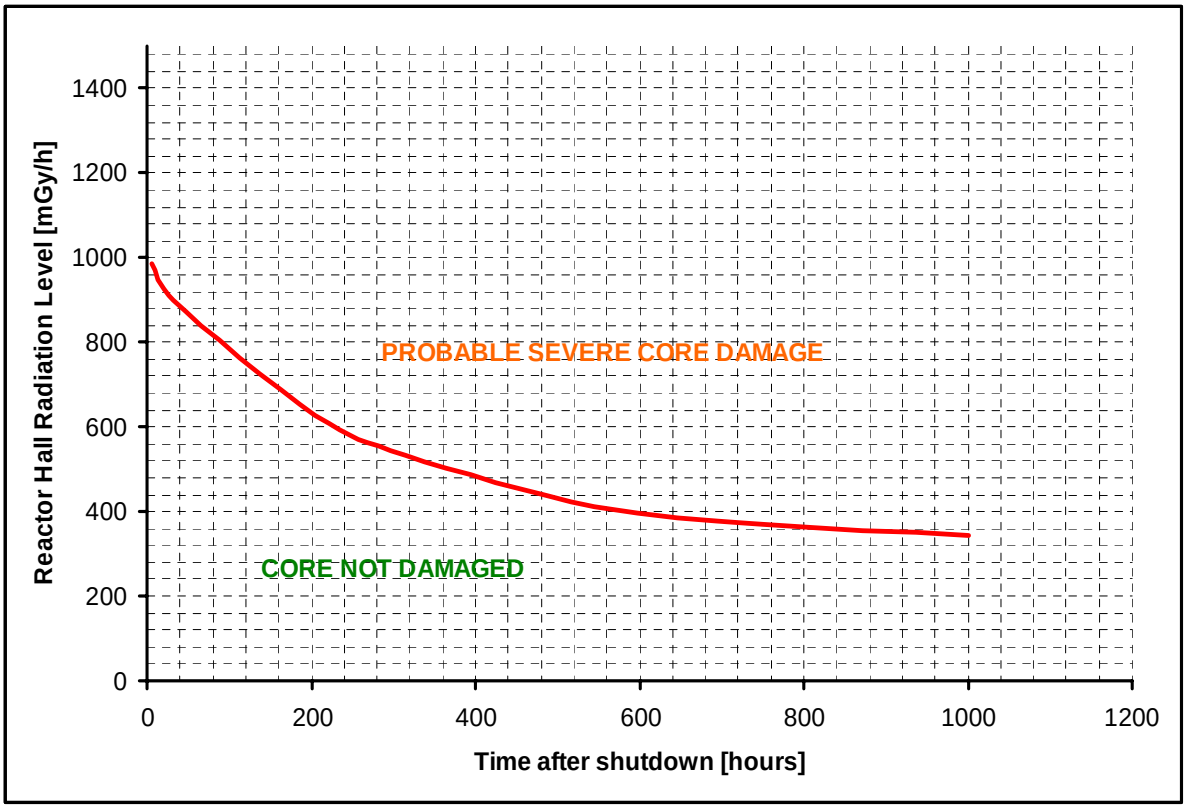


Figure 12
Radiation level in the Reactor Hall versus time after shutdown

Vessel water level: vessel level (if available) could also be correlated to core exit temperature, and is sometimes used as a "backup" parameter.

Disadvantages tend to be system-related, and therefore depend on the plant specifics; however, typical problems include:

- insufficient range,
- need for thermocouples (which are not available),
- difficulties in interpretation of output (some systems),
- doubts about survivability.

Containment hydrogen: in principle, measurement of hydrogen concentration in containment (if available) could be correlated to core conditions. However, the main problem here is that the response is too slow when there is no large opening in the RPV. By the time a measurable hydrogen concentration is reached, core conditions will be much more severe than those used to define the at-power transition core outlet temperature. In addition, the response is sensitive to the type of event (especially the availability of pathways for hydrogen to escape from the primary system to the containment), and on the presence or not of openings due to the plant state. Confidence in the survivability and accuracy of the instrumentation during a severe accident is a concern. Furthermore, if the plant is equipped with Passive Autocatalytic Recombiners, these may "mask" the symptom.

Ex-core neutron flux: the absence of shielding caused by reducing water level could be used to indirectly infer vessel level, and hence core conditions. However, there has never been sufficient confidence in the ability to predict unambiguously the instrumentation readings which indicate onset

of core damage (or rather determine a "universal setpoint"). Additionally, as for containment hydrogen, survivability and accuracy of the instrumentation during a severe accident is a concern.

The structure and prioritization of the diagnostic tools (DFC and SCST) were significantly modified based on key Shutdown PSA insights:

- The operating modes Power Operation, Startup, Hot Standby and Intermediate Shutdown (with steam generators in service and RHR not aligned for service) are equivalent from a severe accident management point of view, and the At-power SAMG package is applicable.
- The first diagnostic distinction required if "RHR is in Service" during Intermediate/Hot Shutdown. If RHR in service/ aligned for service, the Shutdown SAMG must be used.
- The second diagnostic consideration is the primary system integrity. If the vessel head is removed, nozzle dams are installed, pressurizer relief valves removed, or other large openings exist, it is unlikely that the primary system would pressurize, and the priorities in the DFC change (see Figure 13). There is no need to inject into the steam generators or depressurize the primary system. For most PWR reactors, the SGs cannot be used for cooling, however for VVERs the SG is used in "water-water" cooling mode, there is no risk of tube creep rupture, and the primary system pressure will be low.
- The third diagnostic distinction is the containment integrity. During cold shutdown and refueling containment integrity should be prioritized. A severe accident occurring during cold shutdown leads directly to a fission product release severe challenge.
- The location of the fuel has an impact on the diagnostic prioritization. If the fuel is in the vessel, in the refuelling cavity, or in the spent fuel pool, the priorities are different and different SAM actions are required.
- During RHR operation in cooling mode, core damage is possible in less than one hour. This implies the need for control room guidance for these accidents, because the TSC will not be active yet. New control room guide/guides development was required.
- To accommodate shutdown states, only a few SAGs were modified and one new SAG was developed to address spent fuel pool accidents. One new computational aid was also developed. Figure 13 provides an example of a Diagnostic Flow Chart for a VVER plant for all (At-power and Shutdown) plant states.

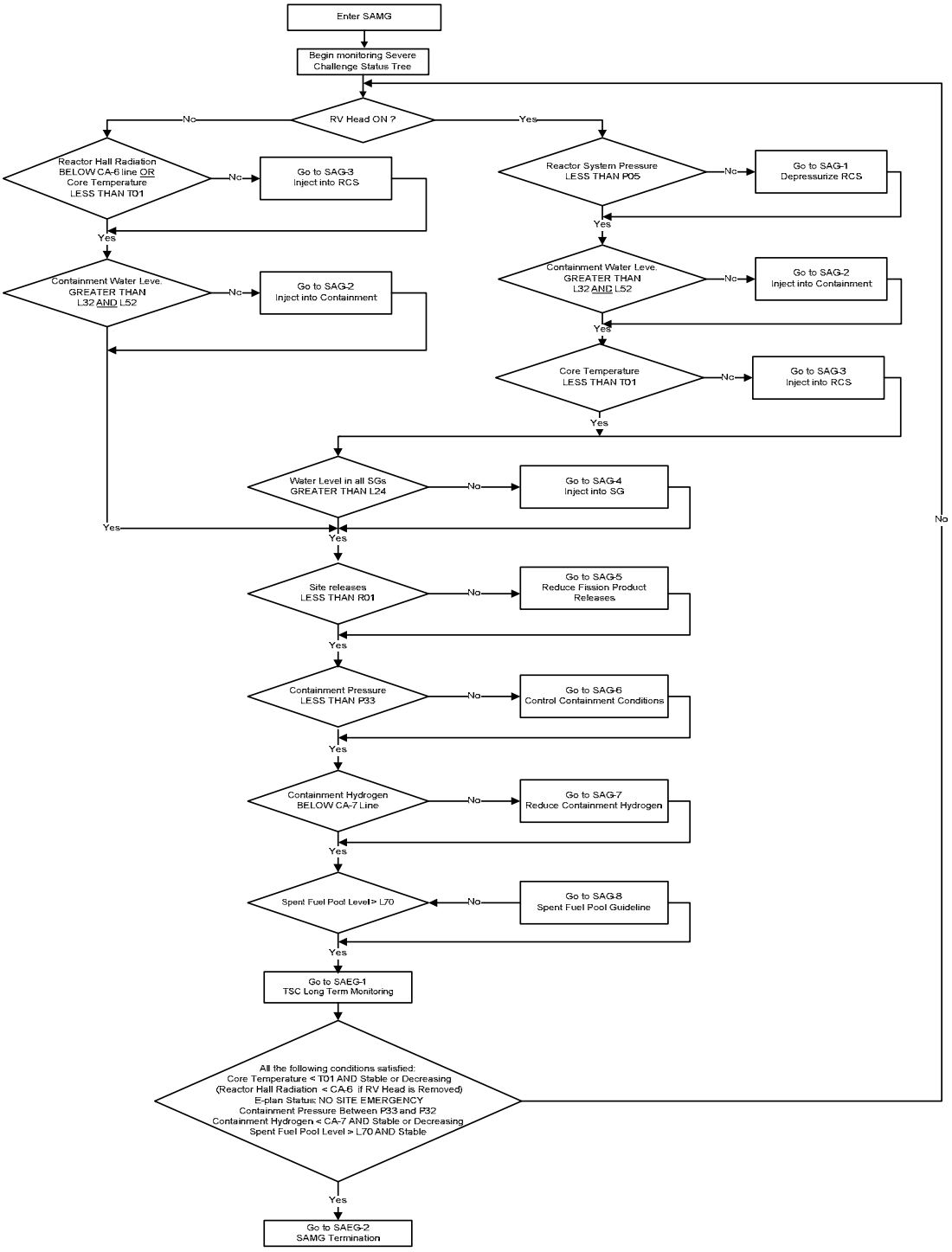


Figure 13 Diagnostic Flow Chart

5. Summary

Major improvements have been made in the latest MAAP5.0.1 code to simulate initial transients and shutdown conditions in nuclear power plants. The capabilities of the MAAP code simulating non-severe accident transients are demonstrated with selected AP1000 transients. Comparisons of the manual reactor trip case between MAAP5 and RELAP5 demonstrate that MAAP5 can predict RCS performances with satisfactory accuracy. The power ramp case shows that MAAP5 is capable of simulating nuclear feedback cases, while the single RCP trip cases shows MAAP5's capability to study asymmetric configurations of SG loops. With these new capabilities, MAAP5 is considered an appropriate tool for severe accidents and for following the Shutdown SAMG development steps:

- Definition of timing of events;
- Definition of recovery actions and success criteria;
- Definition of SD EOP-SAMG transition;
- Definition of setpoints (DFC, SCST, and SAG/SCGs entry, exit, transition);
- Definition of the End State – Controlled Stable State;
- Definition of Accessibility (or inaccessibility) plants compartments (CR, Electrical building, NAB, Turbine Hall, and etc.) and equipment;
- Definition of SAMG- Emergency Plan interface;
- Development SAMG Training Scenarios;
- Interactive TSC and CR personnel training.

MAAP5 is also capable to execute long term non-severe accident transients and PRA level I success criteria calculations.

Due to the flexibility and high adaptability of the Westinghouse At-power SAMGs, they can be modified and extended to effectively cover all plant operating states for different PWR (Westinghouse, AREVA, and Siemens) and VVER plant designs. Comprehensive Shutdown PSA is a key pre-requisite for successful Shutdown Accident Management development.

Procedures for Accident Management during shutdown (EOPs, SAMGs for shutdown modes) represent very cost effective measures to improve shutdown safety. After implementation of a Shutdown Accident Management program, the shutdown core damage frequency is expected to be lower than the CDF from power modes and is mainly dominated by human error rates.

During shutdown modes, several conditions are favourable with respect to restoration of core cooling by alternate Accident Management measures such as mobile equipment. Shutdown risk with respect to large early releases is mainly dominated by scenarios with failure or impossibility to reclose the containment equipment hatches or airlocks.

There are specific challenges to thermal-hydraulic codes for low power and Shutdown plant states; verification of codes, model modifications and improvements required for:

- Small system pressure,
- Small pressure differences,
- Influence of non-condensable gases,

- Low velocity boron transport,
- Large volume mixing,
- Spent Fuel Pools (High Density Racks) accidents.

Regarding the severe accident phenomenology, the remaining uncertainties, and also the diversity of accident scenarios considered, the development of Shutdown SAMG is still a very complex activity.

For SSAMG validation, operator and TSC training exercises and upgrades to Full Scope Simulators are required to support high fidelity simulation of shutdown states, including low reactor inventory states, open reactor and open containment states, refueling operations, and spent fuel pool accidents.

6. Reference

[1] OREGON STATE UNIVERSITY, Quick look report for OSU matrix test SB12, 14, 26, 28, AP600 test program. LTCT-T2R-032, 034, 046, 048, Westinghouse Electric Co., 1994

[2] BARBENSI, A., NOTINI, V., FROGHERI, M., Emergency response guideline (ERG): AES-0.1, AP1000 Reactor Trip Response Analysis, APP-GW-GJA-206, Westinghouse Electric Co., 2005

[3] IAEA Safety Standards, “Severe Accident Management Programs for Nuclear Power Plants, NS-G-2.15”.

[4] WENX-97-06, “Shutdown Severe Accident Management Guidance”.

[5] WCAP-14696, “Core Damage Assessment Guideline”.

[6] MENDLER, O.J., et al. 1986, “Loss of Feed Flow, Steam Generator Tube Rupture, and Steam Line Break Thermohydraulic Experiments.” NUREG/CR-4751. EPRI NP-4786. WCAP-11206.

MAA5 Modeling Capabilities for Initial Plant Transients and Shut-down State, and Application to Shutdown PSA and Full Scope SAMG Covering All Plant States for Operating and New Plants

FAUSKE & ASSOCIATES, LLC

C.Y. Paik[1], O. Solovjanov[2], Q. Zhou[1], S.J. Lee[1],
R.W. Reeves[1], R.E. Henry[1]
W. Luangdilok[1]
[1]Fauske & Associates, LLC
Burr Ridge, IL
[2]Westinghouse Electric Belgium
1400 Nivelles, Belgium

OECD/NEA Workshop June 20-22, 2011

16W070 83RD STREET • BURR RIDGE, ILLINOIS 60527
(877) FAUSKE1 OR (630) 323-8750 • FAX: (630) 986-5481 • E-MAIL: INFO@FAUSKE.COM

INTRODUCTION

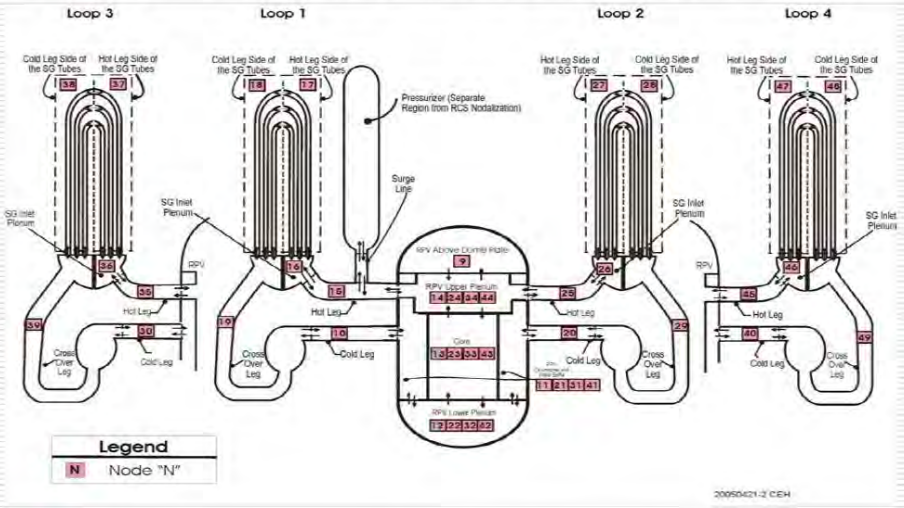
- MAAP4 has been known for nearly three decades as a tool for integrated severe accident analysis for LWRs.
- Over these years, incremental code improvements in MAAP4 have been introduced resulting to several code revisions.
- MAAP5.01 is the culmination of several major improvements in the PWR RCS thermal hydraulics model that bring the code applicability range closer to the PWR DBA regime while retaining all severe accident analysis capabilities.
- This purpose of this paper is to demonstrate the capability of MAAP5.01 in the simulation of reactor transients that normally would be analyzed by the DBA code such as RELAP5.

Major Improvements in MAAP5 over MAAP4

System Model	MAAP5.01	MAAP4
PWR RCS	Individual major system components are modeled including all hot and cold legs, surge line, steam generators, RCPs, etc.	Modeled as different two loops: "broken" and "unbroken" loops.
BWR RPV	Same	same
PWR Main Steam Header	SG interactions such as during MSL break.	N/A
Core neutronics	Point kinetics and 1-d diffusion model for PWR, 1-d diffusion model for BWR	N/A
Containment Model	Applicable to DBA analysis: single node or multi-node.	Not for DBA analysis
Radiation dose	Dose and dose rate for containment, auxiliary building, reactor building, control room. Alternate source term methodology	N/A
Molten-pool RPV lower-head model	Applicable for IVR evaluations	N/A

MAAP5 Nodalization of 4-Loop PWR RCS

Individual hot legs and cold legs of all loops are modeled

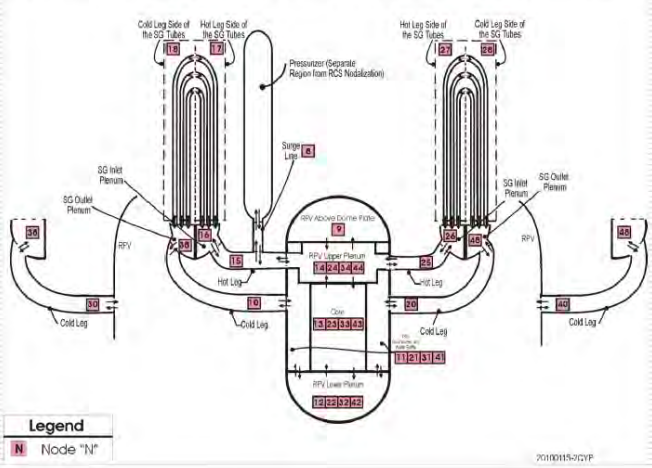


FAUSKE & ASSOCIATES, LLC

OECD/NEA Workshop June 20-22, 2011

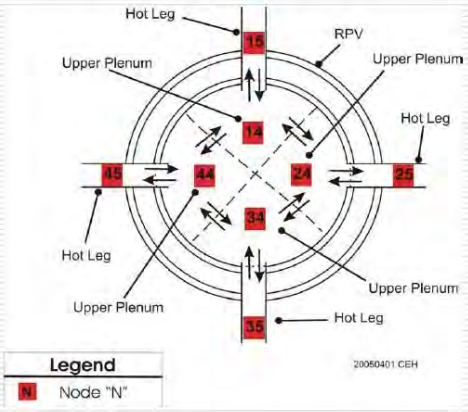
MAAP5 Nodalization of 2-Loop 4-cold-leg PWR RCS

Individual hot legs and cold legs of all loops are modeled



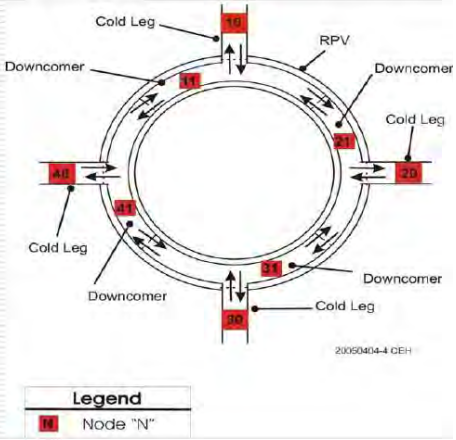
Short-Circuit Flow between hot legs

is allowed

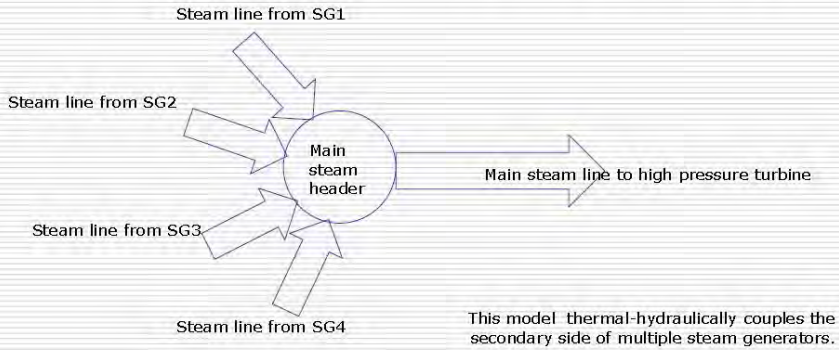


Short-Circuit Flow between cold legs

is allowed



Main Steam Header Model



This model thermal-hydraulically couples the secondary side of multiple steam generators.

FAUSKE & ASSOCIATES, LLC

OECD/NEA Workshop June 20-22, 2011

AP1000® Manual Reactor Trip

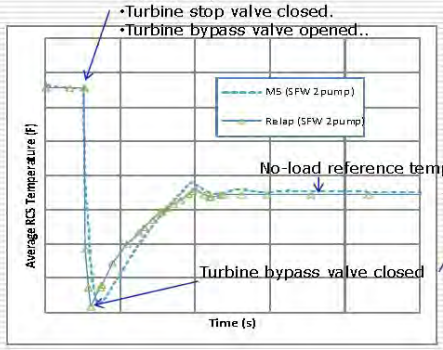
- A reactor trip signal is initiated after a period of steady-state operation.
- Once the signal is received, all shut-down (SD) bank control rods are automatically dropped into the core to trip the reactor.
- The turbine stop valve is closed a few seconds after the reactor trip signal is received to isolate the main steam line.
- Main feed water (MFW) is shut off abruptly after receipt of a reactor trip signal and start-up feed water (SFW) is assumed to start immediately.
- Once the reactor is tripped, a reference no-load temperature is set, and the steam dump system automatically opens the turbine bypass valves to control SG pressures and allows the RCS temperature to match the no-load temperature.

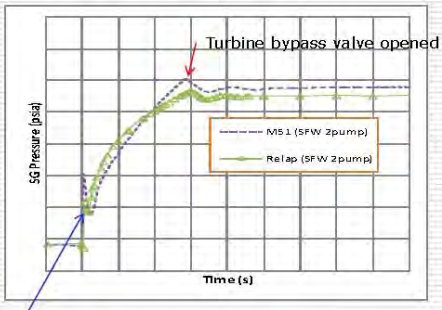
FAUSKE & ASSOCIATES, LLC

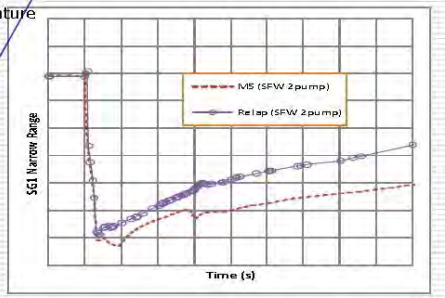
OECD/NEA Workshop June 20-22, 2011

AP1000® Manual Reactor Trip MAAP5.01 vs. RELAP5 (Barbensi, 2005)

•Reactor trip
•Turbine stop valve closed.
•Turbine bypass valve opened..





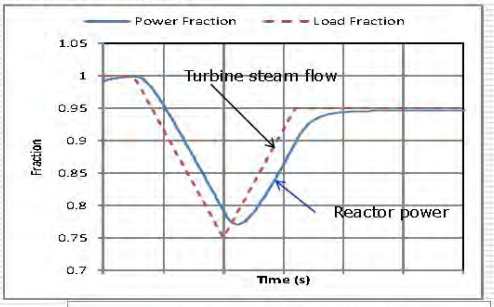


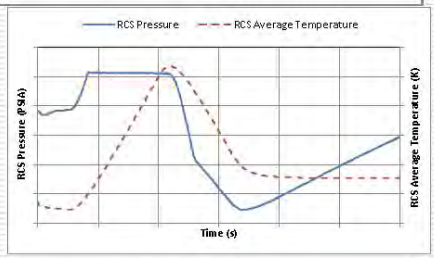
FAUSKE & ASSOCIATES, LLC

AP1000® Turbine Load Following

Maximum Power Ramp-up

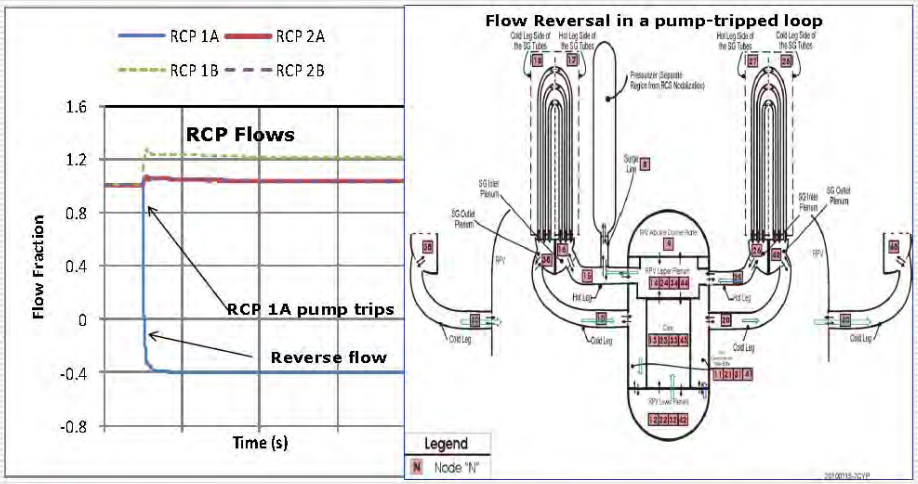
•Transient starts with a reduction of turbine load at rate of 5% per minute to 75% of the nominal load.
•The load then starts to increase at a rate of 5% per minute from 75% to 95%, and the reactor operates at the 95% flow rate for 1 hour.
•As the turbine load changes, reactor power is expected to follow the load change through a nuclear feedback without actuating reactor trip or protection systems.
•During the power ramp, the reactor power responds to the load change only through reactivity feedback mechanisms (Doppler and moderator temperature coefficients).
•The power follows the flow rate change as expected with a slight delay time .
•Peak RCS temperature and pressure are lower than the set-points to trip the reactor.



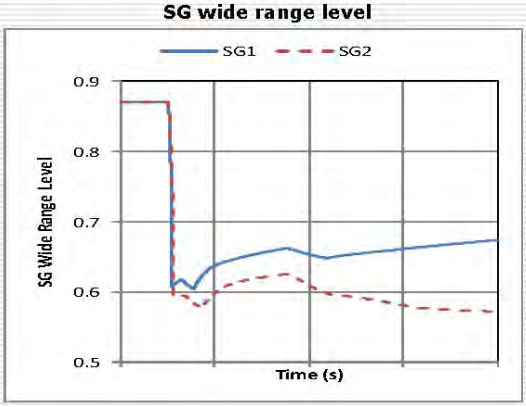


FAUSKE & ASSOCIATES, LLC

AP1000® Trip of Single Reactor Coolant Pump



AP1000® Trip of Single RCP -continued



Reverse flow in loop1 bring less hot coolant to SG in loop1. This leads to
(1) less heat transfer through SG1
(2) less boiling in SG1 and
(3) higher water level in SG 1

Application of MAAP5 for Shutdown SAMG Development

- MAAP5 can model plant shutdown conditions including mid-loop operation and RPV opened-head condition with water filled the refueling pool.
- MAAP5 can model the nozzle dam placed in individual loops.
- MAAP5 can model air or nitrogen injection into the pressurizer during initial shutdown.
- MAAP5 can calculate containment radiation.

FAUSKE & ASSOCIATES, LLC OECD/NEA Workshop June 20-22, 2011

Risks during Low Power and Shutdown States

- Reduced availability of systems;
- Relatively small amount of coolant during certain phases;
- Lack of automatic measures to control abnormal events;
- Lower quality of Emergency Operating Procedures (EOP) and lack of Severe Accident Management Guidelines (SAMG);
- Considerably increased difficulty – compared with power operation – of monitoring and keeping track of plant states;
- Many maintenance and inspection activities take place at the same time.

FAUSKE & ASSOCIATES, LLC OECD/NEA Workshop June 20-22, 2011

Shutdown Risk

- Practically all shutdown PSAs have shown that risk always lies within the same order of magnitude as that of power operation and for some cases exceeds:

  Core damage frequency (CDF) per reactor-year
  ~ **1/4** of the total CDF for PWR,
  and up to **3/4** for VVER.

Westinghouse Shutdown SAMG

- **Westinghouse** has developed the Shutdown Severe Accident Management Guidance (**SSAMG**) which gives guidance for **both** CR and TSC personnel to mitigate severe accidents under shutdown conditions.

Shutdown SAMG - Ground Rules

Ground rules were set and robustly followed:

- The Shutdown SAMG (SSAMG) is **an extension** of the existing SAMG package - the approach is to broaden the range of applicability of the SAMG package;
- The Westinghouse SAMG is symptom based, primarily because in a severe accident it is difficult to identify which events caused the severe accident. For shutdown conditions, the number of possible plant configurations is larger, therefore it is even more important that the **SSAMG is symptom based**;

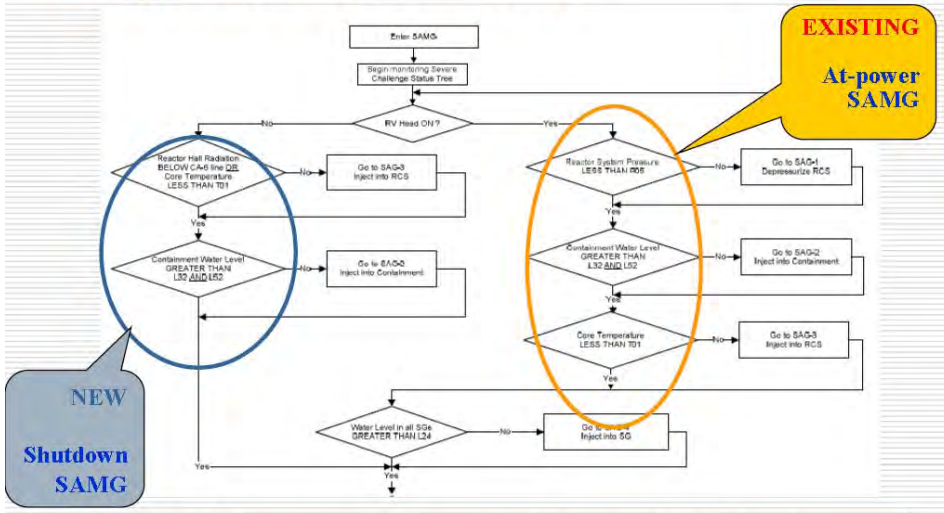
FAUSKE & ASSOCIATES, LLC OECD/NEA Workshop June 20-22, 2011

Shutdown SAMG - Ground Rules

- The **SSAMG** should as far as possible be applicable to all Plant Operating States (POS). Severe accidents could occur and more likely to occur during the transition from one POS to another.
- The potential damage of spent fuel in the spent fuel pool/storage is considered in the **SSAMG**.
- As large scale maintenance is frequently carried out during planned shutdown states, the first concern of **SSAMG** is the safety of the workforce.

FAUSKE & ASSOCIATES, LLC OECD/NEA Workshop June 20-22, 2011

Example of Shutdown SAMG – Diagnostic Flow Chart



Development of Shutdown SAMG

- Over past few years Westinghouse applied these rules to develop plant-specific SSAMGs for several utilities with different reactor types.
- One significant challenge is the choice for transition criterion from EOP to SAM.
- The most suitable criterion is the onset of core damage.
- Different plant parameters and conditions have been considered for performing this function of recognizing the onset of core damage.
- Candidates include core coolant outlet temperature (referred to here as core exit temperature or CET), containment radiation levels, and containment hydrogen concentration and/or reactor vessel level.

Core Damage Diagnostic for Shutdown SAMG when CETs are unavailable

In case of an accident occurring when the CETs are unavailable, an alternative indication of onset of core damage is therefore required.

All suffer from disadvantages of various types. Examples include:

- Containment radiation;
- Vessel water level;
- Containment hydrogen;
- Ex-core neutron flux.

FAUSKE & ASSOCIATES, LLC OECD/NEA Workshop June 20-22, 2011

Core Damage Diagnostic for Shutdown SAMG when CETs are unavailable

Containment radiation:

The method consists of calculating the expected radiation instrumentation response to a severe accident at the time when the core exit temperature (CET) reaches the (no longer measurable) value used for the at-power transition. This has been done for several plants (PWR and VVER).

However, it should be noted that such a calculation is expected to be sensitive to numerous event specific characteristics, including:

FAUSKE & ASSOCIATES, LLC OECD/NEA Workshop June 20-22, 2011

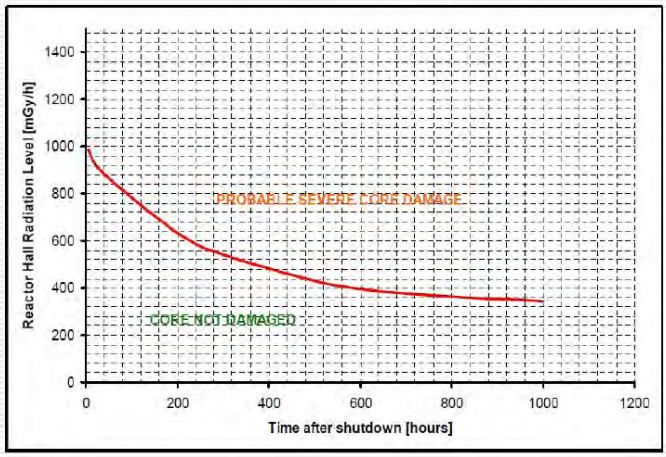
Core Damage Diagnostic for Shutdown SAMG using Containment Radiation

- whether the RV head has been removed or not;
- accident initiator (especially openings or not in the RCS, for example LOCAs versus transients);
- the status of the RCS injection system;
- the status of the containment spray system;
- shielding effects at the detector and detector location;
- deposition of fission products;

In spite of these disadvantages, this is the parameter that has always been chosen for SAM packages that do address shutdown.

FAUSKE & ASSOCIATES, LLC OECD/NEA Workshop June 20-22, 2011

Example of Containment Radiation for Core Damage Criteria used in VVER Plants



FAUSKE & ASSOCIATES, LLC OECD/NEA Workshop June 20-22, 2011

Application of MAAP5.01 for Shutdown SAMG Development

- MAAP5 analyses of shutdown severe accidents provide insights with regard to:
  - dominant accident sequences and initiators,
  - vulnerable plant states,
  - time to boiling, time to core damage, and time to containment failure,
  - consequences of core damage, and
  - the symptoms of severe accident phenomena.

Example of MAAP5.01 Analysis of Shutdown Severe Accident for Zion-Like PWR

Case 1 (base case):

- 120 hours since the reactor scram.
- Reactor head open and the vessel submerged with 2 m of water above it.
- Nozzle dams in place in all loops.
- Nozzle dam failure (large LOCA) in loop 1.
- No injections, no containment sprays, and no RHR cooling available.
- Containment is isolated with a leakage area of 3.35E-6 m^2.

Case2:

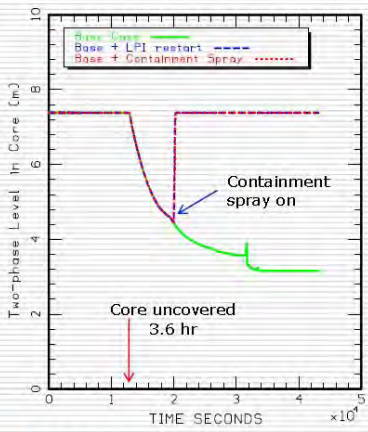
- Same conditions as base case.
- LPI (suction from containment sump) start at 20,000 seconds.

Case 3:

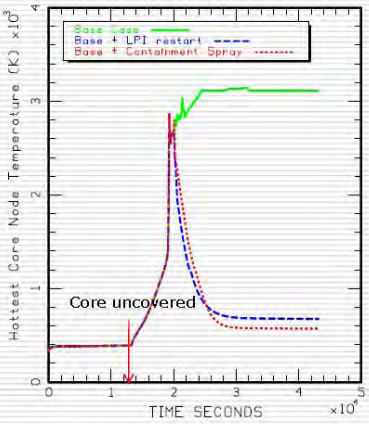
- Same conditions as base case.
- Containment spray (suction from containment sump) is started at 20,000 seconds.

Severe Accident from Shutdown Conditions

Core water level



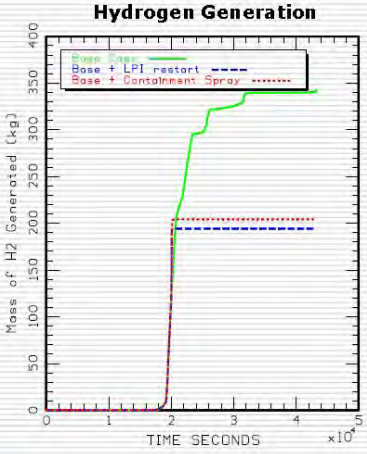
Maximum core Temperature



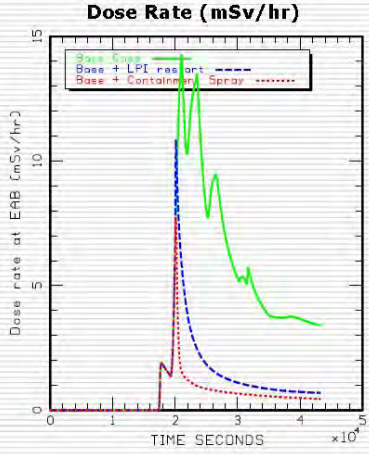
FAUSKE & ASSOCIATES, LLC

Hydrogen Generation and Dose Rate at EAB

Hydrogen Generation



Dose Rate (mSv/hr)



FAUSKE & ASSOCIATES, LLC

Summary

- With all RCS loops and their major components modeled, MAAP5.01 has been demonstrated to have the capability to simulate PWR operational transients.
- With the reactor kinetics model introduced, MAAP5.01 can simulate the load following transient.
- MAAP5.01 has been chosen for AP1000 plant simulator.
- MAAP5.01 is the tool for analyzing shutdown severe accidents and for developing SSAMG.

FAUSKE & ASSOCIATES, LLC

OECD/NEA Workshop June 20-22, 2011

THANK YOU

FOR

YOUR ATTENTION

Wison Luangdilok
Fauske & Associates, LLC
Burr Ridge, IL

FAUSKE & ASSOCIATES, LLC

OECD/NEA Workshop June 20-22, 2011

REGULATORY ASSESSMENT OF THE PSAS FOR THE UK EPR AND AP1000 REACTORS IN THE UK

A.G. Cobo, NII, UK

See the presentation enclosed in this report.

Regulatory Assessment of the PSAs for the UK EPR and AP1000 Reactors in the UK

Ana Gomez, Geoff Grint, Paula Calle

Environment Agency

Office for Nuclear Regulation
An agency of HSE

Outline

- UK Nuclear Licensing Process
- GDA Process and Programme
- Impact of Fukushima
- PSA Assessment in GDA: Standards
- PSA Assessment in GDA: Scope
- PSA Assessment during GDA Step 4
- Outcomes of GDA Step 4
- Interim results and conclusions: AP1000
- Interim results and conclusions: UK EPR
- The future of PSA for New Nuclear Build

Environment Agency

Office for Nuclear Regulation
An agency of HSE

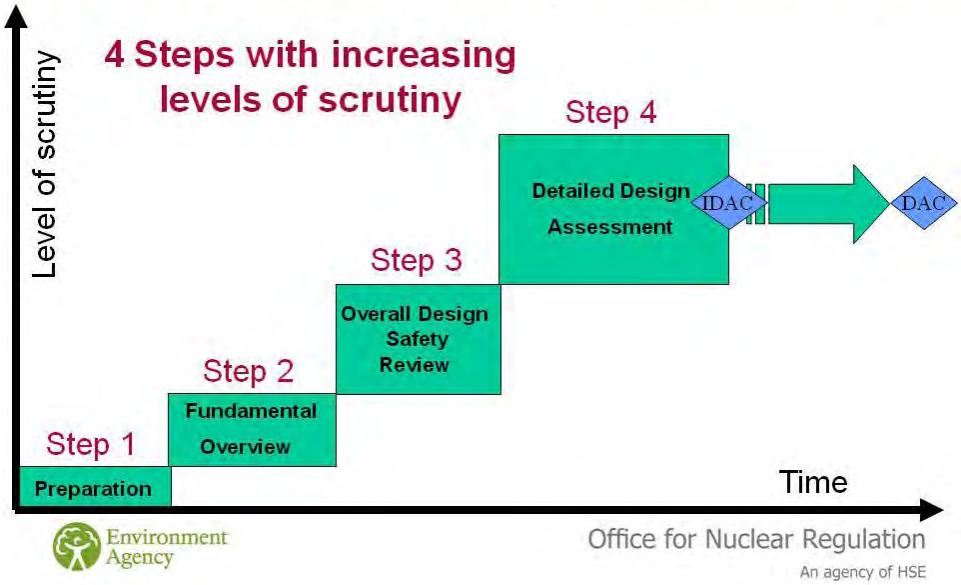
UK Two Phase Nuclear Licensing Process

- Phase 1 : Generic Design Assessment (GDA)
  - Progressive increasing level of assessment as design develops through 4 steps
  - Structure of the safety case based on: Claims / Arguments / Evidence
- Phase 2 : Nuclear Site Licensing & Authorisation
  - Regulation of the development, construction and operation of the selected designs on UK sites

Environment Agency

Office for Nuclear Regulation
An agency of HSE

GDA Process & Programme (before Fukushima)



Environment Agency

Office for Nuclear Regulation
An agency of HSE

Impact of Fukushima

- 5 April 2011: Taking GDA work forward in the light of the unprecedented events in Japan" http://www.hse.gov.uk/newreactors/gda-japan.htm
- First 2011 Quarterly Report addresses the impact of Fukushima on GDA http://www.hse.gov.uk/newreactors/reports/gda-q1-11.pdf
  - Step 4 continues and assessment reports will not be published in June 2011
  - Continue with work to address known GDA Issues
- May 2011: Chief Nuclear Inspector publishes "Japanese earthquake and tsunami: Implications for the UK Nuclear Industry – Interim Report" http://www.hse.gov.uk/nuclear/fukushima/interim-report.pdf
- July 2011: Second 2011 Quarterly Report will launch publication of GDA issues
- September 2011: Chief Nuclear Inspector's "Japanese earthquake and tsunami: Implications for the UK Nuclear Industry – Final Report"

Environment Agency

Office for Nuclear Regulation
An agency of HSE

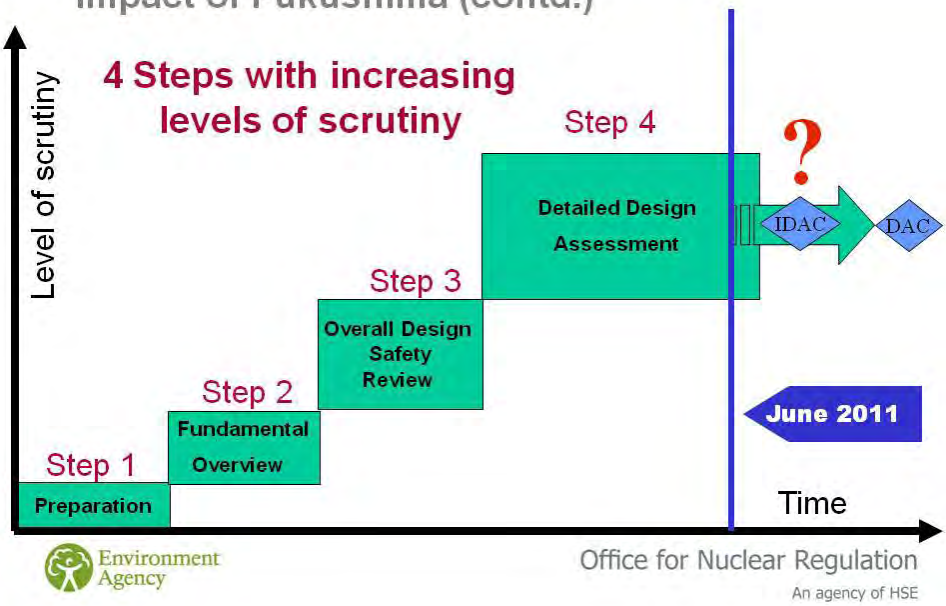
Impact of Fukushima (contd.)

- Impact on GDA:
  - Continue to prepare Step 4 Assessment Reports (as per original programme)
  - Assessment Reports will not be published in June 2011 as outcome of the Fukushima review is unknown
  - From July 2011 work against known GDA Issues will be done as / when agreed with the Requesting Parties
  - There will be a new GDA Issue requesting each RP to "consider and establish action plans to address the lessons learnt from the Fukushima event"
  - Publish assessment reports and issue iDAC/DAC when appropriate
- Overall new build programme continues

Environment Agency

Office for Nuclear Regulation
An agency of HSE

Impact of Fukushima (contd.)



Environment Agency

Office for Nuclear Regulation
An agency of HSE

PSA Assessment in GDA: Standards

- Main standards and criteria: ONR's Safety Assessment Principles (SAPs) FA.10 to FA.14 and numerical targets 7 to 9
  http://www.hse.gov.uk/nuclear/saps/saps2006.pdf
- Relevant IAEA Standards
- WENRA Reference Levels
- ND's Technical Assessment Guide (TAG) on PSA
  http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast030.pdf
  - Embodies the PSA related SAPs, IAEA standards and WENRA reference levels
  - Provides the principal means for assessing the PSA in practice
  - Appendix 1 of the TAG sets up expectations in all areas of PSA
  - Appendix 1 has been thoroughly tested during GDA and has proved very valuable and provided consistency of assessment between both designs
  - GDA PSA assessment had highlighted areas of improvement, so enhancements to the TAG are planned

Environment Agency

Office for Nuclear Regulation
An agency of HSE

PSA Assessment in GDA: Scope

- A hierarchical targeted approach was used which allowed covering the whole PSA without the need to review in detail every aspect of the models, data and supporting analyses
- GDA Step 2 (Sept 2007 to June 2008): Assessment of the high level claims presented in the safety submissions on how the relevant SAPs are met
  - http://www.hse.gov.uk/newreactors/reports/ap1000psa.pdf
  - http://www.hse.gov.uk/newreactors/reports/epripsa.pdf
- GDA Step 3 (June 2008 to November 2009):
  - Assessment of the arguments that support the high level claims:
  - For PSA arguments are the methods, techniques and scope
  - http://www.hse.gov.uk/newreactors/reports/step3-ap1000-probabilistic-safety-analysis-report.pdf
  - http://www.hse.gov.uk/newreactors/reports/step3-uk-epr-probabilistic-safety-analysis.pdf
- GDA Step 4 (November 2009 to June 2011):
  - Assessment of the evidence that supports the arguments
  - For PSA evidence is interpreted as the details of the PSA models and data and the underlying supporting analyses
  - The detailed reviews were conducted on a sampling basis

Environment Agency

Office for Nuclear Regulation
An agency of HSE

PSA Assessment during GDA Step 4

- Detailed reviews in all of the areas addressed at a high level in Step 3
- All the technical areas of PSA were addressed following the guidance and structure established in Appendix 1 of ONR's PSA TAG
- Based on the original PSA documentation submitted by the RPs, subsequent updates submitted during GDA, and additional information received in response to the Technical Queries and Regulatory Observations
- Not each and every fault tree, event tree, supporting analysis or item of reliability data, were examined in detail. Representative samples were selected with a rationale
- It was very important (and sometimes a challenge) to establish clarity on the scope of the RPs' PSA-related material that needed to be referred to during the GDA Step 4 review of the PSAs and how that related to the rest of the design documentation submitted for GDA assessment
- As well as the detailed reviews, a Risk Gap Analysis (RGA) was undertaken by the assessment team for each reactor

Environment Agency

Office for Nuclear Regulation
An agency of HSE

PSA Assessment during GDA Step 4 (contd.)

- Wide use of internationally recognised technical support contractors lead by ONR:
  - Lead PSA Review
  - Thermal-hydraulic Analysis
  - External Hazards and Seismic Fragilities
  - Severe Accident Analysis
  - Containment Structural Analysis (for the Level 2 PSA)
  - Consequence Analysis (Level 3 PSA)
- Continuous interaction and total openness with RPs:
  - Monthly progress meetings; meeting reports shared with RPs
  - Technical exchange workshops and face-to face review sessions throughout
  - TSC's reports provided to RPs with opportunity to comment on factual accuracy

Environment Agency

Office for Nuclear Regulation
An agency of HSE

PSA Assessment during GDA Step 4 (contd.)

Interfaces with other areas of assessment:

- Fault Studies: input to the assessment of the Level 1 PSA success criteria
- Human Factors: input to the HRA assessment
- Civil Engineering / External Hazards: input to the assessment of the screening of external hazards and of the Seismic Margins Analysis regarding definition of hazard curves and fragilities of structures, and to the assessment of the Containment Structural Analysis for the UK EPR Level 2 PSA
- Structural Integrity: input to the assessment of the Containment Structural Analysis for the AP1000 Level 2 PSA and of the Seismic Margins Analysis (SMA) regarding fragilities of metal components
- Severe Accident Analysis: input to the assessment of the Level 2 PSA
- Radiological Protection: input to the assessment of the Level 3 PSA
- C&I: the PSA assessment of the C&I modelling and related sensitivity analyses constituted an input to the C&I assessment
- Continuous two-way informal interactions between PSA and the rest of the technical areas

Environment Agency

Office for Nuclear Regulation
An agency of HSE

PSA Assessment during GDA Step 4 (contd.)

- Risk Gap Analysis (RGA) objectives:
  - Key: Help to reach a conclusion in GDA of whether the reactors can be constructed and operated safely in the UK
  - Evaluation of the importance of the findings in the various PSA technical areas
  - Understand the overall gap between the risk figures claimed by the RPs and an understanding of the risk of the reactors based on a more realistic and complete evaluation
- The items for RGA evaluation were identified during the reviews of the individual technical areas
- Screening of items for further RGA evaluation based on qualitative aspects and / or preliminary quantitative information
- Screened-in items retained for further RGA evaluation, mostly quantitative
- The RGA was not intended to produce alternative PSA results so the precise numbers are of no particular interest
- Qualitative insights from the results of the analysis provided an understanding of the importance of the findings and will inform priorities for their resolution

Environment Agency

Office for Nuclear Regulation
An agency of HSE

Outcomes of GDA Step 4

- Assessment reports (the intention is to publish them later in the year)
- GDA Issues (if appropriate): resolvable issues that must be satisfactorily addressed before a Design Acceptance Confirmation (DAC) will be granted (the intention is to publish them later in the year)
- Resolution Plans developed by the RPs to solve the GDA Issues (the intention is to publish them together with the GDA Issues)
- Assessment Findings: items to be addressed by future Licensees according to the milestones established by ONR during GDA. ONR will deal with them as part of normal regulatory business
- The milestones assigned to the Assessment Findings on PSA have been chosen to ensure that future updates of the PSA capture design, construction and operational developments and that the PSA is used to inform these as appropriate

Environment Agency

Office for Nuclear Regulation
An agency of HSE

Interim results and conclusions: AP1000

- Assessment is complete and draft Assessment Report prepared
- Two GDA Issues: Success criteria & Fire PSA
- Findings of greater or lesser importance in all the technical areas of the PSA
- RGA Insights:
  - CDF and LRF likely to be higher than the figures estimated by Westinghouse but lower than currently operating PWRs
  - Risk profile may change when PSA is complete and improved
  - A number of risk gaps and their importance will depend on matters beyond the generic design (eg, site specific and operator specific)
  - Conservatisms in the current PSA have not been addressed in the RGA
- GDA Issues in other technical areas may impact the PSA and the conclusions extracted from it
- Westinghouse's response to the Fukushima GDA Issue may impact the PSA and the conclusions extracted from it

Environment Agency

Office for Nuclear Regulation
An agency of HSE

Interim results and conclusions: UK EPR

- Assessment is complete and draft Assessment Report prepared
- No GDA Issues have been identified
- Out of scope items will need to be addressed as part of licensing activities
- Findings of greater or lesser importance were identified in all the technical areas of the PSA
- RGA Insights:
  - CDF and LRF unlikely to be significantly different from the figures estimated by EDF and AREVA
  - Need to include more detailed, site specific Seismic PSA
  - Inter-system CCF is potentially important and will need further work
  - Conservatisms in the current PSA have not been addressed in the RGA
- GDA Issues in other technical areas may impact the PSA and the conclusions extracted from it
- EDF and AREVA's response to the Fukushima GDA Issue may impact the PSA and the conclusions extracted from it

Environment Agency

Office for Nuclear Regulation
An agency of HSE

Final remarks: The future of PSA for New Nuclear Build

- Before start of nuclear safety related construction the Licensees shall provide:
  - Site specific screening of external hazards
  - Evidence that the PSA existing at the time is representative, bounding and provides sufficient insights into the relative vulnerabilities and strengths of the plant design in the specific site
  - Task procedures for all the technical areas of the PSA
  - Procedure to maintain the PSA and keep it Living.
  - Procedure for the use of the PSA to support all aspects of design and operation of the NPP
- Before delivery of Mechanical, Electrical and C&I Safety Systems, Structures and Components (SSCs) to the site: Updated PSA addressing all the detailed technical assessment findings
- Before fuel is brought into the site: Updated PSA including as-built and as-(to be)-operated information
- Before power raise: Risk monitor (covering full power, low power, shutdown, reactor and spent fuel pool) and the necessary procedure/s to manage the risk at all times

Environment Agency

Office for Nuclear Regulation
An agency of HSE

Lessons learned form IRSN review of Flamanville 3 Level 1 PSA

G. Georgescu and F. Corenwinder,

Institute for Radiological Protection and Nuclear Safety, BP 17, 92262 Fontenay-aux-Roses, France, gabriel.georgescu@irsn.fr

Abstract

In the frame of the construction and licensing of Flamanville 3 NPP the PSA plays an important role for the EPR Project assessment. The PSA was used for early design verification of EPR Reactor, several design improvement being defined based on these PSA insights and following the discussions with the French and German safety authorities. IRSN, as the French Safety Authority (ASN) technical support organization, performs the review of the PSA developed by the plant operator (EDF). The paper presents the main issues regarding the using of "design PSA", identified by IRSN following the review of the internal events Level 1 PSA transmitted by EDF in the frame of the anticipated instruction of the application for operating license of the Flamanville 3 reactor.

Keywords: New reactors, EPR, PSA, licensing

1. Introduction

In the frame of the construction and licensing of Flamanville 3 NPP (FLA3) the PSA plays an important role for the EPR Project assessment. In fact, the PSA was developed and used for early design verification from the beginning of the design by the EPR reactor designer (AREVA). Several design improvement being defined based on these PSA insights and following the discussions with the French and German safety authorities.

Today, there are many uses of PSA in the frame of FLA3 new reactor project. PSA has a role for the verification of the plant safety level as a complement of the deterministic safety demonstration. It has to be noted that the "Technical Guidelines" for EPR [2] requires the using of the probabilistic approach in order to show the achievement of a significant reduction of the global core melt frequency comparing with the existing NPPs. Many other PSA applications, related to the development of a new reactor, are equally performed. For example, the PSA is used to support the demonstration of "practical elimination" of the large early releases, equally requested by the "Technical Guidelines". The PSA is also involved in the verification of the completeness of the deterministic multiple failures situation (Risk Reduction Categories) features.

2. IRSN assessment of FA3 PSA

In the frame of the FLA3 application for operation license, EDF will provide a rather complete set of Level 1 PSAs:

- Level 1, internal events PSAs related to the reactor core and spent fuel pool,
- internal hazards Level 1 PSAs (fire, explosions, flooding),
- assessment of some external hazards (earthquake, high wind),
- heavy load drop assessment.

Up to now, IRSN fully analyzed the Level 1, internal events PSAs for reactor and for spent fuel pool. The objective of this analysis is to support the ASN position regarding the acceptability of FLA3 PSA

methods at this stage of the project, having in mind that a complementary IRSN analysis will be also necessary in the frame of the technical instruction of the operating license application. It is mainly requested to state on the fulfillment of the French standard requirements (PSA fundamental safety rule [1]) and on the compatibility of the EDF PSA methods with the PSA state-of-the-art methods. ASN also requested to IRSN to analyze the PSA preliminary results (core damage frequency and contributions, systems reliability, etc.).

Following this ASN request, IRSN performed a detailed analysis of the EDF PSA documents. The analysis was also supported by the using of the PSA developed independently by IRSN for EPR reactor. The IRSN report was provided to ASN which released its position statement at the beginning of 2011.

It has to be noted that the decision making process involving the new reactors design PSA is a complex task. The lack of plant-specific operating experience data and operations procedures at the design stage may lead to PSA results that do not reflect the future as-built, as-operated plant. The detailed plant procedures needed to assess human performance may not be available. IRSN attempted to identify the most critical aspects as well as the ways to improve the representativeness of the design PSA in order to allow the decision making-process especially in the frame of licensing activities.

The most important issues, especially when they are specific for a design PSA, are presented in the following paragraphs.

3. Plant available information

3.1 Design information

The design PSA is inevitably based on partial design information, the PSA model including assumptions regarding the future plant design. As a consequence the final design of the plant systems may be different from the design which was considered in the PSA modeling. This is the case mainly for I&C systems, electrical distribution systems (as for example the power supply sources for individual components), equipments type and manufacturer (mainly needed to estimate the possibility for CCF - Common Cause Failures) etc.

This aspect can have an important impact on the PSA results. On the one hand, IRSN believes that the design PSA tractability has to be enhanced. Also, for any new design evolution or clarification, the impact on PSA has to be assessed, and the PSA should then be updated earlier or later depending on this estimated impact.

On the other hand, IRSN estimates that the role of PSA in the designing of new reactors should be better identified and documented.

3.2 Operating profile

In the frame of a design PSA, the operating profile (POS - Plant Operating States and durations) is always provisional, since the operating experience is not available. Then, in the PSA the POS are considered based on assumptions regarding the refuelling, plant availability, etc.

IRSN believes that this aspect is not a major issue for a design PSA and the approach proposed by the utility complied with the PSA safety rule. However, as soon as the operating experience becomes available the PSA should be updated accordingly.

3.3 Accidental procedures

Generally the detailed accident procedures are not available while developing the design PSA. As a consequence the human reliability analysis is performed based on assumptions and simplifications regarding the future accident procedures.

The impact of this aspect on the PSA results can be important. Nevertheless, IRSN believes that using a conservative/screening approach (like, for example, Swain screening model) is an acceptable approach for a design PSA. However, this approach has to be completed by a qualitative verification of the existence of the given operator strategies in the preliminary version of accident procedures or accident guidelines.

3.4 Preventive maintenance

The modelling of the preventive maintenance is an important aspect, mainly if it is foreseen to perform such activities during the power operation. IRSN considers that the modelling of only components unavailabilities based on provisional maintenance durations, is not enough to conclude on the safety impact of the future preventive maintenance strategies and also on the safety importance of the specific design features which are provided for maintenance (like for example the possibility to interconnect redundant electrical trains).

IRSN believes that the design PSA should analyze, beside components unavailabilities, the maintenance specific configurations. Moreover, the possibility for new initiating events occurring during maintenance activities (for example, loss of two electrical divisions) or induced by maintenance activities (mainly by human errors) has to be deeply investigated.

3.5 Technical Specifications

The design PSA considers generic and simplified Technical Specifications (TechSpecs). For IRSN this aspect should not have a strong impact on the PSA results. Moreover, the PSA may be generally used later to define the future TechSpecs. IRSN believes that the PSA can be updated when the detailed TechSpecs will be available and after an initial operating experience, without a strong impact on the licensing processes.

4. Data

4.1 Reliability data

The reliability data employed in a design PSA are taken generally from the existing plants operating experience and from other available sources (NUREG, international data bases). The method to choose the most appropriate data consists on the evaluation of similarity of the new reactor components with the existing available data. For IRSN this approach is acceptable in principle. However, the similarity analysis between new reactor components and the operating experience which was used to quantify the existing reliability data is not an easy work. This analysis has to consider, beside the component type and safety classification, also the operating conditions, the surveillance requirements (test intervals), the component population used to quantify the data, the recent operating experience trends, etc. The justification of choosing a given data has to be fully traceable and documented. Moreover a comparison between several sources may be desirable, especially if the difference between the data is important.

For new or revolutionary components, reliability studies are preformed or expert opinion is used. IRSN believes that sensitivity studies may be useful in order to reduce the uncertainties related to this aspect.

4.2 Common Cause Failure (CCF)

For a design PSA, the CCF parameters are generally based on existing operating experience completed by international available sources (NUREG). Generic values may be also used if it is considered that the available information is not pertinent for the selected CCF group. Since, there are in general no big discrepancies between CCF parameter values from different sources, IRSN considers that this approach is acceptable. However, it has to be documented and traceable.

Regarding the definition of CCF families, the design PSA uses assumptions in order to identify the groups of redundant components for which CCF contributions should be taken into account. IRSN considers that the approach is, in principle, acceptable. However, for IRSN the assumption of fully diversification of some redundant components (when it is assumed that the CCF is not possible) has to be justified by a through analysis. This analysis has to cover all the CCF causes and mechanisms (type, manufacturer, environment, maintenance, etc.) as well as the perpetual character of these conditions over the plant lifetime. This aspect refers mainly to components of a similar type, but produced by different manufacturers (like Diesels, batteries, etc.), and for which some parts may be provided by the same supplier or for which the same maintenance, maintenance materiel or spare parts may apply. Sensitivity studies may be useful in order to identify the potential CCF families for which detailed studies may be necessary.

4.3 Loss of ultimate heat sink

The loss of main ultimate heat sink is generally a dominant contribution initiating event. Consequently the approach used to quantify the frequency and the scope of this initiating event is very important for a design PSA.

The frequency of loss of main ultimate heat sink may be quantified by using the experience (nuclear and non-nuclear). IRSN believes that it is necessary to verify the applicability of available experience to the given site and given design and to assess the related uncertainties.

Another approach is to develop reliability studies based on the intake structure and of the pumping station design. This approach is considered acceptable by IRSN. However the approach has to cover not only the design basis situations (daily or yearly pumping station detritus arrival and cleaning) but also the beyond design basis situations having a longer return period but with potentially much higher intensity.

In the case that a second, diversified ultimate heat sink is foreseen for the new reactor design, the independency between the main heat sink and the secondary heat sink has to be toughly justified. The justification applies to all aspects which may threaten the independency or the diversity of the two heat sinks: sea/river related hazards and other external hazards, design of intake structures, design of pumping station systems, maintenance, internal hazards (flooding, fire and explosion).

5. Support systems modelling

5.1 I&C

I&C is modeled in a design PSA by using fault trees. These fault trees are generally developed at the level of macro-components, since the I&C systems are too complex to be possible to develop fault trees up to individual components. The macro-components can be defined based on a logical

decomposition (as for example the COMPACT model employed by EDF) or based on systems decomposition (more classical model used, for example, by IRSN).

IRSN considers that both approaches are acceptable and can be used in a design PSA. However, justifications have to be provided regarding the validity of the model. These justifications may include:

- the performance of a Failure Mode and Effects Analysis (FMEA) for the different sub-systems of I&C systems (platforms, networks, computers, human machine interfaces, etc.),
- the performance of a dependency analysis between the I&C sub-systems and components (dependency matrix),
- the analysis of the impact of the failure of ventilation and cooling systems on the I&C.

Even the I&C model in the PSA may be simplified at the design stage, IRSN believes that some important aspects have to be carefully modeled: the I&C support systems, the miscalibration human errors and the CCF between redundant I&C systems. Moreover, the potential "loss of I&C systems" as well as "spurious I&C" initiating events have to be deeply analyzed in all reactor states and considered in the PSA model if necessary.

5.2 Ventilation systems

The utility proposed by simplification, the ventilation systems are not modeled in the design PSA. The IRSN position is that this simplification is not acceptable, mainly because it may lead to neglect important interdependencies between safety systems and support systems.

IRSN considers that the design PSA should model the ventilation systems, even in a simplified and conservative way. The initiating events induced by the loss of ventilation should be also investigated and modeled in the PSA if necessary. Moreover, for IRSN, the design PSA should be capable to be used to assess the potential cliff-edge effects related to the variation of the outside temperature (to demonstrate that the risk increase is not important when the outside temperature is higher or lower than threshold values).

6. Human factor assessment

6.1 Pre-accident human factor

In the design PSA the preaccidental human errors are quantified based on incomplete or generic information regarding the components position indicators or alarms, surveillance requirements, maintenance, administrative measures, etc. On the one hand, IRSN considers that the impact of this aspect is not very high on the PSA results. However a mostly conservative model (considering for example the recovery possibilities only when the design can be confirmed) may be preferable.

On the other hand, IRSN considers that the most important issue regarding the pre-accidental human factor is the correct identification of the possible dependencies between different human actions performed on redundant trains, including the calibration of sensors. IRSN believes that the pre-accidental human factor dependencies have to be carefully analyzed and documented.

6.2 Post-accident human factor

As already mentioned, IRSN believes that using a conservative/screening approach (like, for example, Swain screening model) is an acceptable approach for a design PSA. However, IRSN considers that one of the most important issues regarding the post-accidental human factor is the correct identification and modeling of the possible dependencies between redundant human actions.

IRSN believes that the dependencies between the post-accidental human errors have to be carefully analyzed and treated in the design PSA preferably by using conservative rules. The modeling can be further upgraded when the detailed design and accident procedures will be available.

6.3 Crisis team modeling

In the design PSA, the crisis team may be considered in a simplified way. For example all the decision human errors are considered as being negligible if the crisis team is in place. IRSN considers that this modeling of the crisis team, even if it is not in principle wrong, can lead to introduction of some optimism in the PSA model: undeveloped accident sequences, omission of some execution errors and omission of some equipment failures.

IRSN believes that the crisis team modeling should be enhanced by taking into account the crisis team decision error probability (mainly based on available information for the crisis team during the accident), the execution error probability (mainly for the irreversible errors) as well as the reliability of the mitigations.

7. Initiating events

7.1 Initiating events common to reactor and spent fuel pool

In general the reactor and the spent fuel pool are considered in the design PSAs as being independent. As a consequence in the PSA developed for the reactor, respectively for the spent fuel pool, it is considered that all mitigations means and human resources are fully available.

IRSN considers that this assumption may be optimistic, since the mitigation and support systems may be shared between the reactor and the spent fuel pool and that the operating crew has to handle simultaneously both installations in accidental situation.

IRSN believes that these aspects should be carefully treated, especially for the initiators with a long reparation time (like the loss of last heat sink or loss of outside power supply) as well as for the hazards (like for example the internal fire, especially if the spent fuel make-up system is also the firefighting system).

7.2 Reactor PSA initiating events

The initiating events list is generally developed in a design PSA by compiling existing plants PSA initiating events lists and international practices. This list is then completed by using deductive methods, in order to identify specific initiators for the given new reactor type.

For IRSN this approach is acceptable. Nevertheless the approach itself does not guarantee the completeness of the list, especially if the initial boundary conditions definition is not complete or not appropriated for the objectives of the design PSA (as for example the loss of ventilation initiators or loss of I&C initiators may be excluded). IRSN considers that these aspects should be carefully treated.

7.3 Spent fuel pool PSA Initiators quantification

The method used to quantify the initiating events may differ between the reactor PSA and spent fuel pool PSA. In fact for some initiators, the available time to recover the situation before the total loss of cooling of the spent fuel pool can be long. This kind of initiating event can be then interpreted as a pre-initiating event for the loss of cooling initiating event. The quantification of the frequency of the

total loss of cooling initiating event considers then the recovery probability. This quantification can be performed separately from the PSA model by using other methods (Markov chains for example).

For IRSN this approach is acceptable. Nevertheless some precautions should be taken in order to ensure the coherence with the PSA developed for the reactor (as some of the initiating events affect both installations simultaneously) and to ensure the correct modeling of the dependencies (mainly when the pre-initiating event is a loss of support system: electrical busbar or cooling system).

8. Accident sequences

8.1 Functional analysis

In order to develop the accident sequences in the design PSA, functional analyses are generally developed. These analyses are supported by appropriate thermohydraulic studies.

IRSN considers that this approach is the best approach to follow for the development of the event trees, because it allows to define precisely the accident sequences and in the same time to reduce the modeling uncertainties. Nevertheless, the transposition of the functional analysis in the PSA model should be carefully performed, mainly to ensure that all the dependencies identified by these analyses are taken into account in the PSA model.

On the other hand, IRSN mentions that the PSA model cannot be limited to the development level of the functional analyses, since the PSA generates, in fact, many other failures combinations and dependencies which cannot be all explicitly treated in the functional analysis. This aspect should be taken into account while developing the accident sequences and while defining the systems success criteria.

8.2 Recovery factors modeling

The design PSA may consider recovery actions and corrective factors (to take into account for example the fact that some initiators recovery time is much shorter that the modeled systems mission time: ex: short loss of outside power over diesels mission time). The recovery factors consider the repair time and different time for the loss of system using a specific formula. This approach is acceptable in principle, but the effective modeling of the corrective factors may be difficult, especially when a “point” value is used instead of a fault tree. In fact, the using of a point value may lead to fail to identify important dependencies and finally to a non-conservative PSA model.

8.3 Sumps clogging

In the design of new reactors, special devices or systems may be provided to avoid the sumps clogging and to ensure the long term operation of the safety injection system and of the containment cooling system.

IRSN believes that the role of these devices or systems should be modeled in the PSA. This aspect is important for the using of the PSA for design verification, but also for the application of the PSA for TechSpecs definition and surveillance requirements definition.

8.4 By-pass LOCA

The primary circuit interface system breaks which can lead to containment bypass accidents are normally modeled in any design PSA. The core damage frequency related to this kind of accident should be very low (for EPR reactor, this type of situation is included in the category of accidents which have to be “practically eliminated”). One of the most important aspects related to bypass

accident analysis is the assessment of the impact of the primary inventory flow outside containment on the safety and support systems. In general, the most vulnerable systems are the electrical power supply and the I&C systems.

IRSN believes that the modeling of the bypass LOCA in the design PSA should be supported by a detailed analysis of the possible primary flow environmental effects on the electrical and I&C systems located in the buildings which are directly or indirectly impacted.

8.5 Spent fuel pool PSA repairing modeling

In the frame of a spent fuel pool PSA the recovery of cooling systems is one of the most important mitigation. The quantification of the recovery probabilities depends mainly on the systems design and systems installation, as well as on the equipment reliability data (the time to repair). At the design stage, as some of this information may be missing, the PSA considers assumptions to quantify the recovery probabilities for different accident sequences.

IRSN believes that the assumptions used to quantify the recovery actions should be thoroughly documented and traceable. Additionally, the coherence should be ensured between the reliability data used for the reactor PSA and the spent fuel pool PSA.

8.6 Spent fuel pool passive devices

In order to avoid the accidental loss of inventory of the spent fuel pool by siphoning, generally, anti-siphoning devices are considered in all designs. Even if the failure probability of these devices should be very low, IRSN believes that this contribution should be modeled explicitly in the PSA. This aspect is important for the using of the PSA for design verification, but also for the application of the PSA for TechSpecs definition and surveillance requirements definition.

8.7 Definition of the spent fuel pool accident sequence unacceptable consequences

In the frame of a spent fuel pool PSA the definition of the unacceptable consequences is different from the reactor PSA. For example the boiling of the spent fuel pool inventory can be considered as unacceptable consequence if the spent fuel pool building is not a full containment.

IRSN believes that the definition of the spent fuel pool PSA accident sequence unacceptable consequences should be coherent with the global safety objectives of the plant and with the global context of the safety assessment.

9. Conclusions

For the EPR Reactor, the PSA was developed from the beginning of the design by the reactor designer (AREVA). This PSA was used for early design verification, several design improvement being defined based on these PSA insights and following the discussions with the French and German safety authorities.

The decision making process involving the new reactors design PSA is a complex task. The lack of plant-specific operating experience data and operations procedures at the design stage may lead to PSA results that do not reflect the future as-built, as-operated plant. The detailed plant procedures needed to assess human performance may not be available.

IRSN attempted to identify the most critical aspects as well as the ways to improve the representativeness of the design PSA in order to allow the decision making-process especially in the frame of licensing activities.

10. References

6. ASN, “Règle Fondamentale de Sûreté - Développement et utilisation des études probabilistes de sûreté" (2002).
7. Letter ASN, “Options de sûreté du projet de réacteur EPR” (2004).

IRSN
INSTITUT DE RADIOPROTECTION ET DE SÛRETÉ NUCLÉAIRE
Faire avancer la sûreté nucléaire

Lessons learned form IRSN review of Flamanville 3 Level 1 PSA

G. Georgescu and F. Corenwinder
IRSN France

OECD/NEA Workshop on PSA for New and Advanced Reactors, Paris, 20 - 24 June 2011

Introduction

- For the EPR Reactor, the PSA was developed from the beginning of the design by the reactor designer (AREVA)
  - This PSA was used for early design verification, several design improvement being defined (SBO Diesels, Heat Sink diversification…)
- Today there are many uses of PSA in the frame of Flamanville 3 (FA3) new reactor project:
  - Safety level and design verification, classification, demonstration of "practical elimination" of the Large Releases, multiple failures categories (RRC) definition, TechSpec development, preventive maintenance)

Introduction

- IRSN performed the review of the EDF FA3 internal events Level 1 PSA for reactor and spent fuel pool
- Several important issues regarding the using of "design PSA" in the context of new reactors development and licensing were identified
- The ASN letter was published in January 2011

Introduction

- It has to be noted that the decision making process involving the new reactors design PSA is a complex task:
  - The lack of design information, plant-specific operating experience data and detailed plant procedures may lead to PSA results that do not reflect the future as-built, as-operated plant
- IRSN identified the most critical aspects as well as the solutions to improve the representativeness of the design PSA for the decision making-process (licensing activities)
- Here only the most important issues are presented

Design information

- The design PSA is inevitably based on partial design information
- The final design of the plant systems may be different from the considered design
  - I&C systems, electrical distribution systems, equipments type and manufacturer (CCF)...
- IRSN Conclusion:
  - The design PSA tractability should be enhanced
  - For any new design evolutions or clarifications, the impact on PSA has to be assessed
  - The role of PSA in the designing of new reactor should be better identified and documented

Accidental Procedures

- The detailed accident procedures are not available
  - The human reliability analysis is performed based on assumptions and simplifications regarding the future accident procedures.
- IRSN Conclusion:
  - Using a conservative/screening approach (like, for example, Swain screening model) is an acceptable approach
  - The qualitative verification of the existence of the given operator strategies in the preliminary version of accident procedures or accident guidelines should be performed

Initiating events

- The initiating events list is generally developed in a design PSA by compiling existing plants PSA initiating events lists and international practices
- This list is then completed by using deductive methods, in order to identify specific initiators for the given new reactor type
- IRSN Conclusion
  - The approach itself does not guarantee the completeness of the list, especially if the initial boundary conditions definition is not complete or not appropriated for the objectives of the design PSA (as for example the loss of ventilation initiators or loss of I&C initiators may be excluded)
    - These aspects should be considered when defining the initiating events list

Initiating events common to reactor and spent fuel pool

- The reactor and the spent fuel pool are considered in the design PSAs as being independent
  - all mitigations means and human resources are fully available for each one of them
- IRSN Conclusion
  - This assumption may be optimistic
    - mitigation and support systems may be shared
    - the operating crew has to handle simultaneously both installations in accidental situation
  - These aspects should be carefully treated, especially for the initiators with a long reparation time (loss of ultimate heat sink or loss of outside power supply) as well as for the hazards (internal fire, especially if the spent fuel make-up system is in the same time the firefighting system)

Preventive maintenance

- Important aspect, mainly if it is foreseen to perform such activities during the power operation
- IRSN Conclusion
  - The modeling of only components unavailabilities based on provisional maintenance durations, is not enough to conclude on the safety impact
  - The maintenance specific configurations and the possibility for new initiating events occurring during maintenance activities or induced by maintenance activities (mainly by human errors) should be analyzed
    - for example, multiple loss of electrical divisions

Reliability data

- Generally from the existing plants operating experience and from other available sources (NUREG, international data bases)
- IRSN conclusion
  - Beside the component type and safety classification, the operating conditions, the surveillance requirements (test intervals), the component population used to quantify the data, the recent operating experience trends, should be also considered
    - The justification of choosing a given data has to be fully traceable and documented
  - Comparison between several sources may be desirable, especially if the difference between the data is important
    - Sensitivity studies may be useful

CCF modeling

- The CCF parameters are generally based on existing operating experience completed by international available sources and generic values
- The definition of CCF families is generally based on assumptions regarding the design
- IRSN conclusion
  - The assumption of fully diversification of some redundant components has to be justified by a through analysis
    - All CCF causes and mechanisms (type, manufacturer, environment, maintenance, etc.)
      - Ex: components of a similar type, but produced by different manufacturers: some parts may be provided by the same supplier, same maintenance…
    - The perpetual character of these conditions over the plant lifetime

Loss of ultimate heat sink

- The loss of ultimate heat sink initiating event is in general a dominant contribution
  - The approach used to quantify the frequency as well as the scope of this initiating event is very important for a design PSA
  - The frequency of loss of ultimate heat sink may be quantified by using the experience (nuclear and non-nuclear)
- IRSN Conclusion
  - It is necessary to verify the applicability of available experience and to assess the related uncertainties
  - The beyond design basis situations (longer return period but higher intensity) should be also included here
  - The independency between the main ultimate heat sink and the secondary heat sink has to be toughly justified

I&C modeling

- The I&C fault trees are generally developed at the level of macro-components
  - Logical decomposition (EDF COMPACT model) or systems decomposition (IRSN)

- IRSN Conclusion
  - Justifications have to be provided regarding the validity of the model
    - Failure Mode and Effects Analysis (FMEA) for the different sub-systems of I&C systems (platforms, networks, computers, human machine interfaces…)
    - Dependency analysis between the I&C sub-systems and components
    - Impact of the failure of ventilation and cooling systems on the I&C
  - The I&C support systems, the miscalibration human errors and the CCF between redundant I&C systems should be modeled
  - The potential "loss of I&C systems" as well as "spurious I&C" initiating events have to be analyzed in all reactor states

Human factor assessment

- The pre-accidental HRA is based on incomplete or generic information

- The detailed accident procedures are not available for post-accidental HRA

- The crisis team may be considered in a simplified way

- IRSN Conclusion
  - The most important issue regarding the human factor is the correct identification and quantification of the dependencies:
    - pre-accidental HRA: actions performed on redundant trains
    - post-accidental HRA: redundant mitigations
    - conservative assumptions or qualified information should be used
  - The crisis team modeling should take into account the decision error, the execution error (mainly for the irreversible errors), as well as the reliability of the systems

Sumps clogging

- In the design of new reactors, special devices or systems may be provided to avoid the sumps clogging and to ensure the long term operation of the safety injection system and of the containment cooling system
- IRSN Conclusion
  - The role of these devices or systems should be modeled in the PSA
    - This aspect is important for the using of the PSA for design verification, but also for the application of the PSA for TechSpecs definition and surveillance requirements definition

By-pass LOCA

- The By-pass LOCA are normally modeled in any design PSA
- The core damage frequency related to this kind of accident should be very low
  - For EPR reactor, this type of situation is included in the category of accidents which have to be "practically eliminated"
- One of the most important aspects is the assessment of the impact of the primary inventory flow outside containment on the safety and support systems (electrical power, I&C, etc.)
- IRSN Conclusion
  - The modeling of the bypass LOCA in the design PSA should be supported by a detailed analysis of the possible primary flow environmental effects on the electrical and I&C systems located in the buildings which are directly or indirectly impacted

Spent fuel pool PSA initiators quantification

- The available time to recover the situation before the total loss of cooling of the spent fuel pool can be long
  - The quantification of the frequency of the total loss of cooling considers then the recovery probability. This quantification can be performed separately from the PSA model by using other methods (Markov chains for example)

- IRSN Conclusion
  - The coherence with the reactor PSA (as some of the initiating events affect both installations simultaneously) should be ensured
  - The modeling of the dependencies should be treated carefully (mainly when the initiating event is a loss of support system: electrical busbar or cooling system)

Spent fuel pool PSA repairing modeling

- The recovery of cooling systems is one of the most important mitigation

- The quantification of the recovery probabilities depends mainly on the systems design and systems installation, as well as on the equipment reliability data (the time to repair)

- At the design stage, as some of this information may be missing, the PSA considers assumptions to quantify the recovery probabilities for different accident sequences

- IRSN Conclusion:
  - The assumptions used to quantify the recovery actions should be thoroughly documented and traceable
  - The coherence should be ensured between the reliability data (time to repair) used for the reactor PSA and the spent fuel pool PSA

Spent fuel pool PSA unacceptable consequences

- The definition of the unacceptable consequences is different from the reactor PSA
  - For example the boiling of the spent fuel pool inventory can be considered as unacceptable consequence if the spent fuel pool building is not a full containment
- IRSN Conclusion:
  - The definition of the spent fuel pool PSA accident sequence unacceptable consequences should be coherent with the global safety objectives of the plant and with the global context of the safety assessment

CONCLUSIONS

- In the context of the anticipated instruction of the application for operation license of FLA3 reactor, the French Safety Authority (ASN) asked IRSN to analyze the FLA3 EPR
- The decision making process involving the design PSA is a complex task
  - The design PSA specific issues need to be identified
  - The impact of incomplete information needs to be assessed
  - Iterative approaches should be applied

Role of PRA in New NPP Projects

Ari Julin, Jorma Sandberg and Reino Virolainen

Radiation and Nuclear Safety Authority (STUK), Laippatie 4, 00880 HELSINKI, FINLAND

Abstract

In Finland, a plant specific, Level 1 and 2 Probabilistic Risk Analysis (PRA) is required as a prerequisite for issuing the construction license and operating license. The use of PRA in various applications and the main insights are presented. These applications include e.g. PRA support to the design of SSCs, definition of pre-service and in-service inspection programs, evaluation of the safety classification of SSCs, development of procedures, training and in definition of risk informed technical specifications, periodic testing and on-line preventive maintenance programs. In addition, PRA shall be used to assess the adequacy and coverage of the phase and system commissioning programs. Also the potential risks related to commissioning tests during nuclear test phase, shall be assessed with the help of PRA. In OL3 project, risk informed approach has been applied on a large scale for the first time in the design, construction and commissioning of a new NPP unit. Pre-nuclear commissioning tests have started at OL3 site and the plant is foreseen to begin commercial operation in 2013. Decisions have been made to launch new NPP projects. Teollisuuden Voima Oyj (TVO) is planning to build a new unit (OL4) at Olkiluoto site and a new utility, Fennovoima, is planning to build one unit at one of two alternative green field sites in Northern parts of Finland. Insights from PRAs of operating NPPs have been used in the evaluation of possible new sites to ensure that the site specific concerns and environmental conditions are adequately taken into account in the design of SSCs. Although the seismic activity at the Olkiluoto site is low, a comprehensive seismic risk analysis is being conducted. Its results support the review of the deterministic seismic design. For new sites, a probabilistic seismic hazard analysis has been carried out for the determination of the design earthquake. Experiences from OL3 licensing have been utilized in the further development of risk informed requirements in Finland.

Keywords PRA/PSA, Licensing, PRA applications, Risk-Informed

1. Introduction

In Finland, PRA is a formal licensing document. A plant specific, full scope Level 1 and 2 PRA has to be submitted to the regulatory authority (STUK) for approval in the context of construction and operating license application. Regulatory requirements are also set forth for the use of PRA in all phases of the NPP built. Hence, the risk informed approach is to be applied in several areas during the design and construction of NPPs, e.g. supporting the detailed design of systems, structures and components (SSC), definition of pre-service and in-service inspection programs, evaluation of the safety classification of SSCs, development of procedures, training of NPP staff and in definition of risk informed technical specifications, periodic testing (in-service testing) and on-line preventive maintenance programs. In the past, risk insights have led to several modifications of the operating NPPs in Finland, as well as to many design changes to the EPR plant (OL3) under construction. In addition to the internal events PRA, internal and external hazard analyses provided useful insights to ensure that the site specific concerns and environmental conditions are adequately taken into account in the design. Risk informed approach has also been applied to grading of quality assurance requirements of certain organizational activities, as well as for assessing the risk related to different commissioning phases. Experience from risk informed safety management of operating NPPs and from the licensing of OL3 EPR have been utilised in the further development of risk informed regulation in Finland.

2. Risk informed licensing

2.1 NPP licensing process in Finland

The Nuclear Energy Act (990/1987) and Decree (161/1988) define the licensing procedure in detail. Licensing of a new NPP is performed in three stages.

1. Decision in Principle: can it be done?
2. Construction license: how will it be done?
3. Operating license: was it done right?

1. Decision in Principle (DiP)

An environmental impact of the new plant unit has to be investigated prior to the application for the Decision in Principle in compliance with the Law on Environmental Impact Assessment (EIA) Procedure. For OL3 EPR plant the EIA was performed in 1998.

The construction of a nuclear power plant requires a DiP made by the Government. The main criterion in DiP process is to ensure that the construction of a new NPP is in line with the overall good of society. The DiP is then forwarded to Parliament for perusal. Parliament may reverse the DiP as such or may decide that it remains in force. The application may include alternative sites and reactor types to be chosen later.

The Government pays special attention to

- the need for the nuclear facility project with respect to the country's energy supply
- the suitability of the intended site of the nuclear facility and its effects on the environment, and
- the arrangements for the nuclear fuel and waste management.

STUK prepares a preliminary safety assessment of the application. In the safety assessment, STUK aims to ensure that all safety related requirements set forth in government decrees are adequately met.

A positive statement of the municipality of the site planned for the nuclear facility is also a prerequisite for approving the DiP.

2. Construction license

The license to construct a nuclear power plant is granted by the Government. The application and hearing procedures of the license are prescribed in detail in the Nuclear Energy Act and Decree. At this stage, a full scope preliminary Level 1 and 2 PRA has to be sent to STUK for approval, together with other licensing documentation. This so-called “design phase PRA” shall demonstrate the plant's compliance with the probabilistic design objectives for core damage frequency CDF and large release frequency (LRF). In addition the licensee has to indicate by means of the design phase PRA that the foundation of the plant design is fit and the norms used are adequate. This concerns especially events like harsh weather or other exceptional environmental conditions and seismic events, the frequencies and consequences of which may comprise large uncertainties. The design basis for external events has to be defined so that the probabilistic safety target can be fulfilled. The purpose of the design phase PRA is to support the development of a balanced plant design. The aim is also to reveal the inter-connections and interactions between the safety, support and surrogate systems as well as common cause failures and potential weak points in the plant design. STUK will review the design phase PRA and assess the acceptability of the design phase PRA prior to giving a statement on the construction license.

PRA will be complemented during construction as the detailed design of the plant unit will be finalized. Design has to be modified unless these objectives are met. If dominant risk factors are identified after issuing a Construction license, all reasonable efforts have to be taken to reduce the risk.

3. Operating license

The Government issues the license for the operation of the nuclear power plant. The application and hearing procedures of the license are presented in detail in the Nuclear Energy Act and Decree. STUK makes a statement on the application for the operating license. A safety assessment will be attached to the statement. At this stage, a full scope updated Level 1 and 2 PRA has to be sent to STUK for approval, together with other licensing documentation. In addition, PRA applications required by regulatory guides have to be submitted to STUK, as well. During construction, PRA shall be updated to comply with the detailed design information of SSCs and more detailed modelling of plant response to various initiating events. The fulfilment of the numerical criteria for CDF and LRF has to be demonstrated as well.

In Finland, the operating license of a nuclear power plant is granted only for a fixed term. Usually the period of validity of the license is twenty years. In considering the duration of the license, special attention is paid to safety precautions and the estimated duration of operations. STUK can interrupt the operation of a nuclear power plant if necessary for ensuring safety. Table 1 summarises the NPP licensing process an the role of PRA.

1. Decision in principle (DiP) on the construction of a nuclear power Plant • Political debate on whether using nuclear energy is for the overall good of society • Government decision and Parliament ratification/rejection • STUK's preliminary safety assessment (PRA not required at this stage)
2. Application for a construction license, (CDF < 1E-5 /a, LRF < 5E-7 /a) • Submission of level 1 and 2 design phase PRA to STUK • Evaluation of the acceptability of design phase PRA – (Upgrade of PRA and/or the plant design)
Construction phase • Completion of design phase PRA (Applications such as RI-ISI, RI-IST, RI-TS, RI-PM, Training, Procedures, Safety classification of SSC)
3. Application for an operating license, (CDF < 1E-5 /a, LRF < 5E-7 /a) • Submission of level 1 and 2 PRA to STUK • Evaluation of the acceptability – (Upgrade of PRA and/or the plant)
Operation phase • Utilization of PRA during operation (Plant modifications, RI-ISI, RI-IST, RI-TS, RI-PM, Training, Procedures, Incident and Event Analysis)

Table 1. PRA and Licensing of NPPs in Finland

2.2 Concept of Risk Informed Regulation and Safety Management

As a necessary complement to the deterministic safety design, a probabilistic risk analysis (PRA) is required to verify the reliability of all vital safety functions. PRA results indicate the balance of the design features from the safety point of view, and the weakest points that possibly need to be strengthened. The guidelines for performing and applying PRA are set forth in the Regulatory Guide YVL 2.8 issued by STUK in 1987 and renewed in 1996 and 2002. The guide is currently being revised and the new revision will be issued in 2012. Regulatory guide YVL 2.8 and the new draft guide YVL A.7 "Probabilistic Risk Analysis for NPPs" specify the following probabilistic design objectives:

- mean value of the core damage frequency (CDF) is less than $1.0 \cdot 10^{-5}$/year; assessed and verified in full scope Level 1 PRA
- mean value of a large radioactive release frequency (LRF) is less than $5.0 \cdot 10^{-7}$/year; assessed and verified in full scope Level 2 PRA.

PRA is formally integrated in the regulatory process of NPPs already in the early design phase and it is to run through the construction and operation phases all through the plant service time, as shown in Fig. 1. The life cycle model of PRA forms the concept of risk informed regulation and risk informed safety management. In the life cycle model the risk informed regulatory activities and safety management activities are tightly connected.

A full scope plant specific Level 1 and 2 PRA includes internal initiators, fires, flooding, harsh weather conditions and seismic events for full power operation mode and for low power and shutdown mode. It is essential that the plant staff performs PRA as far as possible in-house in order to become well prepared for using the PRA for decision making purposes. The regulatory guide includes specific prerequisites for the quality of PRA. Accordingly the licensee has to use state-of-the-art PRA methods including human factor analysis, best estimate thermal hydraulic analyses and to perform quantitative uncertainty and sensitivity analyses. In addition the licensee has to draw up and maintain guidelines for ensuring an adequate quality level of evolving PRA model and for using PRA for safety management activities.

In the same living PRA spirit STUK`s personnel conducts thorough reviews in-house. The value of PRA insights in decision making process is greatly diminished if there are shortages in the PRA scope. In Finland, the scope is one of the main attributes that define the quality of PRA. With a thorough in-house regulatory review STUK aims to gain assurance that also other important quality aspects, e.g. transparency, level of detail, state-of-the art methodology, good documentation and QA process, are adequately accounted for. Since the requirements for a plant specific PRA are comprehensive, the quality of PRA is usually adequate for all applications, with only small changes.

<table>
<tr><th colspan="2">RISK INFORMED REGULATION
(STUK)</th><th>RISK INFORMED SAFETY MANAGEMENT
(utilities)</th></tr>
<tr><td colspan="3">UTILIZATION OF LIVING PRA IN FINLAND</td></tr>
<tr><td>Use of PRA for
Design and Construction</td><td>Plant operation and maintenance
(PRA Level 1 & Level 2)</td><td>Strategic SAM Planning
(PRA level 2)</td></tr>
<tr><td rowspan="3"><u>Design and Construction Issues</u>
• Resolutions in Early Design Process
• D&EO Procedures
• Program for on-line PM
• Program for Systems Testing
• Safety Classification and Graded QA of SSC
• Review of Tech Specs
• Compliance with Safety Objectives</td><td>LONG TERM
• Main risk contributors
• Plant Modifications and Backfitting
• In-Service Inspection (ISI)
• In-Service Testing (IST)
• Analysis of Tech Specs
• Maintenance Planning
• Personnel Training
• D&EOP Improvements
• Graded QA
• (Cost Benefit Analysis)</td><td rowspan="3">• Uncertainty Issue
• Quantification Techniques
• Recognition of Critical Sequences and Phenomena
• Evaluation of Significance of Critical Phenomena and Human Factor
• Evaluation of Mitigation Measures</td></tr>
<tr><td>SHORT TERM
• Exemption from Tech Specs
• Analysis of Safety Margins during Incidents</td></tr>
<tr><td>PSA Based Event Analysis (incl. risk follow-up of licensee events and precursor studies)</td></tr>
</table>

Figure 1. Living PRA framework in Finland

The essence of the risk informed regulation and safety management in Finland is that the PRA works as an interactive communication platform between the licensee and STUK. Identical, reviewed PRA model used for resolution of safety issues both by the licensees and STUK. Licensees are committed to provide STUK with a PRA model in electronic form and to regularly maintain and update it.

During the past decade, more requirements have been set forth to extend the use of PRA to various risk informed applications. Many of these PRA applications have been examined through pilot applications initiated by STUK and conducted in full co-operation with the licensees. STUK has also developed a powerful and versatile PRA code (FinPSA) for model development, calculations and review purposes. In the course of risk informing the safety regulation, STUK initiated several research projects, such as methodology development for fire risk analysis (experiments, modelling tools, fire propagation analyses, probabilistic fire simulation), software reliability studies and modelling of severe accidents.

3. Examples of risk informed design

3.1 Use of PRA during the design of OL3 EPR

Even though the EPR design is based on deterministic rules and standards, PRA has systematically been utilized during the design process to optimize the design with respect to safety and availability. First, the PRA covered only internal initiators at Level 1, but soon it was complemented with a Level 1+ model to assess the containment phenomena and accident mitigation measures. For the OL3 construction license application, PRA was further developed towards a full scope Level 1 and 2 analysis, in order to meet Finnish requirements.

EPR design includes several features strongly contributing to low risk and well balanced design of a nuclear power plant. Examples of such design features include:

- Four redundant, separated safety trains (divisions)
- Diversity in systems design and safety functions
- Physical separation against internal & external hazards
- Station Black-Out (SBO) diesel generators (diverse of EDGs)
- Reactor Coolant Pump (RCP) stand-still seal system, back-up for normal seal system
- Double-wall containment with steel liner
- Severe accidents are taken into account in design (e.g. cooled corium spreading area and dedicated severe accident mitigation systems)

Furthermore, the design of the OL 3 systems is based on the following principles:

- Each system needed to support reliable normal operation has at least two trains (2x100%). Therefore no single failure is expected to initiate a plant wide transient
- For controlling anticipated operational transients, and also many class 1 postulated accidents, functional diversity is required. Both of the respective systems have to fulfill the single failure criterion.
- For controlling postulated accidents, there are four-redundant subsystems with capacity of 50 to 100% (depending on the accident type), and thus at least two subsystems can be lost without loss of safety function.
- The systems designed for severe accident management shall fulfill the single failure criterion.

Probabilistic tools have proven to be very useful in identifying potential design weaknesses, optimizing the design by exploring the safety benefits of various design alternatives taking also into account economy. Examples of risk informed design modifications and identified issues in OL3 are briefly discussed in the next Chapter.

3.2 Examples of Risk Informed Design Modifications in OL3

During the pre-licensing phase, following design changes were made mainly based on STUK's remarks on EPR conceptual design and discussions between regulatory body, power utility and the vendor:

- Emergency Boron System (EBS) capacity to meet N+2 failure criterion (additional redundancy added, now 3x100% capacity)
- Safety injection System capacity to meet N+2 failure criterion
- Leak tightness of inner containment - a steel liner added
- Containment heat removal system capacity to meet single failure criterion (N+1)
- Primary circuit was provided with pipe whip restraints to limit loads resulting from large breaks (to complement LBB)
- Diversity of safety systems was improved, e.g., emergency feed water and emergency core cooling systems (ECCS): component cooling, power supply, SBO-diesel backup)
- Hard-wired back-up system of digital I&C for the most important functions
- Separation of safety related systems and components was improved
- Arrangements for removal of fuel from the reactor after LOCAs
- Simplification of the phases of molten core handling by removing the need for layer flip (flip of metal and oxide layers when transported from the reactor to the corium spreading area)

In addition, the following remarks were made by STUK:

- Primary to secondary leakage prevention - no release of coolant to the atmosphere (prim. and sec. pressure reduction)
- Design of the recirculation of the safety injection system (containment sump design)
- Highest design burn-up difficult to license
- New physical protection requirements
  - Aircraft crashes: large passenger jet as design basis
  - Chemical and biological weapons and electromagnetic pulses (HEMP) and microwave beams

As a result of the regulatory review of construction license documentation additional changes were required to the original plant design. Some of these modifications and identified issues are briefly discussed below.

Risk informed changes and issues related to internal hazards (fires & floods)

Some issues concerning the concept of physical separation emerged in STUK`s review 2004 for construction license. Main concern was the existence of heavy fire loads, e.g. the lubrication oil system of RCP motors and FRNC-cables planned to be installed without fixed fire extinguishing systems. Fire separation concept by fire compartmentation is not complete in certain areas as in reactor containment, reactor building annulus and in control room areas. According to Reg. guide YVL 4.3, STUK required specific fire analysis for reactor containment, reactor building annulus and MCR where all safety divisions (e.g. power and I&C-cables) are located in the same fire compartment.

Based on the results of fire analyses, fire separation of safety divisions in the reactor building annulus is implemented by vertical and horizontal fire barriers by mineral wool elements, which were not included in the original design.

In reactor containment, one RCP contains more than 1000 liters lubrication oil in total. Burning of big amount of oil is not acceptable and shall be prevented by strict means. Applied defense in depth concept covers additional double casing oils systems to collect oil leaks, drainage on pump room floor, fire detection, CCTV-cameras, water deluge extinguishing system by manual actuation in MCR, RCP protection & monitoring on vibration, bearing temperature etc.

Fire loads in many cable rooms and tunnels are very heavy and the defense in depth concept is required to prevent long term fires which could endanger integrity and function of fire compartments. STUK kicked off FRNC-cable fire safety research with Technical Research Centre (VTT) in 2004. A representative set of power and I&C FRNC-cables, to be installed at OL3, have been tested at VTT: cone calorimeter tests, thermogravimetric analysis (TGA), differential temperature analysis and differential scanning calorimeter (DTA/DSC) have been applied. In addition, fire spreading tests have been made by the new testing device for vertical cable specimen (2 meters in length), which is heated up to different temperatures and then ignited by a burner.

VTT developed a multilayer cable fire model for one FRNC cable type and performed fire simulations (CFD simulation by FDS code) for a typical cable tunnel and cable spreading room including sensitivity studies (boundary conditions for ignition and fire spreading along the cables; also different pilot fires and ventilation conditions were varied). The results pointed out sensitivity on air flow provided by ventilation system which was modeled in a simplified way due to the limitations of the FDS code. The results indicated that long-term fires are not probable, if room ventilation is stopped and room is isolated i.e. fire damper and fire door closed. The smallest initial fire causing fire ignition and spreading on FRNC cables was not estimated exactly but the critical heat release rate was expected to be quite high (even some MWs/several minutes) based on the fire simulations performed so far.

The cable spreading area below the main control room will be equipped with a gas fire extinguishing system (manual start from the MCR). Cables of all four divisions are located in this area. Other heavy fire loads as DGs, DG fuel tanks, oil filled big transformers, TGs lubrication oil spreading areas are protected with water extinguishing systems with automatic actuation.

Major flood sources in safeguards buildings are service water systems, intermediate cooling circuits and fire water systems. Flood spreading between safety divisions is primarily designed to be prevented by water tight barriers below ground level. However, in many areas prevention of flood spreading is provided by flood drainage and flood alarm systems, and in addition by operator measures of stopping pumps and isolating of leaking system. Additionally, the physical protection against floods was improved in essential service water pumping stations.

Risk informed changes and issues related to external hazards

Loss of sea water cooling due to frazil ice or algae is a potential risk at Finnish NPP sites. The original design of OL3 from the beginning covers some specific features to prevent these risks. Water intake for service water system is possible to switch to outlet channel. For prevention of frazil ice formation, dedicated anti-icing system have been designed to pump warm water to inlet channel and to heat coarse bar screens by electricity.

In winter time, a heavy snow storm may block DG air intake(s). This is a potential risk since a simultaneous LOOP due to high wind may occur. Diesel generator air intakes have been modified to prevent snow blockage and in addition alternative air intake is possible from inside the building.

Other design changes and issues identified

- Process Systems
  - Provisions for cooling in case of Loss of Ultimate Heat Sink (72 hours) - feed to EFWS tanks from Demineralized water system and fire water systems
  - Diversification of containment isolation valves
  - Modification of SGTR management to minimize direct releases to environment
- Electrical systems
  - Gas turbine plant to improve reliability of the off-site AC power supply to the site
  - Additional manual start-up and control power supply for SBO diesel generators
- I&C systems

  - Diversification of priority and actuator control (PAC) modules
  - Diverse safety injection system start-up signal (from SAS)
- To decrease the importance of Safety Chilled Water System (QKA), the room cooling in safeguard buildings was diversified by adding new heat exchangers cooled by CCWS
- Changes to Severe Accident Management
  - Additional primary system depressurization valve to meet single failure criterion
  - Reliability of hydrogen management was improved (arrangements to improve hydrogen distribution)
  - Separate pressure sensors (hot leg and containment) were introduced for design basis accidents (DBA) and severe accidents
  - Additional temperature measurements were introduced in the reactor pit and corium spreading area to follow fulfillment of SAM measures
  - Reliability of electric supply for SAM loads was improved by separating the supply from DBA supplies. In addition, dedicated 12 hour batteries were introduced in division 1 and 4 to supply power in the early phases of the accident (I&C, isolation valves, depressurization)
  - Design of corium spreading area hatch (aluminium)

4. Use of PRA during construction and commissioning

4.1 Risk Informed Pre- and In-Service Inspections (RI-PSI/ISI)

OL3 will be the first new NPP in the world to fully apply risk informed methodology for the development of pre- and in-service inspection programs for both the safety classified and the non-safety classified piping. Methodologies for RI-PSI/ISI applications have been developed for approximately 20 years. So far, these methodologies have only been applied to existing NPPs and the detailed guidance concerning their application to new NPPs is still in progress. This has imposed great challenges for the regulatory body, licensee and the vendor in ensuring the adequate scope and coverage of OL3 inspection programs when combining the traditional approach with risk informed.

It is stated in the regulatory guides YVL 2.8 and YVL 3.5 that the insights of PRA must be used in the development of the pre-service and in-service inspection programs for piping (RI-PSI/ISI). Related to pre-service inspections, the risk informed approach shall be applied to safety class 2 (SC2) piping to at least 7,5% of the total number of SC2 welds/targets. Inspection coverage in safety class 1 is 100%. Risk informed methodology for in-service inspections shall be applied for both the safety classified (SC1-SC3) and non-Safety classified piping (EYT class). Methodological approaches presented in *ASME XI, appendix R* can be used as a reference in RI-PSI/ISI applications. Combining the consequence evaluation by PRA and the estimation of degradation potential, taking into account the secondary impacts of pipe breaks, the inspections are focused on risk significant piping segments. The limitation of radiation doses (ALARA principle) shall also be taken into account by focusing inspections and optimizing inspection periods.

For OL3 NPP, a preliminary RI-PSI program has been developed by the vendor. After the initial screening, mainly based on the exemptions rules from the ASME Section XI, altogether eleven out of 40 systems containing SC2 piping were analyzed. The risk informed process identified potentially important inspections locations on nine systems. This reduced scope was the basis given to an Expert Panel in charge of the selection of the welds to be included in the RI-PSI program. Wide technical expertise was presented in the expert panel: layout, PRA, system design, degradation mechanism, in-service Inspection, non destructive examination (NDE) and radiation. As a result of the expert panel process, 62 welds were added to the inspection scope. Thus, the preliminary pre-inspection scope is now 223 welds, which corresponds approximately to 12.7% of the total number of SC2 inspectable welds/targets defined with all exemption rules from ASME XI.

The latest update of OL3 RI-PSI program, currently under review by STUK, addresses the level 2 PRA results, high energy line break studies, shutdown analysis, and identification of risk outliers, as required by STUK. The same methodology will be applied to risk informed in-service inspection program.

4.2 Risk Informed Technical Specifications (RI-TS)

Regulatory guide YVL 2.8 states that the requirements and conditions for operation set forth in Tech Specs shall be assessed with the help of PRA. The assessment shall include the optimization of the test intervals and test strategies of components and systems as well as the assessment of the allowed outage times (AOT). PRA has to be used for identifying such situations in which the transition to other operating mode may cause higher risk than that of continuing power operation and fixing the failures. Hence, the PRA has to include the modeling of transition phases, such as planned shutdown. A method for risk informed Tech Specs has been developed for OL3 and a draft application has been submitted to STUK.

4.3 PRA Support for Safety Classification

According to Finnish regulations, the functions important to the safety of the SSC of a nuclear power plant shall be defined and classified according to their safety significance. PRA shall be used to support the Safety classification of SSCs.

In the classification process of OL3 SSCs, some changes were made based on PRA insights. For example, the component cooling water system and essential seawater system classification was upgraded from SC3 to SC2 and reactor coolant pump trip breakers from SC4 to SC2. The safety classification document was reviewed already in conjunction with the application for a construction licence and it will be re-assessed during construction in case of substantial design modifications or changes in the PRA model followed by additional re-assessment in operating license phase. In case PRA results suggest a high safety significance for a system, the changing of safety class can also be avoided by modifying the design, e.g. by adding redundancy or diversity.

PRA assessment shall also be used to demonstrate that the requirements for quality management system concerning the safety classification of each component are in accordance with the risk importance of the component (Graded QA approach).

4.4 Other Risk Informed Applications

Optimization of on-line maintenance

The insights of PRA must be applied in drawing up a program for the on-line preventive maintenance. Accordingly if the licensee wants to perform preventive maintenance work during operation, an acceptable risk impact of on-line preventive maintenance program must be demonstrated. For OL3 NPP, the flexibility in maintenance planning is possible, since most of the systems have four trains, thus fulfilling the single failure criterion and most limiting failure combination, even when one redundant train is under maintenance during power operation.

Staff Training

The results of PRA must be taken into account in the planning of personnel training. The most important accident sequences and significant operator actions in terms of risk have to be trained at least in the period of three year. In the planning of training of maintenance crew, attention needs to be paid to risk significant measures identified in the context of HRA.

Procedures

In order to ensure the coverage of disturbance and emergency operating procedures, PRA must be used to determine those situations for which the procedures shall be drawn up. Accordingly, in case shortcomings in the coverage would appear, the licensee has to write new Emergency Operation Procedures (EOP) to provide guidance for operators to better manage certain accident sequences which the PRA indicated to be of high importance to risk.

Use of PRA in Commissioning

OL3 commissioning is divided into five phases: pre-operational tests in phase A and B, nuclear commissioning tests in phase C and D, and finally a demonstration run in phase E. STUK has required that PRA shall be used to assess the adequacy and coverage of the phase and system commissioning programs of OL3 NPP. Also the potential risks related to commissioning tests during nuclear test phase, shall be assessed with the help of PRA. In case the risk related to a specific test is relatively high, potential measures to reduce the risk should be discussed. Risk reduction measures could include for example following considerations:

- development of specific test procedures and additional precautions, e.g.
  - the test may be replaced by another test
  - the test may be shifted to the non-nuclear commissioning phase B
  - adequate information may be received from other tests
- reducing the test related risk by decreasing the probability of potential disturbances or by strengthening the plant response by e.g. additional testing of redundant/diverse system functions

The licensee will submit risk assessments related to OL3 commissioning tests as a part of phase and system commissioning documentation.

5. Conclusions

For more than 20 years, STUK has actively promoted the use of PRA in risk informed safety management. In Finland, PRA is a licensing document, which shall be included in both the construction license and the operating license applications. PRA shall be plant specific and cover full range of potential initiating events and operating modes and it has to be used to demonstrate the plant's compliance with the probabilistic design objectives for core damage frequency CDF and large release frequency (LRF), and that the foundation of the plant design is fit and the norms used are adequate. In OL3 project, risk informed approach has been applied on a large scale for the first time in the design, construction and commissioning of a new NPP unit.

After the construction license was granted for OL3 NPP, STUK has continued intensive regulatory control of the detailed design process of SSCs and construction of the plant. While the construction work progresses, the role of PRA and risk informed approach in the oversight process increases significantly. Already prior the OL3 NPP Project, requirements had been set forth to extend the use of PRA to various risk informed applications. The objective is to enhance the effective implementation of risk informed safety management at the NPPs and also to increase risk awareness and risk informed regulation at the regulatory body. In OL3, the risk informed approach has been applied in several areas during the design and construction of OL3, e.g. supporting the detailed design of SSCs, ensure adequate provisions against internal and external hazards, definition of pre-service and in-service inspection programs, evaluation of the safety classification of SSCs, development of procedures, training of NPP staff and in definition of risk informed technical specifications, periodic testing (in-service testing), on-line preventive maintenance programs. Further, the experience gained from STUK´s oversight activities with the operating NPPs as well as during the OL3 licensing process have clearly shown that risk informed regulation and safety management contributes largely to strengthening of safety, reducing of licensee’s burden and increasing of public confidence.

CSNI/WGRISK Workshop on PSA for New and Advanced Reactors
OECD Conference Centre, Paris, France
20 - 22 June 2011

Role of PRA in New NPP Projects

A. Julin, J. Sandberg and R. Virolainen
Radiation and Nuclear Safety Authority (STUK),
Helsinki, Finland

Index of presentation

1. Introduction
2. Risk Informed Licensing Requirements
3. Use of PRA in Licensing Process
4. New NPP Projects
5. Concluding remarks

1.1 Introduction

- **In Finland, the foundation for the risk informed decision making is set forth in the nuclear safety legislation**
- **The detailed requirements for conducting the PRA and use of PRA applications are set forth in Regulatory Guides issued by STUK**
- **PRA has to be applied already in the early design phase and is to run all through the plant service time, covering construction, commissioning and operation phases**

1.2 Introduction

- **STUK has actively promoted the use of PRA in risk informed safety management for more than 20 years**
- **Several PRA applications have been required in Regulatory Guides as a condition for construction and operating licenses**
- **During the past decade, more requirements have been set forth to extend the use of PRA to various risk informed applications**
  - Many of the these PRA applications have been examined through pilot studies initiated by STUK
  - STUK has also developed a powerful and versatile PRA code (FinPSA) for model development, calculations and review purposes

1.3 Introduction

Deterministic and probabilistic approaches work in parallel and interact

- results of deterministic assessment provide input for PRA models and data
- PRA provides insights on adequacy and focus on deterministic assessment and criteria
- PRA provides insights on the need to improve the reliability of safety functions and plant systems

⇨ PRA complements the deterministic approach and determines the appropriate extent of Defence-in-Depth

2. Risk Informed Licencing Requirements (1/4)

- **Nuclear Energy Degree level: Applicant has to submit to STUK**
  - **Design phase PRA while applying for a Construction Licence**
  - **PRA while applying for an Operating Licence**
  - **Government Decision level: Nuclear power plant safety and design of its safety systems shall be substantiated by PRA**
    - **Regulatory Guide level: Detailed requirements on PRA and its applications have been set forth in the regulatory guides**

2.1 Risk Informed Licencing Requirements (2/4)

- Full scope plant specific PRA (Level 1 and 2)
  - Internal initiators, fires, internal flooding, harsh weather conditions and seismic events
  - Full power and shutdown modes
- Design Phase PRA and PRA for new unit are performed by vendor in close contact with the applicant
  - Several risk informed applications
- Thorough regulatory review
  - STUK personnel performs reviews
- Continuous updating to reflect the actual plant configuration

2.2 Risk Informed Licencing Requirements (3/4)

- **PRA is formally integrated in the licensing process of NPP**
  - Acceptable Design phase PRA is a prerequisite for issuing a Construction Licence
  - Acceptable PRA is a prerequisite for issuing an Operating Licence
  - Design Phase PRA and PRA have to demonstrate that the plant meets the numerical design objectives
    - Core Damage Frequency < 1E-5/a
    - Large Release Frequency < 5E-7 /a

2.3 Risk Informed Licensing Process (4/4)

Decision in Principle on the construction of a NPP unit (Political decision)
- "a new NPP is in line with the overall good of society"
- Applicant of a licence performs an Environmental Impact Assessment (EIA)
- STUK evaluates in a preliminary safety assessment whether the candidate plant designs fulfill Finnish regulations

Application for a Construction Licence, CDF < 1E-5 /a, LRF < 5E-7 /a
- Submission of Level 1 and 2 Design Phase PRA to STUK and application (Safety classification of SSC, Preliminary RI-ISI method, Preliminary PRA for Decommissioning)
- Evaluation of the acceptability of Design Phase PRA (and applications)
  - Design Phase PRA is to demonstrate that the plant design basis is adequate and design requirements are sufficient

Construction Phase
- Complements to Design Phase PRA and working on applications (RI-ISI, RI-IST, RI-TS, RI-PM, Training, EO Procedures, Safety classification of SSC)

Application for an Operating Licence, CDF < 1E-5 /a, LRF < 5E-7 /a
- Submission of Level 1 and 2 PRA and applications to STUK
- Evaluation of the acceptability, ensure the conclusions made in the design phase PRA
- set a basis for the risk informed safety management

Operation Phase
- Utilization of PRA during operation and updates (Plant modifications, RI-ISI, RI-IST, RI-Tech Specs, RI-PM, Training, Procedures, Incident and Event Analysis, PRA for Decommissioning)

Requirements for a Construction License Application 1/2

Draft Regulatory Guide YVL A.7 (and Regulatory Guide YVL 2.8)

#	PRA Submittal	To STUK
	Design Phase PRA Level 1 and 2, documentation and computer model – full Scope - internal events, internal & external hazards – demonstrate that the plant design basis is adequate and design requirements are sufficient • balanced plant design – operating experience from similar type of plants • if not available, expert judgment, experience and information from corresponding applications or sites – quantitative design criteria has to be met CDF ≤ 1E-5 /a, LRF ≤ 5E-7 /a – upgrade of PRA and/or the plant design	For acceptance
	PRA assessment of the safety classification of SSCs, incl. methodology description (together *with Safety Classification Document)*	For acceptance

Requirements for a Construction License Application 2/2

Draft Regulatory Guide YVL A.7 (and Regulatory Guide YVL 2.8)		
#	**PRA Submittal**	**To STUK**
	Preliminary Risk Informed PSI/ISI Methodology Description	For information
	Preliminary risk assessment for decommissioning phase – risk of fuel damage and potential radioactive release shall be considered in the plant design (e.g. fuel cooling system dependencies, transportation, handling, storages) – systems shared between NPP units	For information (a separate analysis)

Requirements for a Construction Phase (prior to operating license application)

Draft Regulatory Guide YVL A.7		
#	**PRA submittal**	**To STUK**
	Update of PRA model and documentation: a) Updated system analyses, FMEAs, importance measures and fault tree models b) Level 1 and 2 computer model, basis for modifications and update of results	For information, incl. in system pre-inspection documentation and modification plans For information annually or more often
	PRA assessment of the safety classification of SSCs – if significant changes have been made during construction	For information
	Risk informed Tech Specs (scope and balance) – all operating modes – continued operation vs. shutdown risk	For information (methodology and application)
	Risk informed ISI, RI-IST, preventive maintenance, training program, disturbance and emergency operating procedures	For information as a part of each application (including methodology)

Requirements for a Operating License Application 1/2

Draft Regulatory Guide YVL A.7		
#	**PRA Submittal**	**To STUK**
	Final full scope plant specific PRA Level 1 and 2 documentation and computer model – ensure the conclusions made in the design phase PRA – set a basis for the risk informed safety management – quantitative design criteria has to be met CDF≤ 1E-5 /a, LRF≤ 5E-7 /a – upgrade of PRA and/or the plant design	For acceptance

Requirements for a Operating License Application 2/2

Draft Regulatory Guide YVL A.7		
#	**PRA submittal**	**To STUK**
	PRA assessment of the safety classification of SSCs	For acceptance
	Risk informed Tech Specs (scope and balance) – all operating modes – continued operation vs. shutdown risk	For acceptance (application)
	Risk informed ISI, RI-IST, preventive maintenance, training program, disturbance and emergency operating procedures	For acceptance as a part of each application

Requirements during Operation 1/2

Draft Regulatory Guide YVL A.7		
#	**Documentation**	**Delivery to STUK**
	Assessment of the risk impact of a plant modification	For acceptance as a part of pre-inspection documentation
	Update of SSC safety classification assessment (if changes)	For acceptance
	Risk assessment of annual outages	For information
	Risk informed Tech Specs (exemptions and needs for change)	For acceptance
	Risk informed ISI, IST, preventive maintenance, training program, improvements of plant life management and quality management programmes	For acceptance as a part of each application.
	Risk informed development of disturbance and emergency operating procedures and training programmes	For information
	Update of PRA documentation and computer model	For acceptance annually or more often.
	PRA related procedures and instructions (e.g. use of PRA and its applications).	For information
	- Log book of changes made to PRA model, basis for changes and impact on results. - Computer model	For information regularly & in significant changes For information in significant changes

Requirements during Operation 2/2

Draft Regulatory Guide YVL A.7		
#	**PRA submittal**	**To STUK**
	Risk assessment for decommissioning phase – risk of fuel damage and potential radioactive release shall be considered in the plant design (e.g. fuel cooling system dependencies, transportation, handling, storages) – systems shared between NPP units	For acceptance (well before decommissioning)

3. Use of PRA in Design Process

- **PRA are used to identify strengths and weaknesses of plant design and to demonstrate that**
  - the safety systems are adequate
  - the plant design is well balanced
  - the defense in depth requirement has been realized
  - the risk estimates meet the quantitative criteria
- **In OL3 NPP Project, risk-informed analyses have proven to be very useful in identifying potential design weaknesses and optimizing the design**
- **As a result of risk informed approach, several design modifications were identified and implemented**
  - In addition, risk insights led to further analysis of the adequacy of provisions against internal and external hazards, e.g. fire risks, additional studies (by VTT) on FRNC cables

3.1 Risk Informed design changes in OL3 1/2

- **Fire risks**
  - Changes to MCP design to limit oil spreading and consequences of possible fire
  - Vertical and horizontal walls in the annulus were added between redundant cable routings
  - Cable routings of different redundancies to MCR were separated from each other by fire resistant tunnels
  - Main and auxiliary transformers were provided with sprinkler systems
- **External hazards**
  - Structures to protect diesel engine combustion and cooling air intakes against weather phenomena and external fire
  - Cooling in case of Loss of Ultimate Heat Sink (72 hours) was improved - additional feed to EFWS tanks from DMW and fire water systems
  - Sea water intake coarse bar screens have to be protected with electrical heating against frazil ice blocking

3.1 Risk Informed design changes in OL3 2/2

- **Safety classification changes**
  - CCWS and ESWS active components in cooling chain, SC3 to SC2
  - RCP trip breakers SC4 to SC2
  - the demineralized water system (DMW) EYT to SC4
- **I&C changes**
  - Diversification of priority and actuator control (PAC) modules
  - Diverse safety injection system start-up signal (from SAS)
- **Other changes**
  - Physical protection against floods
    - ESWS pumping stations
    - Flood barriers and drainage in safety building corridors
  - Addition of manual (local) start up of SBOs
  - The room cooling in the safeguard buildings was diversified by adding new heat exchangers cooled by CCWS

3.2 OL3 PRA Applications, *example* 1/3

- **Risk Informed Pre-Service Inspection Program (RI-PSI/ISI)**
  - OL3 will to fully apply risk informed methodology for the development of pre- and in-service inspection programs for both the safety classified and the non-safety classified piping
  - RI-ISI Methodologies have mainly been applied to existing NPPs and the detailed guidance concerning for new NPPs is still in progress
    - ⇨ This has imposed great challenges for the regulatory body, licensee and the vendor in ensuring the adequate scope and coverage of OL3 inspection programs when combining the traditional approach with risk informed
  - Acceptable RI-ISI methods are described in "ASME Code, Section XI Nonmandatory Appendix R"
  - Acceptable application guidelines are given in a European Union report, ENIQ Report nr 23, "European Framework Document for Risk-informed In-service Inspection"
  - While drawing up the risk-informed inservice inspection program, the results must be evaluated by an expert panel
  - In addition to power operation, low power and shut down states and the transfers between them shall be considered in the RI-ISI approach

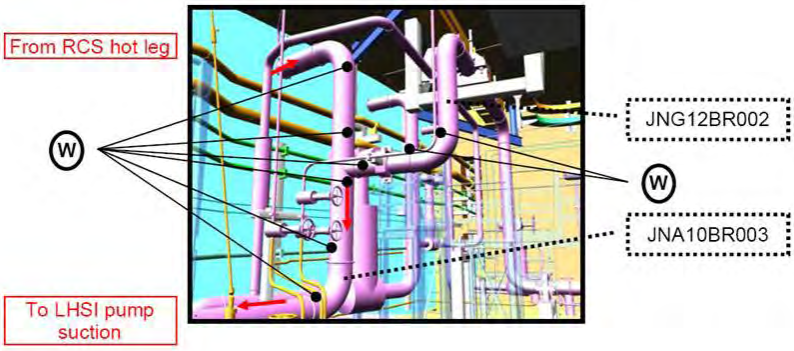
3.2 OL3 PRA Applications, *example* 2/3

- **OL3 RI-PSI/ISI Methodology**
  - A methodology for OL3 RI-PSI/ISI was developed by the vendor
    - Mainly based on EPRI RI-ISI Methodology
  - STUK identified some issued related to the first revisions of the methodology description e.g
    - Inspection scope (number of welds, inclusions of all safety related systems)
    - Assessment of degradations mechanisms (water hammering etc.)
    - Isolation of breaks
    - Spatial analysis: secondary (indirect) effects of pipe breaks (e.g. humidity, temperature, water jets)
    - The role and use of expert panel
  - After discussions between licensee, vendor and STUK, these issues were adequately addressed in the methodology and the revised methodology description was accepted with a few remarks
  - Combining the consequence evaluation by PRA and the estimation of degradation potential, taking into account the secondary impacts of pipe breaks, the inspections can be focused on risk significant piping segments

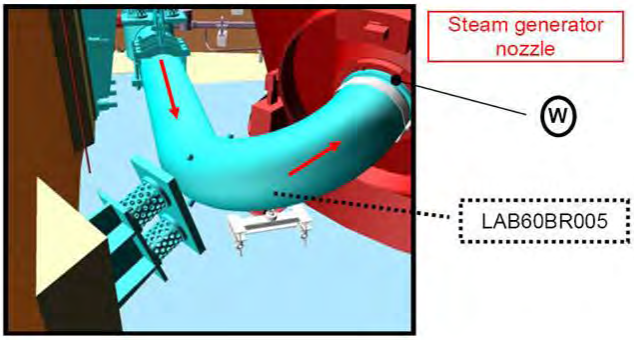
3.2 OL3 PRA Applications, *example* 3/3

- **RI-PSI Program, Preliminary inspection Scope**
  - Deterministic scope for SC2 piping is at least 7,5% of total number of SC 2 welds/targets
  - Inspection coverage in safety class 1 is 100%
  - After the initial screening, mainly based on the exemptions rules from the ASME Section XI, altogether eleven SC2 systems were analyzed
  - Risk informed process identified potentially important inspections locations on nine SC2 systems
  - This scope was the bases given to an Expert Panel in charge of the selection of the welds to be included in the RI-PSI program
    - Technical expertise presented in the expert panel: layout, PRA, system design, degradation mechanism, in-service Inspection, non destructive examination (NDE) and radiation protections
  - As a result of RI-PSI application, the preliminary pre-inspection scope is **223 welds**, which corresponds to ~ 12,7% of all inspectable welds in SC2 systems

Risk Informed Pre Service Inspection targets (Safety Class 2)



Risk Informed PreService Inspection targets (Safety Class 2)



3.3 PRA and OL3 Commissioning

- **OL3 commissioning in five phases: pre-operational tests (A,B), nuclear commissioning tests (C, D) and demonstration run (E)**
- **STUK required PRA to be used to assess the adequacy and coverage of the phase and system commissioning programs, e.g.**
  - Assessment of the potential risks related to commissioning tests during nuclear test phase, including potential measures to reduce the risk
- **Risk reduction measures could include for example following considerations:**
  - Development of specific test procedures and additional precautions, e.g.
    - the test may be replaced by another test
    - the test may be shifted to the non-nuclear commissioning phase B
    - adequate information may be received from other tests
  - Reducing the test related risk 1) by decreasing the probability of potential disturbances or 2) by strengthening the plant response by e.g. additional testing of redundant/diverse system functions
- **The licensee will submit risk assessments related to OL3 commissioning tests as a part of phase and system commissioning documentation**

4. New NPP Projects

- **The Government has granted two DiP's to TVO and Fennovoima (for a single reactor)**
  - The Parliament ratified both granted applications 1.7.2010
- **STUK has continued discussions with license applicants on construction licence application requirements**
  - some principal design issues under review, especially concerning external hazards (see next slides)
- **The applicants shall submit nuclear safety related bid requirements to STUK for information**
  - That is the first step for STUK to prepare regulatory project for construction license review

4.1 New Reactor Projects - Teollisuuden Voima Ltd – OL4

- Environmental Impact Assessment procedure for OL4 (1000-1800 MWe) has been completed by the statement of the Ministry of Employment and the Economy (TEM) in June 2008
- Application for Decision in Principle (DiP) was submitted to the Ministry (TEM) in April 2008
- Feasibility studies with potential vendors
  - ABWR, Toshiba Westinghouse
  - APWR, Mitsubishi Heavy Industry
  - AP1400, KHNP (Korea)
  - EPR, Areva
  - ESBWR, GE Hitachi
- STUK's preliminary safety assessment was issued in May 2009:
  http://www.stuk.fi/

Olkiluoto

SÄTEILYTURVAKESKUS • STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

STUK

4.2 New Reactor Projects - Fennovoima Ltd - FV1

Fennovoima has two Site candidates

- Fennovoima is a new utility that was established in 2007 to construct a nuclear power plant with one or two 1000–1800 MW units in Finland.
- Feasibility studies with potential vendors are ongoing:
  - ABWR, Toshiba Westinghouse
  - EPR, Areva
  - SWR-1000, Kerena ("German BWR"), Areva
- Environmental Impact Assessment procedure for FV1 (1000-1800 MWe) has been completed by the statement of the Ministry of Employment and the Economy (TEM) February 2009
- Application for Decision in Principle submitted in January 2009
- STUK's preliminary safety assessment was issued in October 2009:
  http://*www.stuk.fi/*

Simo, Karsikko

Pyhäjoki, Hanhikivi

Photos: Fennovoima

SÄTEILYTURVAKESKUS • STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

STUK

4.3 Some issues under study for new NPPs

- **Geological and seismic conditions in northern part of Finland**
  - Fennovoima apply seismic design criteria for Pyhäjoki (PGA=0,2 g) and Simo (PGA=0,35 g)
  - with similar logics OL4 would be PGA=0,11 g
  - STUK requested independent assessments from external experts
- **Design basis against harsh environmental conditions**
  - high wind, high&low temperatures, sea water intake blockage (algae, oil, frazil ice)
- **Possibility to apply American standards and products in civil engineering**
  - TVO's application approved with comments on anchorage and crack control of concrete reinforcement
- **Composite construction technology of massive concrete structures for modular construction**
  - TVO apply the possibility to use Japanese standard JEAC 4618-2008 for designing composite steel and concrete walls.

SÄTEILYTURVAKESKUS • STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

STUK

4.4 Determination of the design basis for external events in new NPP projects

- **Design basis earthquake determined with Probabilistic Seismic Hazard Analysis (PSHA)**
  - Annual probability of exceedance 1E-5 with 50 % confidence level
- **For other external events no detailed quantitative requirements are given in current YVL guides**
  - General building code is not sufficient for NPPs
  - Quantitative risk targets provide some guidance
    - core damage frequency < 1E-5/a
    - large release frequency < 5E-7/a
    - no single factor shall dominate
  - Intensity-frequency distributions have been determined based on available observations
    - reliable observations for ~ 100 years
    - return periods of interest up to 10 000 - 1 000 000 years
    - uncertainties are very large at high return periods

SÄTEILYTURVAKESKUS • STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

STUK

4.5 Design basis for meteorological and hydrological events at new NPP units

- Highest and lowest outdoor air temperature and humidity
  - instantaneous, short term, long term
- Extreme wind speed, including tornadoes (trombs) and downbursts
- Precipitation (rain, snow, snow load)
- Lightning peak current, rise time etc.
- Seawater level, extreme high and low
  - all sites are coastal
  - including seiche, surge waves due to geological, meteorological events
  - effects of global climate change, range of estimates
- Seawater temperature
  - high temparature
  - subcooling, frazil ice formation
- Ice conditions, including ice walls
- Combinations of correlated events are potentially important
  - snow and wind: potential for loss of offsite power and simultaneous failure of diesel generators due to combustion air intake blockage
  - high wind and high seawater and impurities in cooling water are correlated: possibility of simultaneous LOSP and blockage of EDG cooling

5. Summary and Conclusions... 1/2

- **Strengths of risk informed process**
  - OL3 design phase PRA proved to be very useful in identifying design vulnerabilities that eventually led to design and procedural changes e.g. in process systems, electrical systems, I&C systems and in fire protection systems
  - During construction, PRA updates has provided valuable insights into the detailed design of SSCs, which eventually led to further design changes
- **Improvements needed**
  - Analyses (PRA & other) were not fully utilised in the design process - unintentional dependencies and shortcomings in design process were found in STUK's review
  - Utilisation of PRA in the technical change management process was not timely, interactive and systematic enough

PRA should be integrated in an iterative design process and not only for demonstration of acceptable risk level after design freeze

5. Summary and Conclusions... 1/2

- **Experiences from OL3 licensing will be utilised in the revisions of nuclear safety legislation and regulatory guides**
- **Use of PRA and its applications in licensing process and during plant life time has been described in more detail in the draft regulatory guide YVL A.7**
  - Submittal and content of required documentation, computer models, methodology descriptions and applications
- **More detailed requirements will be set forth especially concerning the maturity of design and the content and scope of the documentation in various licensing phases, for example**
  - Preliminary justification of adequate provisions and design bases against internal & external hazards already in decision in principle (DiP) phase
  - In Construction License Application
    - Layout planning shall be essentially completed, including adequate provisions (and demonstration) against internal and external hazards
    - Design of Structures and Systems shall be mature enough to facilitate the requirements specification for components

INTRODUCTION OF PSA TEAM WORKS IN CNPE

Zhao Bo, CNPE, China

See the presentation enclosed in this report

Activities Related PSA&SA in CNPE

2011.01.10

第 页

CNPE

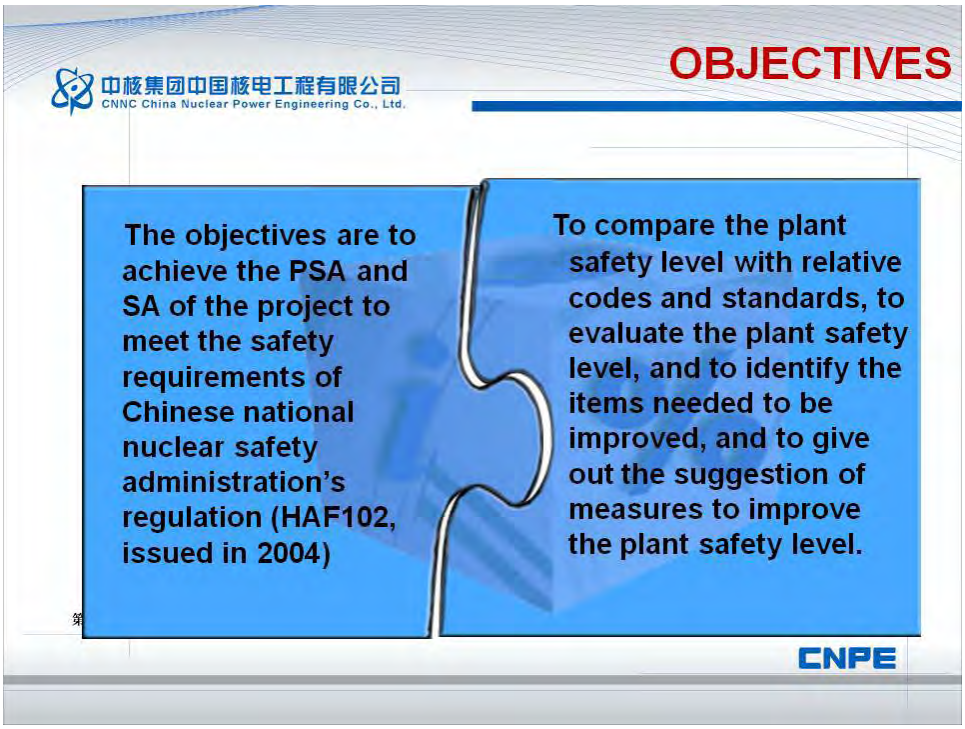
CONTENT

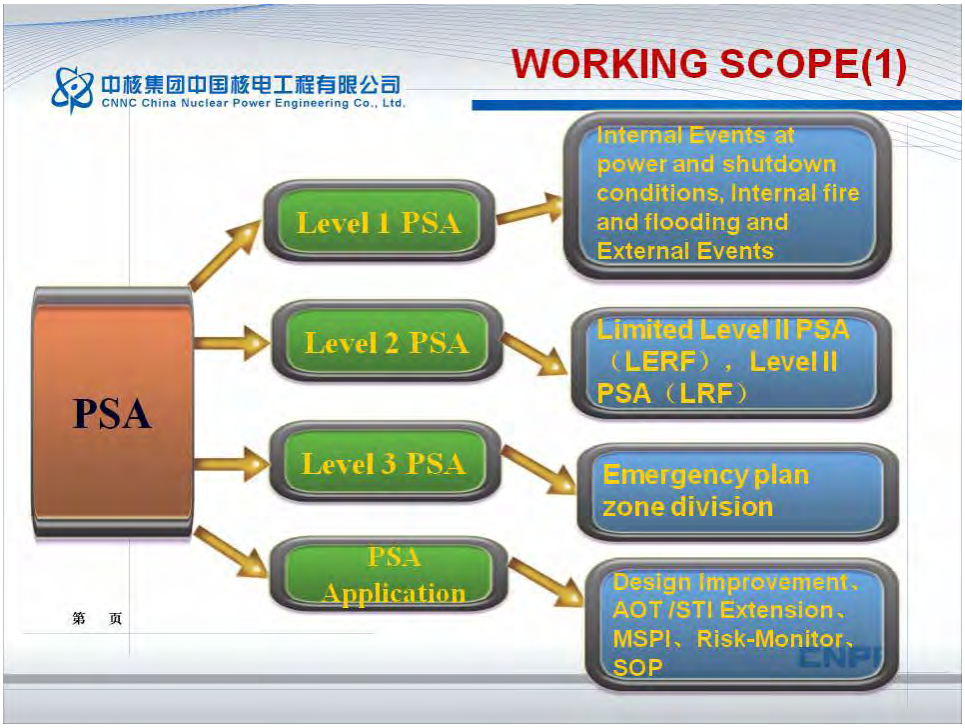
中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

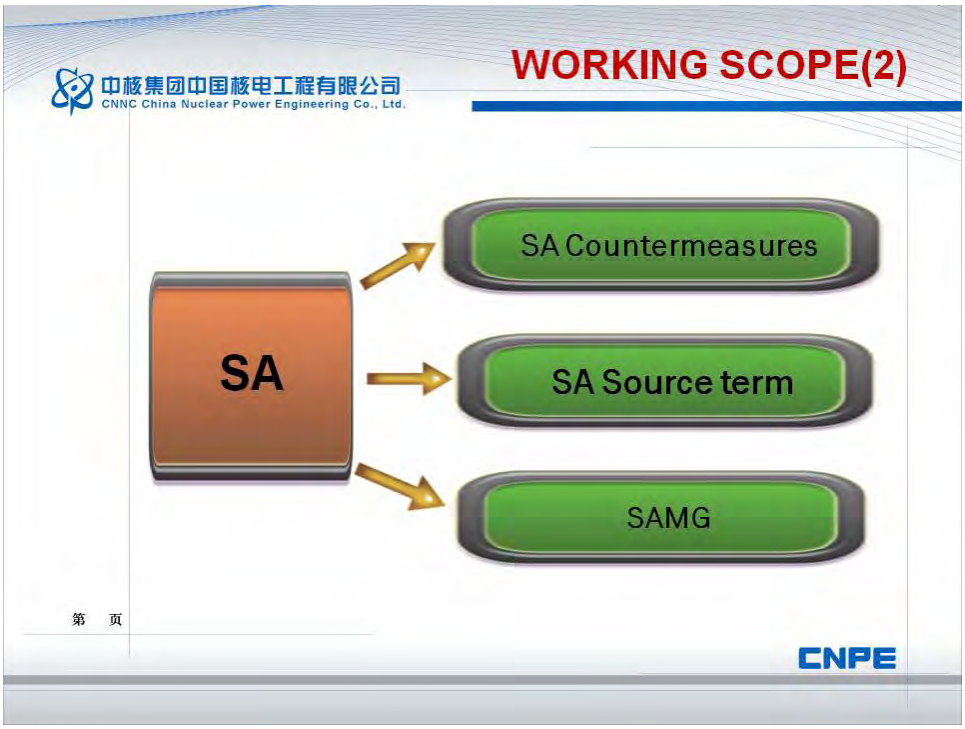
第 2 页

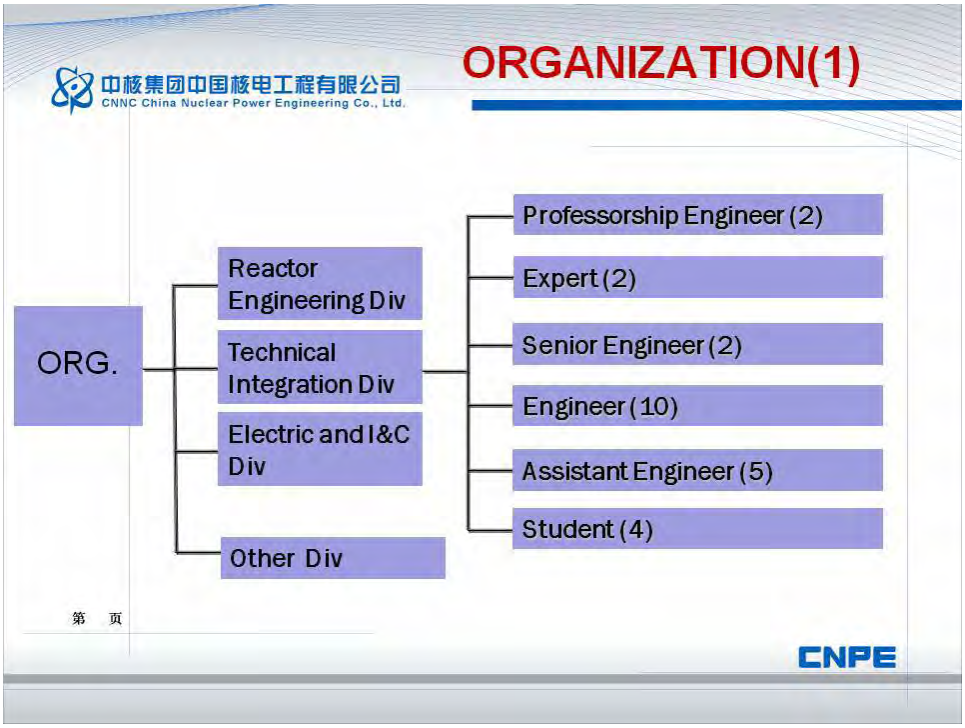
CNPE


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
BACKGROUND
NEW ORGNIZATION ESTABLISHED IN 2004
As the development of the nuclear industry in China, NNSA has issued new regulations (HAF102,issued in 2004) requiring probabilistic safety assessment (PSA) and severe accident analysis for new NPPs
第 页
CNPE


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
OBJECTIVES
The objectives are to achieve the PSA and SA of the project to meet the safety requirements of Chinese national nuclear safety administration's regulation (HAF102, issued in 2004)
To compare the plant safety level with relative codes and standards, to evaluate the plant safety level, and to identify the items needed to be improved, and to give out the suggestion of measures to improve the plant safety level.
CNPE


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
WORKING SCOPE(1)
PSA
Level 1 PSA
Level 2 PSA
Level 3 PSA
PSA Application
Internal Events at power and shutdown conditions, Internal fire and flooding and External Events
Limited Level II PSA（LERF）, Level II PSA（LRF）
Emergency plan zone division
Design Improvement、AOT /STI Extension、MSPI、Risk-Monitor、SOP
第 页


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
WORKING SCOPE(2)
SA
SA Countermeasures
SA Source term
SAMG
第 页
CNPE


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
ORGANIZATION(1)
ORG.
Reactor Engineering Div
Technical Integration Div
Electric and I&C Div
Other Div
Professorship Engineer (2)
Expert (2)
Senior Engineer (2)
Engineer (10)
Assistant Engineer (5)
Student (4)
第 页
CNPE


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
ORGANIZATION(2)
◆Reactor Eng. Division：
thermal-hydraulic calculation support for the successful criteria and time window and severe accident sequences.
◆I&C Division：HRA
◆Other Divisions：Containment structure evaluation 、instrument and equipment assessment 。
◆Technical Integration Division：
Besides mentioned above belong to this division.
Three Groups
PSA Development 、PSA Application、SA&L2PSA
第 页
CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

TECHNIQUE COMMUNION AND COOPERATION(1)

- Periodically inviting internal and external experts to tutor us to meet the work needs
- Though the Inducing Foreign Experts Projects, inviting foreign experts to have academic communication
- Inviting experts to have a peer review in the critical milestones of the projects
- Though the projects co-operation, Inviting foreign experts to give a technical suggestion or sending someone abroad to further study
- Attending international seminar. And developing academic communication with universities and organization, i.e., Tsinghua university、Taiwan Nuclear Institute, etc.
- Frequently visiting the NPPs to have an interview and a technical communication with operation personnel
- Periodically attending other in-company related professional meetings
- Attending EPR、AP1000 review

第 页

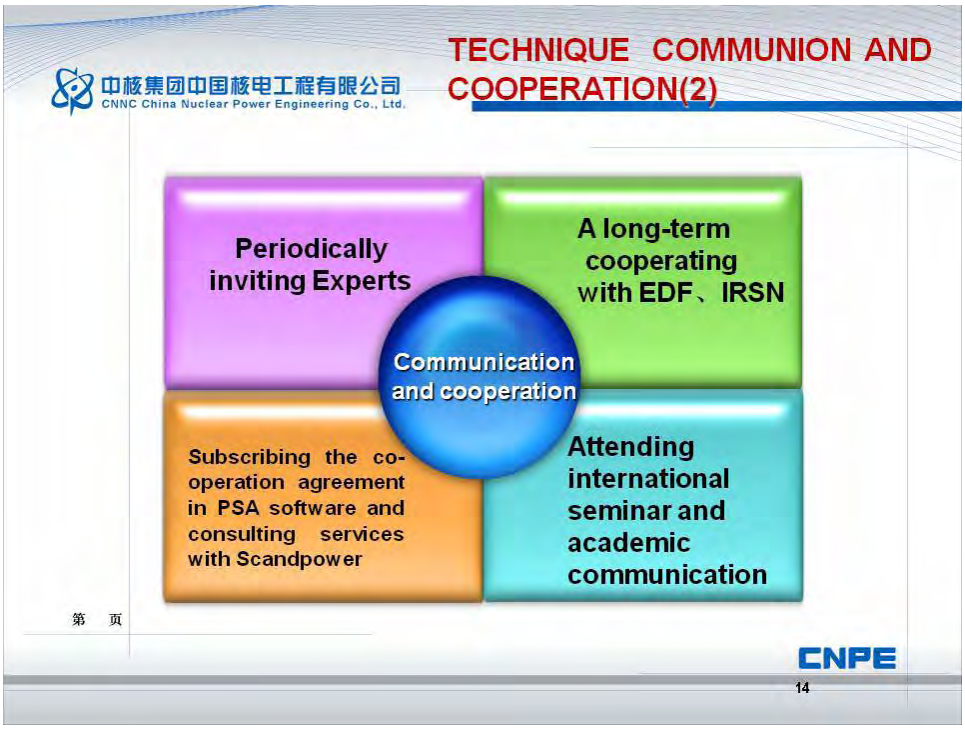
CNPE

CNPE

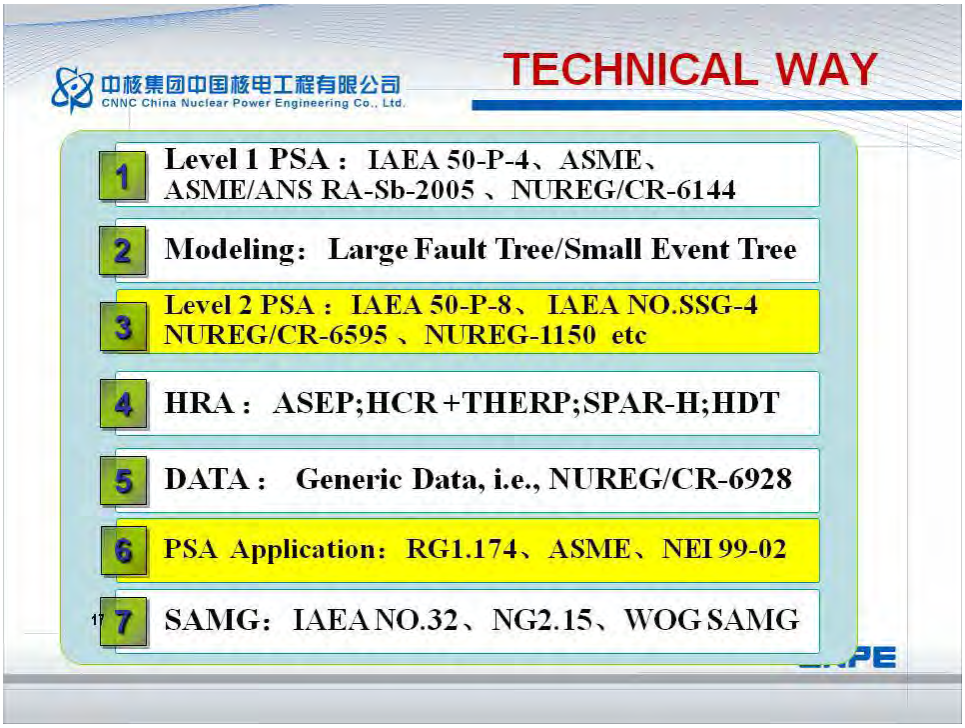
第 12 页

CNPE

13


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
TECHNIQUE COMMUNION AND COOPERATION(2)
Periodically inviting Experts
A long-term cooperating with EDF、IRSN
Communication and cooperation
Subscribing the co-operation agreement in PSA software and consulting services with Scandpower
Attending international seminar and academic communication
第 页
CNPE
14


CNPE和Scandpower PSA软件和应用服务合作框架协议
15
CNPE


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
TECHNICAL WAY
1 Level 1 PSA： IAEA 50-P-4、ASME、ASME/ANS RA-Sb-2005 、NUREG/CR-6144
2 Modeling： Large Fault Tree/Small Event Tree
3 Level 2 PSA： IAEA 50-P-8、IAEA NO.SSG-4 NUREG/CR-6595 、NUREG-1150 etc
4 HRA： ASEP;HCR+THERP;SPAR-H;HDT
5 DATA： Generic Data, i.e., NUREG/CR-6928
6 PSA Application：RG1.174、ASME、NEI 99-02
7 SAMG：IAEA NO.32、NG2.15、WOG SAMG
17


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
WORKING OUTCOMES(1)
Activities Related PSA
Almost , Each NPP has completed Internal Events at Power and LPSD Level 1 PSA
Qinshan Phase II NPPs have completed Limited L 2 PSA(LERF)
Fuqing1/2 and5/6 units are developing Level 2 PSA.
Qinshan Phase II and Fangjiashan NPP are developing fire and flooding PSA study.
Risk-informed Nuclear Regulation taking PSA as one aspect of it's technical basis, which is developing in China. Fangjiashan NPPs have completed some related AOT and STI extend PSA analysis.
Tianwan Phase I and Qinshan Phase II and extend NPPs are developing RM, MSPI and SDP. Tianwan Phase I NPP is developing refueling outage optimization.
第
CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

WORKING OUTCOMES(2)

◆Finished works— PSA

Projects	CDF (POWER)	CDF (LPSD)	Level II PSA
CNP1500	1.10E-5/r·y	N/A	N/A
Qinshan Phase II extension	1.80E-5/r·y		LERF：1.69E-6/r·y
Fuqing 1,2,	8.26E-6/r·y	4.68E-6/r·y	Underway
Fuqing 3,4,	8.26E-6/r·y	4.68E-6/r·y	N/A
Fuqing 5,6,	7.21E-6/r·y	Underway	Underway
Fangjiashan	8.26E-6/r·y	4.68E-6/r·y	N/A
Hainan	7.97E-6/r·y	4.77E-6/r·y	N/A
Tianwan 5,6	8.70E-6/r·y	4.68E-6/r·y	N/A

第 19 页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

WORKING OUTCOMES(3)

◆Finished works— PSA Application

- AP1000 PRA Research and Discussion

PSA Application

- LINGAO Phase II DEL system upgrade PSA support analysis
- Fangjiashan SEC system airplane crash PSA support analysis
- Fangjiashan emergency diesel AOT extension PSA analysis
- Fuqing units 5、6 project design modification PSA analysis

第 20 页

CNPE

WORKING OUTCOMES(4)

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

Finished works— Severe Accident Management

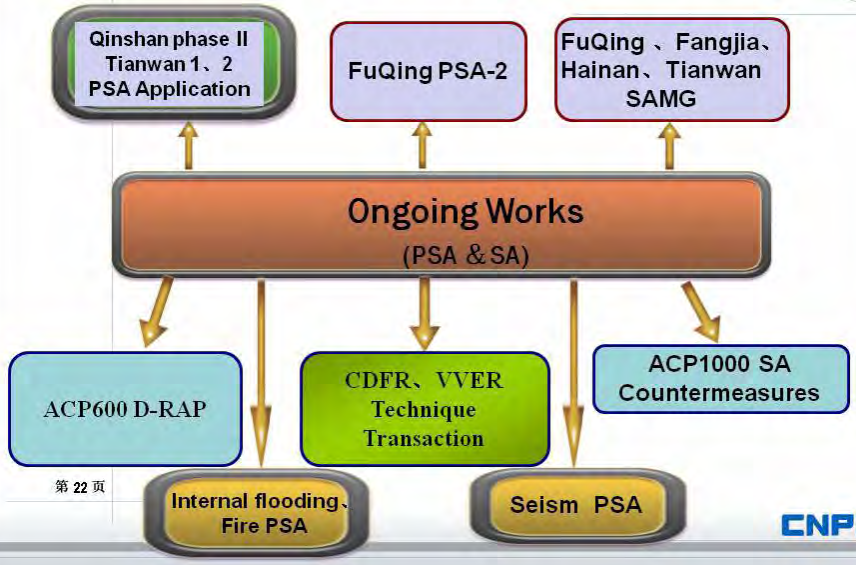
- Qinshan Phase II extension emergency source term analysis
- AP1000 SAMG research and discussion
- Application of MELCOR、ASTEC 、MAAP integrated codes
- 《hydrogen concentration control after accidents 》standard
- SAMG (draft) for the NPPs with two loops
- SAMG (draft) for the NPPs with three loops

第 21

PE

WORKING OUTCOMES(5)

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.



第 22 页

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

WORKING OUTCOMES(6)

◆Ongoing Works ——SAM etc.

SAM
- SAMG update
- SAMG verification and validation
- Three integrated codes cal.(MAAP、 MELOCR、ASTEC）
- Main severe accident sequences and source term analysis

PSA Application:Qinshan phase II 、Tianwan unit 1、2
- MSPI
- SDP
- Risk monitor

23

CNPE

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.

WORKING OUTCOMES(7)

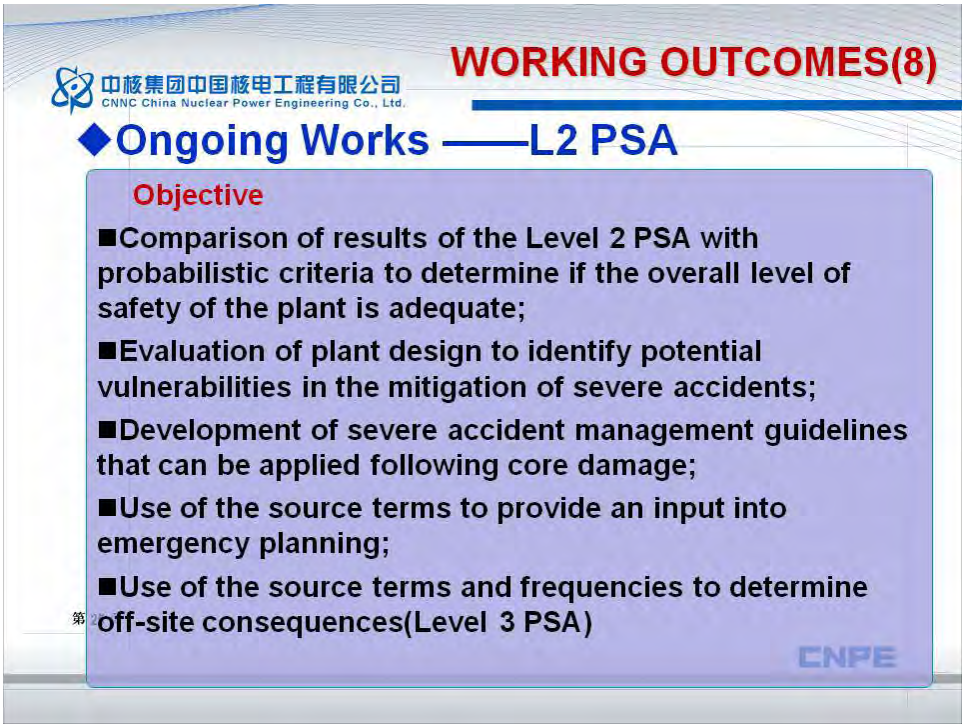
◆Ongoing Works ——L2 PSA

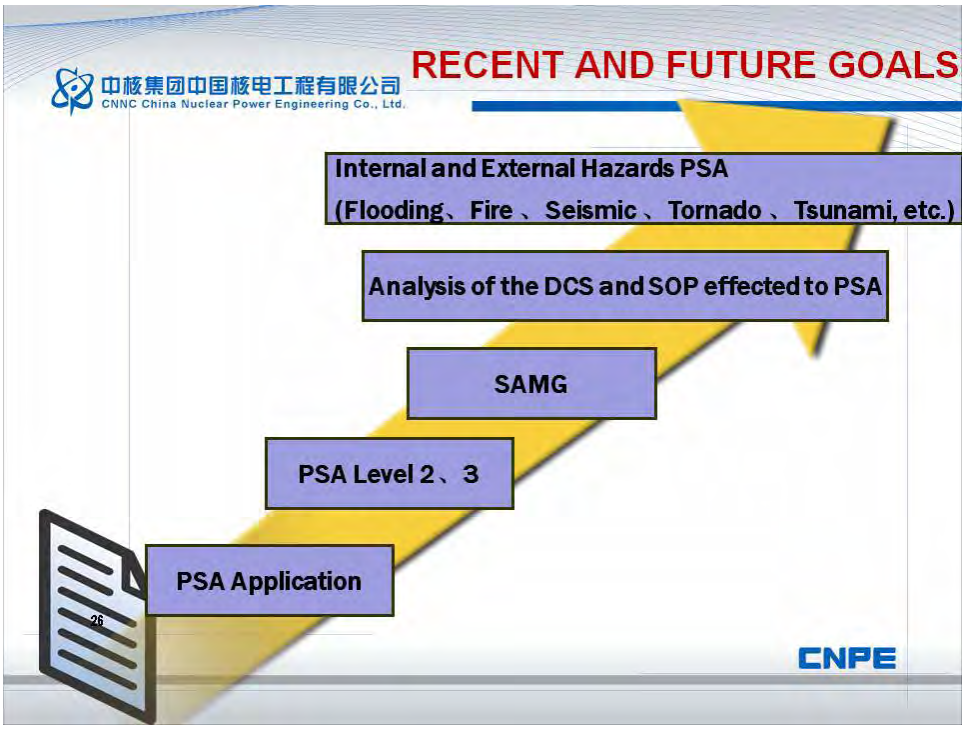
- ◆ NPP：Fuqing 1,2、 Fuqing 5,6
- ◆ Scope: Full power operation，Internal events，Core
- ◆ Probabilistic software： Risk Spectrum
- ◆ Model：Integrated L1-L2 PSA model
- ◆ L2 PSA methodologies:
  IAEA procedures (IAEA 50-P-8、 IAEA NO.SSG-4),
  Plant specific L2 PSA(EPR、AP1000 、NUREG-1150 etc)

第 页

CNPE

24


中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
WORKING OUTCOMES(8)
◆Ongoing Works ——L2 PSA
Objective
■Comparison of results of the Level 2 PSA with probabilistic criteria to determine if the overall level of safety of the plant is adequate;
■Evaluation of plant design to identify potential vulnerabilities in the mitigation of severe accidents;
■Development of severe accident management guidelines that can be applied following core damage;
■Use of the source terms to provide an input into emergency planning;
■Use of the source terms and frequencies to determine off-site consequences(Level 3 PSA)
CNPE

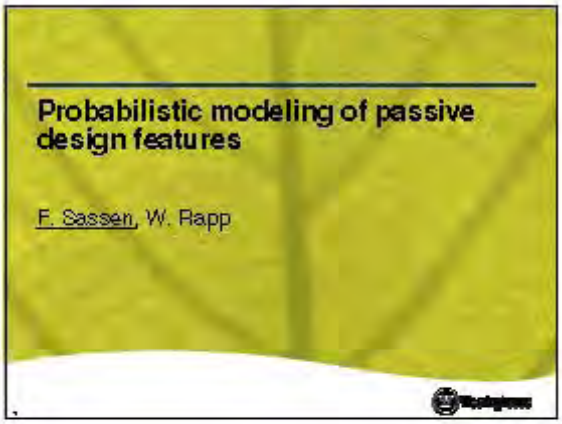

中核集团中国核电工程有限公司
CNNC China Nuclear Power Engineering Co., Ltd.
RECENT AND FUTURE GOALS
Internal and External Hazards PSA
(Flooding、Fire 、Seismic 、Tornado 、Tsunami, etc.)
Analysis of the DCS and SOP effected to PSA
SAMG
PSA Level 2、3
PSA Application
26
CNPE


Thanks for your attention
第 页
CNPE

PROBABILISTIC MODELING OF PASSIVE FEATURES

F. Sassen, Westinghouse, Germany

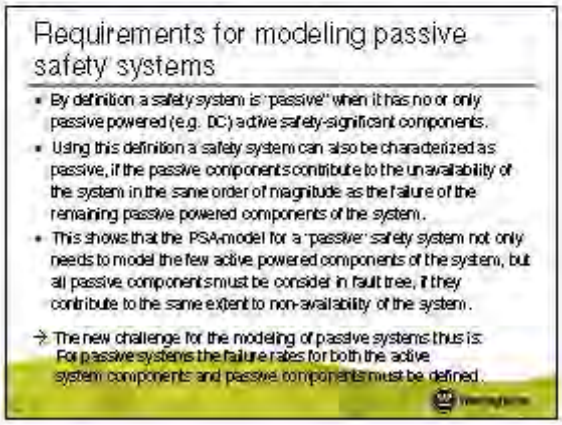
See the presentation enclosed in this report


Probabilistic modeling of passive design features
F. Sassen, W. Rapp


Content
Requirements for modeling:
passive systems (example: AP1000™)
other reactor types than light water reactors:
Application of existing regulations
Approaches of the German HTR-development
Draft regulations
Suggestions
Summary

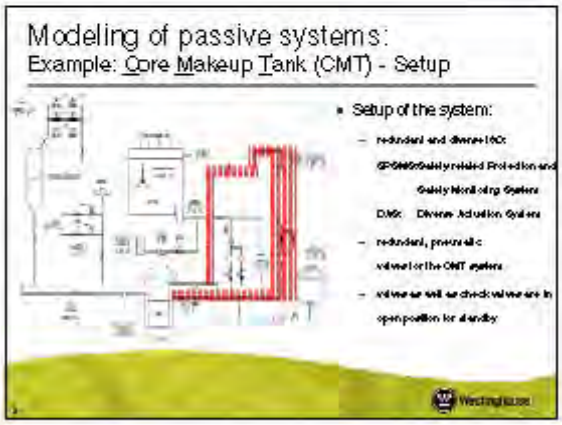
1

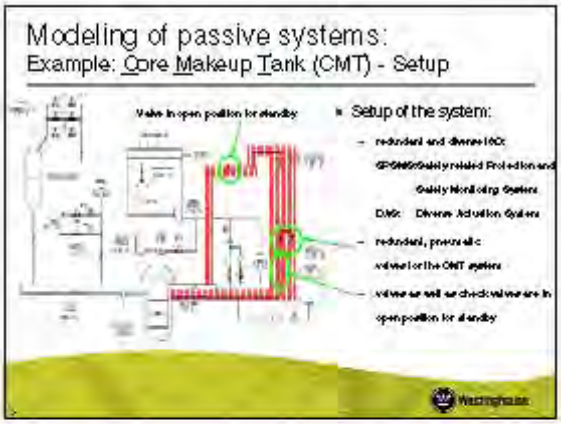

Introduction
• The current PSA-guidelines in Germany can in some aspects only be applied to LWR with active safety systems.
• The application of the relevant PSA-rules on modern future reactor typs (e.g. high temperature reactors) demands an interpretation of these rules.
• The PSA for advanced light water reactors with passive safety features has increased demands on data for the event tree and fault tree modeling.

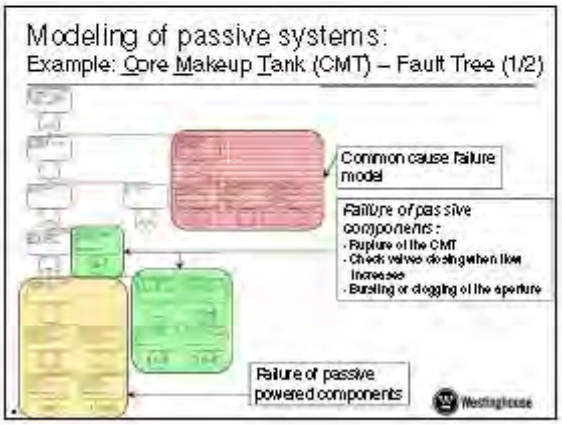

Requirements for modeling passive safety systems
• By definition a safety system is "passive" when it has no or only passive powered (e.g. DC) active safety-significant components.
• Using this definition a safety system can also be characterized as passive, if the passive components contribute to the unavailability of the system in the same order of magnitude as the failure of the remaining passive powered components of the system.
• This shows that the PSA-model for a "passive" safety system not only needs to model the few active powered components of the system, but all passive components must be consider in fault tree, if they contribute to the same extent to non-availability of the system.
→ The new challenge for the modeling of passive systems thus is: For passive systems the failure rates for both the active system components and passive components must be defined.

2


Modeling of passive systems:
Example: Core Makeup Tank (CMT) – Small Leakage

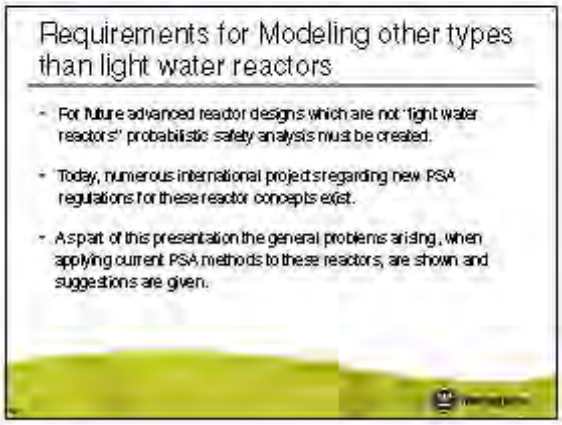

Modeling of passive systems:
Example: Core Makeup Tank (CMT) - Setup
• Setup of the system:

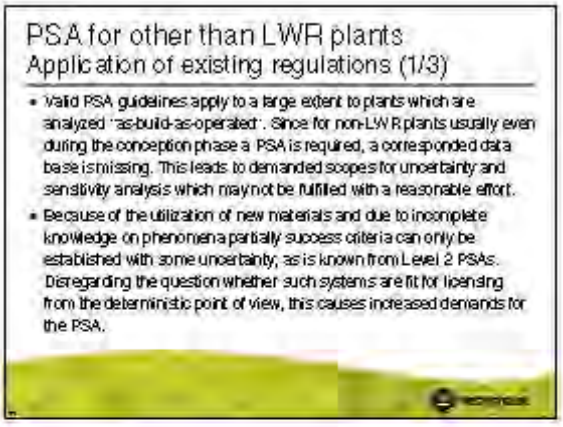

Modeling of passive systems:
Example: Core Makeup Tank (CMT) - Setup
Valve in open position for standby
Setup of the system:
redundant, pneumatic
Westinghouse

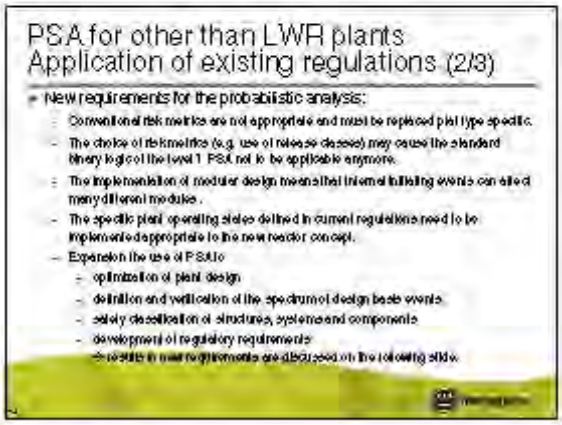

Modeling of passive systems:
Example: Core Makeup Tank (CMT) – Fault Tree (1/2)
Common cause failure model
Failure of passive components :
- Rupture of the CMT
- Check valve closing when flow increases
- Bursting or clogging of the aperture
Failure of passive powered components
Westinghouse

4


Modeling of passive systems:
Example: Core Makeup Tank (CMT) – Fault Tree (2/2)
• Reasons for omitting the motor-driven valve:
• Failure mode of the check valve:
• Example for failure mechanisms, with increased importance in passive systems:


Requirements for Modeling other types than light water reactors
- For future advanced reactor designs which are not "light water reactors" probabilistic safety analysis must be created.
- Today, numerous international projects regarding new PSA regulations for these reactor concepts exist.
- As part of this presentation the general problems arising, when applying current PSA methods to these reactors, are shown and suggestions are given.


PSA for other than LWR plants
Application of existing regulations (1/3)
• Valid PSA guidelines apply to a large extent to plants which are analyzed "as-build-as-operated". Since for non-LWR plants usually even during the conception phase a PSA is required, a corresponded data base is missing. This leads to demanded scopes for uncertainty and sensitivity analysis which may not be fulfilled with a reasonable effort.
• Because of the utilization of new materials and due to incomplete knowledge on phenomena partially success criteria can only be established with some uncertainty, as is known from Level 2 PSAs. Disregarding the question whether such systems are fit for licensing from the deterministic point of view, this causes increased demands for the PSA.

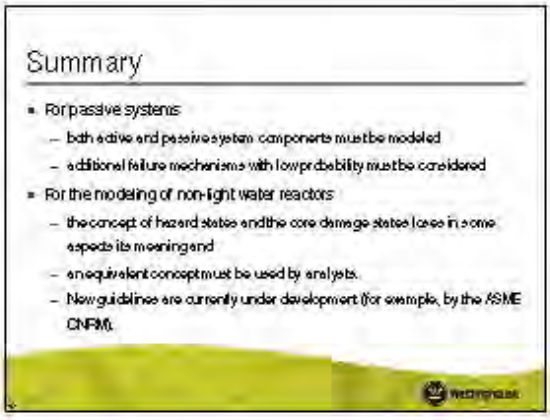

PSA for other than LWR plants
Application of existing regulations (2/3)
• New requirements for the probabilistic analysis:
– Conventional risk metrics are not appropriate and must be replaced plant type specific.
– The choice of risk metrics (e.g. use of release classes) may cause the standard binary logic of the Level 1 PSA not to be applicable anymore.
– The implementation of modular design means that internal initiating events can affect many different modules.
– The specific plant operating states defined in current regulations need to be implemented appropriate to the new reactor concept.
– Expansion the use of PSA to
– optimization of plant design
– definition and verification of the spectrum of design basis events
– safety classification of structures, systems and components
– development of regulatory requirements
→ results in new requirements are discussed on the following slide.


PSA for other than LWR plants
Application of existing regulations (3/3)
Requirements coming from extended application of PSA:
– Optimization of system designs requires a realistic assessment of reliability data, particularly the data for common cause failure (CCF).
– Suitability for defining the spectrum of design basis events
– Usefulness for development of licensing requirements
– Use of PSA in early design phases, such as for the development of a concept for the new plant type that corresponds to the "defense in depth" concept from the probabilistic point of view.


PSA for other than LWR plants
Approaches from the German HTR-development
As part of the HTR development in Germany PSA applications took place prior to the development of the German regulations.
Use of appropriate metrics instead of releases/damage: For example, the frequency of conditions without residual heat removal from the core for more than 4 hours was used to optimize the emergency core cooling systems.
The PSA works especially for advanced HTR concepts (helium turbine) have shown how successful an extension of the PSA concept to early design phase for reactor concepts can be, even when no experience from existing plants exists.
The PSA workshave shown, how helpful target reliability data for individual system is for achieving design goals. This target may be derived from PSA.


PSA for other than LWR plants
Draft rules and regulations in the U.S.
The PSA guidelines developed in the USA for non-LWR plants take into account in particular:
Using bounding scenarios of the design spectrum instead of core damage frequencies and the use of a set of release categories customized for the reactor design under consideration instead of the Large Early Release Frequency (LERF).
Requirements for the PSA are graded according to risk-informed applications and to the point in the life cycle of the plant.
Extension of ASME PSA standard to include the analysis of plant operating states
If the frequency of internal initiating events can not be derived from operating experience, the frequency of flawed human actions causing an initiating event must be analyzed.
The requirements concerning the reliability analyzes for containment integrity can be extended to fission product barriers in general.


PSA for other than LWR plants
Suggestions
From the experience and background of the PSA work for German HTR-projects the following suggestions can be derived:
The generalized design independent PSA approach requires from the analyst complex design specific adjustments (e.g. definition of risk metrics). Design specific PSA guidelines are needed to carry out PSAs with reasonable effort.
The life-cycle dependent requirements for the PSA ensure a pragmatic effort for sensitivity and uncertainty analysis. The assessment of the overall safety level must always provide a reliable result.
The PSA technical evaluation of various fission product barriers (containment, primary system, fuel cooling, ...) appears pragmatic, but at this point basic work is still required.


Summary
• For passive systems
– both active and passive system components must be modeled
– additional failure mechanisms with low probability must be considered
• For the modeling of non-light water reactors
– the concept of hazard states and the core damage states loses in some aspects its meaning and
– an equivalent concept must be used by analysts.
– New guidelines are currently under development (for example, by the ASME CNRM)

Uncertainty Analysis Methods for Estimation of Reliability of Passive System of VHTR

Seok-Jung HAN

Integrated Safety Assessment Division, Korea Atomic Energy Research Institute, 1045 Daedeokdaero, Yuseonggu, Daejeon, 305-353, Korea, hanseok@kaeri.re.kr

Abstract

An estimation of reliability of passive system for the probabilistic safety assessment (PSA) of a very high temperature reactor (VHTR) is under development in Korea. The essential approach of this estimation is to measure the uncertainty of the system performance under a specific accident condition. The uncertainty propagation approach according to the simulation of phenomenological models (computer codes) is adopted as a typical method to estimate the uncertainty for this purpose. This presentation introduced the uncertainty propagation and discussed the related issues focusing on the propagation object and its surrogates. To achieve a sufficient level of depth of uncertainty results, the applicability of the propagation should be carefully reviewed. For an example study, Latin-hypercube sampling (LHS) method as a direct propagation was tested for a specific accident sequence of VHTR. The presentation discussed the obtained insights (benefit and weakness) to apply an estimation of reliability of passive system.

Keywords: Reliability of passive systems, uncertainty analysis, uncertainty propagation, probabilistic safety assessment.

1. Introduction

The Reliability of Passive Systems (RoPS) is not only a safety issue to evaluate the safety performance of Very High Temperature Reactor (VHTR) but also a major issue to perform a VHTR's PSA (Chang, 2007). The typical methodologies of RoPS are related with the uncertainty evaluation of the system performance. In order to obtain a useful result of RoPS under the viewpoint of PSA, analyzers should carefully understand the features (strength and weakness) of the uncertainty evaluation approaches with an adequate level of depth and evaluate the uncertainty of the system performance.

The essential approach of this estimation is to measure the uncertainty of the system performance under a specific accident condition. The uncertainty propagation approach according to the simulation of phenomenological models (computer codes) is adopted as a typical method, not the experiences to estimate the uncertainty of the system performance. There are a few of well-known issues on the typical uncertainty propagation on simulation methods by using computer programs for the safety analysis. To achieve a sufficient level of depth of uncertainty results, the applicability of the propagation should be carefully reviewed.

This presentation introduced the uncertainty propagation and discussed the related issues focusing on the propagation object and its surrogates. For an example study, Latin-hypercube sampling (LHS) method as a direct propagation was tested for a specific accident sequence of VHTR. The presentation discussed the obtained insights (benefit and weakness) to apply an estimation of reliability of passive system.

2. Uncertainty evaluation approaches for PSA

The typical RoPS procedures consist of the following five essential parts (Fig. 1):

- Identification of the system
- Characterization of the system functional requirements
- Evaluation of the system performance
- Estimation of the system reliability
- Modeling of the system

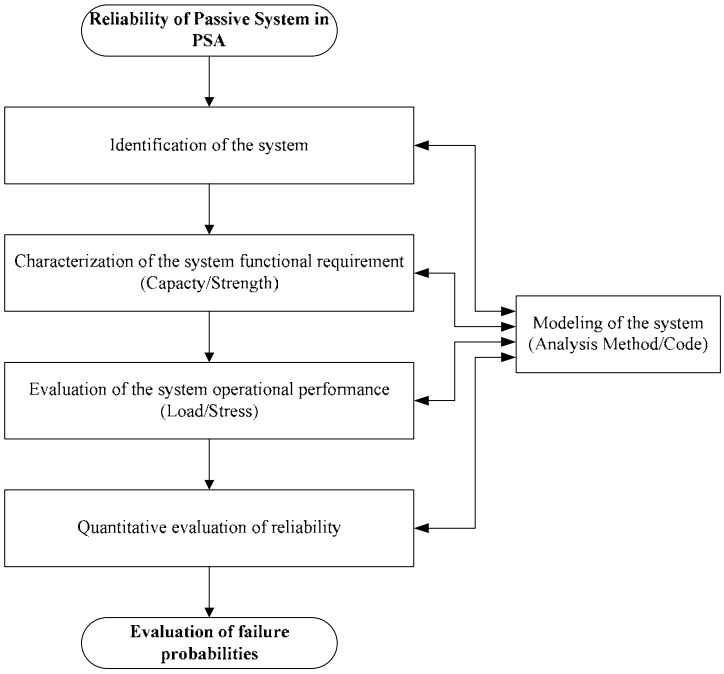


Fig. 1. A typical RoPS procedure for VHTR's PSA (Han, 2010)

A main concerning of this presentation is to evaluate the system operational performance, i.e., the uncertainty evaluation. Although there are many subsidiary issues on the uncertainty evaluation, the essential aspects are related with the uncertainty evaluation approaches, i.e., uncertainty propagation.

2.1 Uncertainty Propagation

The uncertainty propagation approaches are originated from the error propagation, as a well-known technique (Fig. 2). In the uncertainty propagation, the error sources in input variables are replaced into the uncertainty of input variables. The basic assumption on this approach is that the complete uncertainty as a representative result could be achieved by the experimental propagation according to the perturbation of the uncertainties of input variables.

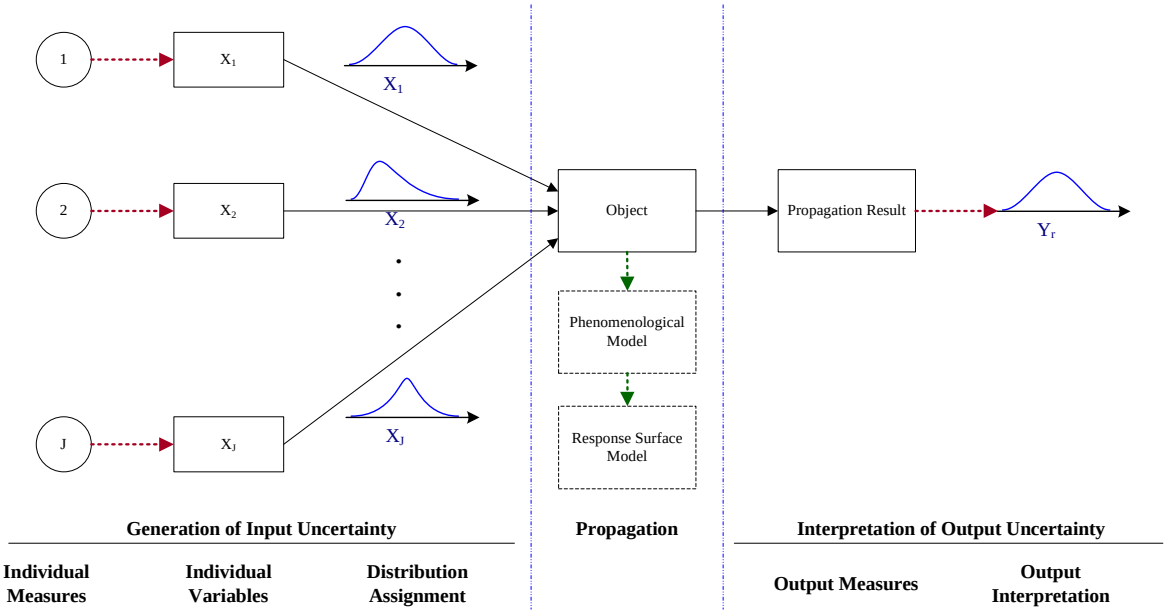


Fig. 2. A schematic diagram of the uncertainty propagation approach

The basic features of the uncertainty propagation approaches are divided into three parts:

- Generation of input uncertainties
- Propagation
- Interpretation of output uncertainty

Essential features and operation of the subsidiary processes of the uncertainty propagation are summarized as Table 1.

Table 2. Essential features of subsidiary processes of the uncertainty propagation approach

#	Process	Features	Operation
1	Individual measures	Individual identities of uncertainty	Measurement of uncertainty
2	Individual variables	Model parameters	Replace/substitute individual measures
3	Uncertainty assignment	Estimation of uncertainty distribution	Mapping of uncertainty of individual measures
4	Propagation	Propagation approaches	Sampling of individual variables and propagation on object
5	Output measurement	Output identities	Selection of representative output identities
6	Output interpretation	Interpretation of anticipated (desired) variables	Interpretation of uncertainty

2.2 Issues on Uncertainty Propagation

The usefulness of the uncertainty propagation approaches is essentially ranked on the degree of their acceptability from engaging stakeholders in safety decision making. In nuclear engineering as a narrow sense, the engagement of stakeholders could be simplified as the relationship between designers and regulators. If the stakeholders accept that the uncertainty could be quantified by the propagation approach as description in the basic assumption, the remaining issues on the propagation approaches may be considered as follows.

- Generation of input uncertainties
  - Substitution of individual measurable identities into individual variables on the object or surrogate's model
  - Measurement of uncertainty of individual identities and mapping of uncertainty on individual variables
- Propagation
  - Surrogates of object
    - Experimental object (system itself/experimental mockup)
    - Phenomenological model (simulation computer code)
    - Response surface model (RSM)
  - Propagation approaches (sampling methods of input variables) are classified by its strategy
    - Direct propagation
    - Indirect propagation
- Interpretation of output uncertainty
  - Selection of representative output variables on the object (or surrogate's model)
  - Compression of dynamic aspects on output variables to treat their probabilistic nature according to the required interpretation

As describing in Introduction, the issues on the generation of inputs uncertainties[6] and the interpretation of output uncertainty are out-of-scope. The main concern of this presentation only focuses on the issues of the propagation. Especially, the objects of propagation as RoPS are also substituted by the mathematical models or computer programs, not the objects themselves. There is some doubt that the results from the surrogate could be a representative results of the uncertainty of the considering object. This is about the creditability of the choose models that constructs the degree of belief for the uncertainty. The best solution of uncertainty propagation is to use the experimental object but it has a limitation of experiences to infer the uncertainty because of engineering practices.

[6] The first critical point of view is that the errors could be considered as the uncertainty. This is related with the confidence of the assigned uncertainties in input variables.

The well-known techniques of the uncertainty propagation by simulation are classified as direct and indirect propagation. The indirect methods adopt a surrogate model to replace the simulation results. The issue on the selection between direct and indirect propagation is related to the interpretation of output uncertainty. It is noted that the safety performance is generally interested in the success aspect, i.e., the reliability of the considering system, whereas PSA is interested in the failure aspect, reversely. The differences of each assessment may be enlarged to choose the applying techniques.

As a typical propagation method to obtain an uncertainty distribution for the failure aspect, direct methods require so many simulations to obtain an appropriate uncertainty result. This is due to that the expected probability of the RoPS in a considering system is too low to apply the direct methods. To perform a large number of simulations is an unrealistic situation in engineering practices. Indirect simulations as realistically available methods have a fundamental weakness, i.e., the incompleteness of model according to adopt a surrogate to replace the original object.

The awkwardness of indirect methods is the absence of evidences in the outer boundary of the estimated probabilistic distribution. Most of all, the deviation from experimental evidences according to using the simulation approaches maybe disturb the acquirement of the knowledge of uncertainty to do a realistic engineering decision. Because passive safety systems adopted in innovative reactors may be anticipated as extremely high reliable, the uncertainty evaluation by using indirect methods should be carefully choose and applied under the understanding of its weakness due to the incompleteness of model.

The issues of the surrogates as an indirect method are that they are able to replace the original object with a sufficient level of depth. For the applicability of surrogates, the analyzers should show how to well replace the object. The starting point to show the applicability is to understand the characteristics of the propagation surrogates.

2.3 Characteristics of Propagation Surrogates

Mainly considering characteristics of surrogates are as follows:

- Biasness in output
- Enhancement of uncertainty
- Reduction of uncertainty
- Non-linear aspects

Some comments on the aforementioned characteristics are summarised in Table 3.

Table 3. Characteristics of propagation surrogates

Characteristic	Issue		Remark
Biasness in output	Conservatism in the phenomenological safety analysis		Recommendation of using a best-estimated (unbiased) analysis
Enhancement of uncertainty	Steepness (Sensitivity)		Accumulation of residuals (uncertain variables vs. sensitivity variables)
	Instability of object	Divergence	Typically, instability is eliminated in modelling, but the instability in the object should be carefully assessed.
		Oscillation	
Reduction of uncertainty	Filtering effect against input perturbation		Usually mathematical models have a filtering effect. Water reserve system (real phenomena) Averaging techniques in modelling (mathematical formula)
Non-linear aspects	Change of material phase		Water/steam Melting structure
	Rapid chemical reactions		Hydrogen explosion Fire
	Change of system configurations		Water injection Valves operation (steam dump)
	Logical methods pertaining to phenomenological models		Selection of models or correlations to model phenomenology

It should be assessed that the considering surrogate has a managing capability against the aforementioned characteristics of propagation. For the biasness in output, it is believed that the bias in safety analysis is mainly due to conservative approaches in the phenomenological models, so it is recommended that a best-estimated analysis as an unbiased approach should be applied in safety analysis. For the enhancement of uncertainty, most engineering objects are designed to remove their instability although there is a little approach to the instability of object itself. The steepness in the behavior of the object could be controlled by an assessment of the sensitivity. It is noted that highly sensitive input variables are not always the uncertainty variables, so the sensitive variables should be carefully assessed for the potentialities of uncertainty variables. There are little effective approaches to the non-linear aspects on the object, but they should be carefully assessed because they would interrupt an effective way of the interpretation of the uncertainty output.

First of all, to emphasize in this presentation is the reduction of uncertainty. This effect is able to be explained as a filtering effect against input perturbation. The concern of this effect is that it is able to make an underestimation of the regarded uncertainty because this effect independently of the object itself is able to be imposed in the mathematical formula in the examples of Table 3. Usually mathematical models have some degree of filtering effect because the typical mathematical model considers its stability for the practicality. This effect is able to be enhanced in surrogates such as response surface models rather than phenomenological models. If a response surface model is considered as a propagation surrogate, it is necessary to assess the filtering effect on surrogate. However, this effect on surrogate is generally unknown to us. Especially, there is some doubt that the obtained result to failure aspects of propagation by a surrogate is meaningful, because the estimated failure probability distribution for a highly reliable system is able to be located in outer boundary of propagation results to generate a surrogate model. For this case, the evidences of the surrogate lack to show its applicability. As considering this effect, it is required the accumulation of case studies to obtain the applicability of the surrogate model.

To apply the uncertainty propagation approaches to an uncertainty evaluation, the aforementioned characteristics of the considering propagation surrogates should be carefully assessed. This presentation discussed the aforementioned issues by using an example study.

3. Example study

3.1 Application Example

A reactor cavity cooling system (RCCS) for a VHTR developed by KAERI was considered for an example study (Chang et al., 2007, Han, 2010). The conceptual diagram of RCCS is shown in Fig. 3. This is an air-cooled type passive system that has no active components for its operation. It is noted that this example provides a provisional results since the considered system is under a pre-conceptual design stage, but it provides sufficient insights to discuss the aforementioned propagation issues.

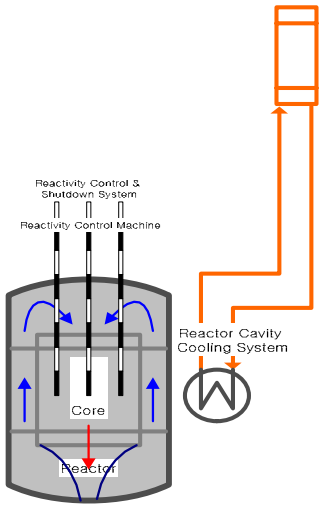


Fig. 3. A conceptual diagram of the RCCS of the Korean VHTR

The considered VHTR is a block type reactor core with 200MW thermal power and 450°C - 950°C core-inlet and outlet temperature. The basic features and design parameters of this reactor system are summarized in Table 4 (Han, 2010).

The considering accident sequence is a low pressure conduction cooling (LPCC) accident that is considered as a design basis accident for the safety design of VHTR. This sequence is due to a large failure of the pressure boundary of the reactor system such as a guillotine break of coolant pipe lines.

Table 4. Major design parameters of PMR200

Design parameters	Unit	Design values
Thermal power	MWth	200
Coolant inlet temperature	°C	490
Coolant outlet temperature	°C	950
Nominal coolant flow rate	kg/s	83.7
Number of fuel columns		66
Number of fuel blocks per column		6
Total number of fuel blocks		66 x 6 = 396
Active core height	m	4.758
Nominal linear heat generation rate	kW/m	3.122
Top/bottom reflector height	cm	135
Total core height	cm	745.8
UO_2 enrichment	w/o	15.5
Kernel diameter	cm	0.035
TRISO diameter	cm	0.077
RCCS inlet air temperature	°C	43

The GAMMA code, which is an integrated safety analysis code developed by KAERI for VHTRs, has been used for the evaluation of the system performance of the RCCS in the LPCC accident scenario (Lim and No, 2006 and Jun et al., 2009). The first process is to evaluate the nominal aspect on the system performance under the given accident condition. The normal analysis result of the LPCC by using the GAMMA code is shown in Fig. 4.

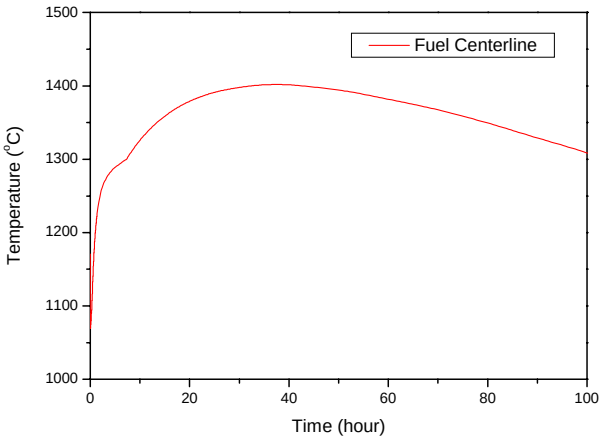


Fig. 4. A transient of maximum TRISO temperature during LPCC event at begin-of-cycle (BOC) for PMR 200MWth reactor design

The identification and screening of the input variables is a main process of uncertainty propagation, but the details of this estimation process is out-of-scope. This presentation described a brief summary of this process. Six parameters (i.e., graphite heat capacity, graphite conductivity, vessel emissivity, RCCS tube emissivity, core effective conductivity multiplier and decay heat ratio) were selected as the uncertainty related parameters as shown in Table 5 (Jun et al., 2009). After selecting uncertainty parameters, the range and distribution type of each selected parameter should be estimated.

Table 5. The selected uncertainty parameters and their ranges

Uncertainty parameter	Unit	Nominal value*	Range**	Standard Deviation***	Distribution type	Remark
Graphite heat capacity	kJ/kg·K·m^3	1.0	0.95 ~ 1.05	0.025511	Normal	Function of temperature & pressure
Graphite conductivity	W/(m·K)	1.0	0.8 ~ 1.2	0.102043	Normal	Function of temperature
Vessel emissivity		0.8	0.72 ~ 0.88	0.040817	Normal	
RCCS tube emissivity		0.8	0.72 ~ 0.88	0.040817	Normal	
Core effective conductivity multiplier		1.0	0.9 ~ 1.1	0.051021	Normal	
Decay heat ratio	%/full power	1.0	0.95 ~ 1.05	0.025511	Normal	Function of normal reactor power

* The nominal value is a representative value of the GAMMA code lookup table.
** The range assigned 95% confidence boundary of a normal distribution.
*** The standard deviation can be estimated by $\sigma_X = | X_R - \mu_X | / Z_{0.95}$ where $Z_{0.95} = 1.95996$, X_R is a range value and μ_X is a nominal value in this table.

It is noted that considering the parameters are related with the phenomena and modelling rather than the parameters related to the uncertainty of design, construction and operation. The reasons for this are that a primary concern of the safety analysis is the validation and verification of the analysis method.

3.2 Uncertainty Propagation

The MOSAIQUE software is used in the uncertainty propagation by using the GAMMA code, which has been developed by KAERI to simulate the uncertainty propagation for large-scale computer simulation codes, such as a RELAP code (Lim and Han, 2009). The Latin-hypercube sampling (LHS) method using the code simulation with 80 runs was adopted for a direct estimation of the uncertainty

distribution (Helton and Davis, 2003). The simulation results by using the GAMMA code for the LPCC accident scenario are shown in Fig. 5.

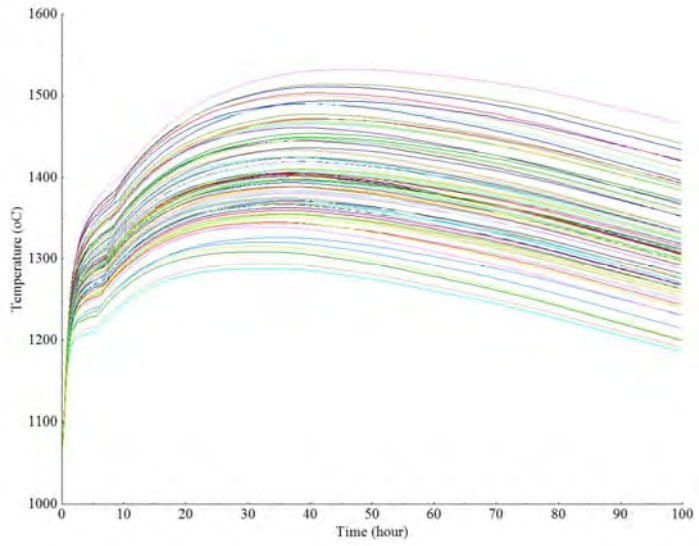


Fig. 5. Propagation results of the GAMMA code by LHS for the LPCC accident scenario

3.3 Applicability of Uncertainty Propagation

For this example, it seems that the propagation surrogate has a sufficient applicability to generate uncertainty distribution if the input uncertainties would be adequate to represent the uncertainty of input variables.

According to the characteristics of the propagation surrogate, the propagation results in the example can be assessed to show its applicability. The propagation results showed that non-linear aspect to affect a critical perturbation on the output uncertainty did not appear in the example propagation. Main causes of the non-linear effect on system are usually due to the change of system configurations. The non-linearity does not appear because RCCS in VHTR does not adopt active components such as valves or pumps. For the filtering effect, it seems that the filtering effect is related with the phenomenological model (GAMMA code) not a surrogate model itself because this results obtained by a direct method, so there is a little difficult to apply the propagation results as a representative uncertainty. In the current state, it is regarded that the biasness is not involved in the example. To assess the biasness of the example requires a sufficient progress of the development of VHTR, so this is out-of-scope of the current presentation. As the brief assessment, this propagation results has a sufficient applicability of uncertainty estimation under the representative input uncertainties.

For this example, the uncertainty distribution was estimated by the statistical inference, of which the normal distribution of same mean and standard deviation $\Pr(S) = N(1405.55, 53.98)$ was applied in the propagation results (Fig. 6).

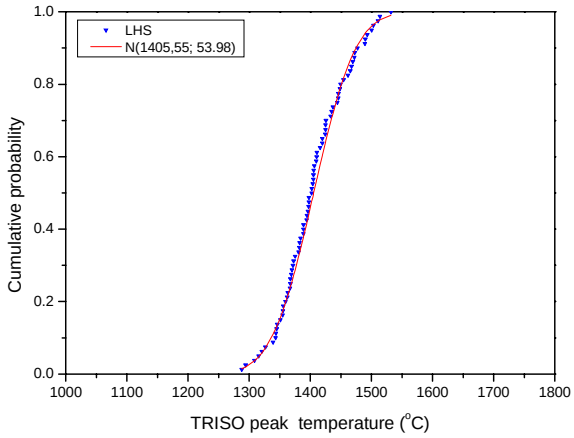


Fig. 6. Cumulative distributions of TRISO peak temperature for the LPCC accident scenario

4. Concluding remarks

This presentation introduced the uncertainty propagation and discussed the related issues focusing on the propagation object and its surrogates. To achieve a sufficient level of depth of uncertainty results, the applicability of the propagation should be carefully reviewed. For an example study, Latin-hypercube sampling (LHS) method as a direct propagation was tested for a specific accident sequence of VHTR. The obtained insights (benefit and weakness) will be applied in an estimation of reliability of passive system for VHTR's PSA.

References

Chang, J. et al, (2007). A study of a nuclear hydrogen production demonstration plant, Nuclear Engineering and Technology, Vol. 39, No. 2, pp.111-122.

Han, S. and Yang, J., (2010). A quantitative evaluation of reliability of passive systems within probabilistic safety assessment framework for VHTR, Annals of Nuclear Energy, Vol. 37 (3), pp. 345-358.

Lim, H., Han, S.H., (2009). Development of T/H uncertainty analysis S/W MOSAIQUE. Korea-Japan Joint Workshop on PSA, KJPSA10, Jeju, Korea.

Lim, H.S., No, H.C., (2006). GAMMA multidimensional multicomponent mixture analysis to predict air ingress phenomena in an HTGR. Nucl. Sci. Eng. 152, 1-11.

Jun, J.S., et al, (2009). Thermal-fluid analysis of the PMR 200MWth reactor system at the steady state and transient conditions. Transactions of the Korean Nuclear Society, Spring Meeting, Jeju, Korea, May 22.

Helton, J.C., Davis, F.J., (2003). Latin hypercube sampling and the propagation of uncertainty in analyses of complex systems. Reliability Engineering and System Safety, 81, 23-69.

OECD/NEA Workshop on PSA for New and Advanced Reactors
June 20-24, 2011
OECD Conference Centre, Paris, France

Uncertainty Analysis Methods for Estimation of Reliability of Passive System of VHTR

June 22, 2011

Seok-Jung HAN

Contents

Korea Atomic Energy Research Institute

1. Introduction

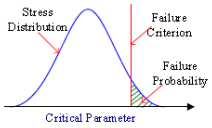
2

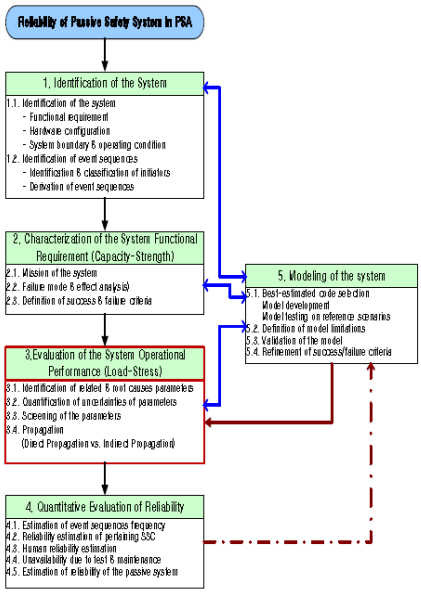
- An estimation of the RoPS (Reliability of Passive Systems) is an essential issue of PSA for a VHTRs (Very High Temperature Reactors).
  - Key issue is **to measure the uncertainty** of system performance.
- Prerequisite
  - To understand **strength and weakness** of the uncertainty evaluation
- **Uncertainty propagation** : Typical uncertainty evaluation
  - Simulation of phenomenological models (computer codes)
  - Not experiences
- **Applicability of propagation surrogate**
  - To achieve a sufficient level of depth of uncertainty results.
- Objectives:
  - To **introduce key aspects** of uncertainty propagation
  - To **discuss** issues focusing on the propagation object and its surrogates.

Typical RoPS Procedure

3

- Objective: Estimation of functional failure probability
- Essential Parts
  1. Identification of the system
  2. Characterization of the system functional requirements
  3. **Evaluation of the system operational performance**
     - Uncertainty Propagation
  4. Estimation of the reliability of the system
  5. Modeling of the system





2. Uncertainty Evaluation Approaches

4

- Types of uncertainty
  - Completeness
  - Modeling uncertainty
  - Parametric uncertainty
- Uncertainty Analysis → Parametric uncertainty
  - Error propagation → Uncertainty propagation

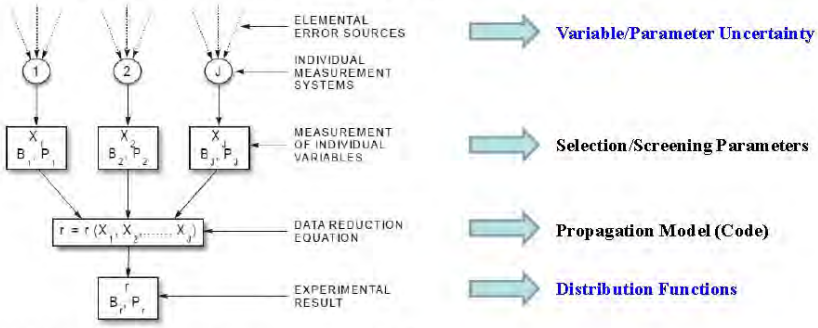
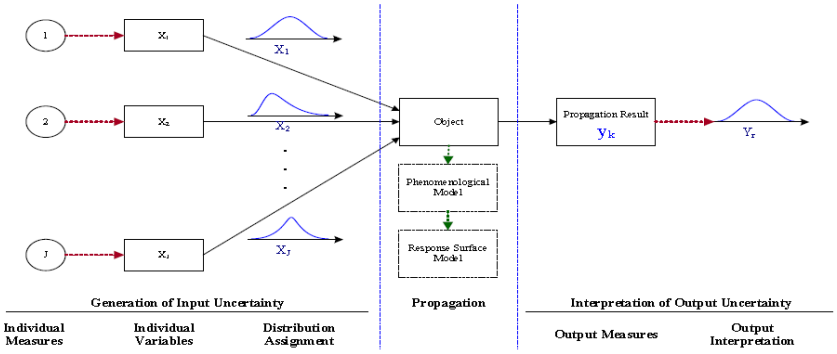


Figure 3. Propagation of errors into experimental results (AIAA, 1995)

Uncertainty Propagation

5

- The basic assumption :
  - The complete uncertainty as a representative result could be achieved by the experimental propagation according to the perturbation of the uncertainties of input variables.
- Features
  - Generation of inputs uncertainties
  - Propagation
  - Interpretation of outputs uncertainty



Note: Essential Features of Uncertainty Propagation

6

#	Process	Features	Operation
1	Individual measures	Individual identities of uncertainty	Measurement of uncertainty
2	Individual variables	Model parameters	Replace/substitute individual measures
3	Uncertainty assignment	Estimation of uncertainty distribution	Mapping of uncertainty of individual measures
4	Propagation	Propagation approaches	Sampling of individual variables and propagation on object
5	Output measurement	Output identities	Selection of representative output identities
6	Output interpretation	Interpretation of anticipated (desired) variables	Interpretation of uncertainty

Issues on Uncertainty Propagation

7

- Generation of Inputs Uncertainties
  - Mapping of individual measurable identities into individual variables on a model of the object
  - Measurement of uncertainty of individual identities and mapping of uncertainty on individual variables
- **Propagation**
  - Surrogates of object
    - Experimental object (System itself/Experimental mockup)
    - Phenomenological model (Simulation computer code)
    - Response surface model
  - Propagation approaches (sampling methods of input variables) are classified by its strategy
    - Direct propagation
    - Indirect propagation
- Interpretation of output uncertainty
  - Selection of representative output variables
  - Compression of dynamic aspects on output variables to treat their probabilistic nature due to the required interpretation

Issues of Propagation (1/2)

8

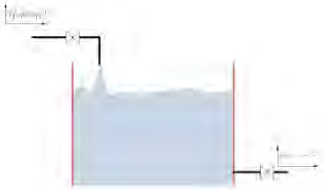
- Creditability of Propagation Object (Degree of belief for Uncertainty)
  - Experimental object
    - Limitation of experiences to infer the uncertainty
  - Surrogates
    - How to well replace the object
- Well-known techniques of the uncertainty propagation by simulation:
  - Direct propagation
  - Indirect propagation
- The issue on the selection between direct and indirect propagation:
  - Success aspect: Safety performance
  - Failure aspect: PSA
- For failure aspect
  - Direct methods require so many simulations
    - unrealistic situation in engineering practices.
  - Indirect simulations as realistically available methods
    - incompleteness of model

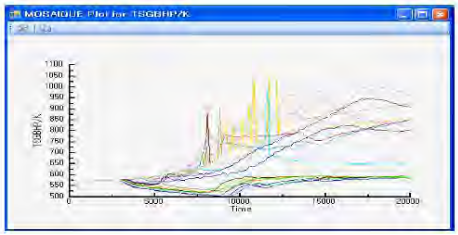
Issues of Propagation (2/2)

- Awkwardness of indirect methods is due to the absence of evidences in the outer boundary
  - Ex: passive safety systems (extremely high reliable)
- Understanding of its weakness due to incompleteness of model
  - Analyzer should show the applicability of surrogates
- The starting point to show the applicability is to understand the characteristics of the propagation surrogates.

Characteristics of Propagation Surrogates

Characteristic	Issue		Remark
Biasness in output	Conservatism in the phenomenological safety analysis		Recommendation of using a best-estimated (unbiased) analysis
Enhancement of uncertainty	Steepness (Sensitivity)		Accumulation of residuals (uncertain variables vs. sensitivity variables)
	Instability of object	Divergence	Typically, instability is eliminated in modelling, but the instability in the object should be carefully assessed.
		Oscillation	
Reduction of uncertainty	Filtering effect against input perturbation		Usually mathematical models have a filtering effect. Water reserve system (real phenomena) Averaging techniques in modelling (mathematical formula)
Non-linear aspects	Change of material phase		Water/steam Melting structure
	Rapid chemical reactions		Hydrogen explosion Fire
	Change of system configurations		Water injection Valves operation (steam dump)
	Logical methods pertaining to phenomenological models		Selection of models or correlations to model phenomenology





Reduction of Uncertainty

11

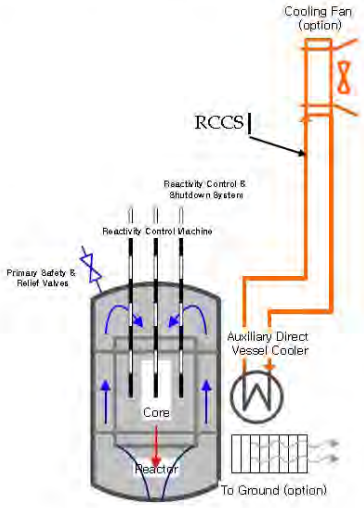
- An underestimation of the regarded uncertainty
  - This effect independently of the object itself is able to be imposed in the mathematical formula.
- Usually mathematical models have some degree of filtering effect
  - The typical mathematical model considers its stability for the practicality.
  - This effect is able to be enhanced in surrogates such as response surface models rather than phenomenological models.
- If a response surface model is considered as a propagation surrogate, it is necessary to assess the filtering effect on surrogate.
  - This effect on surrogate is generally unknown to us.
- There is some doubt that the obtained result to failure aspects of propagation by a surrogate is meaningful
  - Estimated failure probability for a highly reliable system is able to be located in outer boundary of propagation results to generate a surrogate model.

3. Example Study

12

- Reactor Cavity Cooling System (RCCS): Passive Cooling System
  - Air cooled type system
  - No active components (Valves)
  - Normally operated

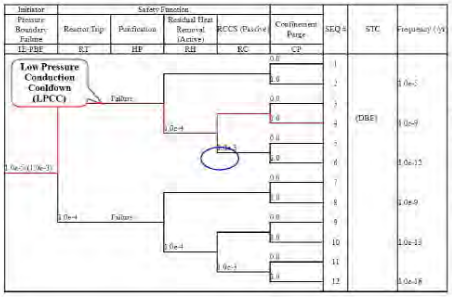
Design parameters	Unit	Design values
Thermal power	MWth	200
Coolant inlet temperature	°C	490
Coolant outlet temperature	°C	950
Nominal coolant flow rate	kg/s	83.7
Number of fuel columns		66
Number of fuel blocks per column		6
Total number of fuel blocks		66 x 6 = 396
Active core height	m	4.758
Nominal linear heat generation rate	kW/m	3.122
Top/bottom reflector height	cm	135
Total core height	cm	745.8
UO_2 enrichment	w/o	15.5
Kernel diameter	cm	0.035
TRISO diameter	cm	0.077
RCCS inlet air temperature	°C	43

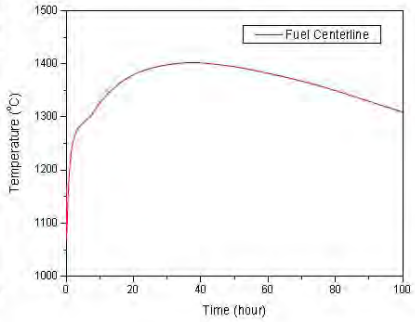


Example Case

13

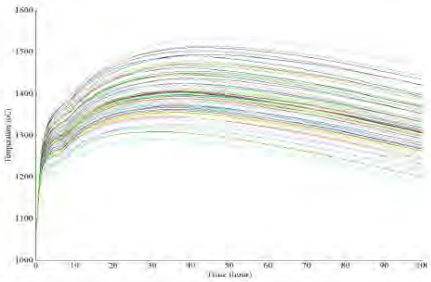
- Scenario: Low Pressure Conductive Cooldown (LPCC) Accident
  - Large failure of pressure boundary
  - No cooling by coolant loop
  - Direct cooling by vessel conductivity & radiation heat transfer
- Estimation Parameter:
  - Peak TRISO fuel temperature
    ps. TRISO design criterion (1,600°C)
- GAMMA code
  - Integrated safety analysis code for VHTRs developed by KAERI





Uncertainty Propagation

- Uncertainty Inputs: 6 Parameters
- Propagation: Latin Hypercube Sampling (LHS)
  - 80 samples
  - Centerline fuel temperature



Uncertainty parameter	Unit	Nominal value	Range	Standard Deviation	Distribution type
Graphite heat capacity	kJ/kg·K·m^3	1.0	0.95 ~ 1.05	0.025511	Normal
Graphite conductivity	W/(m·K)	1.0	0.8 ~ 1.2	0.102043	Normal
Vessel emissivity		0.8	0.72 ~ 0.88	0.040817	Normal
RCCS tube emissivity		0.8	0.72 ~ 0.88	0.040817	Normal
Core effective conductivity multiplier		1.0	0.9 ~ 1.1	0.051021	Normal
Decay heat ratio	%/full power	1.0	0.95 ~ 1.05	0.025511	Normal

14

Applicability of Uncertainty Propagation

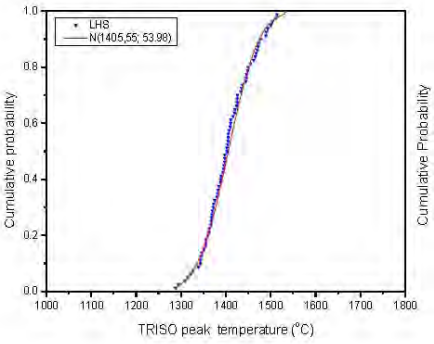
15

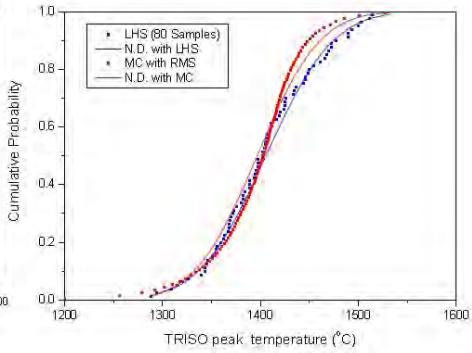
- According to the characteristics of the propagation surrogate, the propagation results can be assessed to show its applicability.
  - The non-linearity does not appear because RCCS in VHTR does not adopt active components such as valves or pumps.
  - The filtering effect is related with the phenomenological model (GAMMA code) not a surrogate model itself
    - direct method
  - Biasness is not involved
    - To assess the biasness of the example requires a sufficient progress of the development of VHTR
  - There is a little difficult to apply the propagation results as a representative uncertainty
- As the brief assessment, this propagation results has a sufficient applicability of the uncertainty estimation under the representative input uncertainties.

Note: Reduction of Uncertainty

16

	Direct Propagation of LHS	Normal Distribution with LHS results	Crude Monte Carlo by RMS (10,000)	Normal Distribution with LHS results
Mean	1405.55	1405.55	1396.64	1396.64
Std	53.98	53.98	50.33	50.33
1600	0.000.E+00	1.577.E-04	3.000.E-04	2.670.E-05
1700	0.000.E+00	2.450.E-08	0.000.E+00	8.354.E-10
1800	0.000.E+00	1.361.E-13	0.000.E+00	0.000.E+00



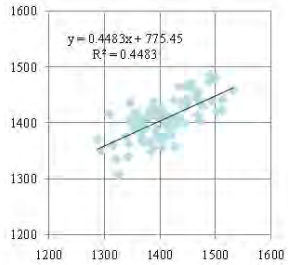


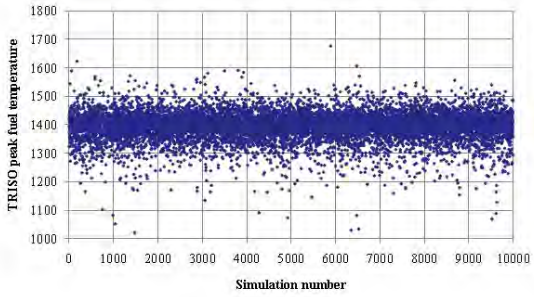
Note : RMS

17

- 2nd order polynomial with 80 LHS results

$$Y = f(\mathbf{x}) \approx A + \sum_{i=1}^{6} B_i X_i + \sum_{i=1}^{6}\sum_{j=1}^{6} C_i X_i X_j$$





4. Concluding Remark

18

- This presentation introduced the uncertainty propagation and discussed the related issues focusing on the propagation object and its surrogates.
  - Four characteristics involved in surrogate model
  - Reduction of uncertainty (Filtering effect)
- The applicability of the propagation should be carefully assessed.
- The obtained insights will be applied in an estimation of reliability of passive system for VHTR's PSA.

Thank you for your attention!

Problems Facing the Use of Passive Safety Systems

Luciano Burgazzi

ENEA, Italian National Agency for New Technologies, Energy and Sustainable Economic Development, Technical Unit for Reactor Safety and Fuel Cycle Methods
Via Martiri di Monte Sole, 4, 40129 Bologna, Italy - luciano.burgazzi@enea.it

Abstract

- *This study will analyze the current state of the art in the reliability of passive systems for extensive use in future nuclear power plants. This case study uncovers the insights on the technological issues associated with the reliability of the systems based on thermal – hydraulics, for which, methods are still in developing phase.*

Keywords: Passive Systems, Natural Circulation, Reliability

1. Introduction

Within the framework of the development of advanced nuclear technologies, the reliability of passive systems has become an important subject and area under discussion, for their extensive use in future nuclear power plants, (NEA, 2002).
Following the IAEA definitions, (IAEA, 1991), a passive component does not need any external input or energy to operate and it relies only upon natural physical laws (e.g. gravity, natural convection, conduction, etc.) and/or on inherent characteristics (properties of materials, internally stored energy, etc.) and/or 'intelligent' use of the energy that is inherently available in the system (e.g. decay heat, chemical reactions etc.).
The term "passive" identifies a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation.
Inclusion of failure modes and reliability estimates of passive components for all systems is recommended in probabilistic safety assessment (PSA) studies. This has aroused the need for the development and demonstration of consistent methodologies and approaches for their reliability evaluation and eventually for their integration in the accident sequences, within the community of the nuclear safety research. Special emphasis has been placed on the reliability of the systems based on thermal-hydraulics (i.e. resting on natural circulation), for which there isn't yet an agreed approach and for which different methods have been conceived and implemented, as illustrated by Burgazzi (2007a).
However, the efforts conducted so far to deal with the passive safety systems reliability, have raised an amount of open issues to be addressed in a consistent way, in order to endorse the proposed approaches and to add credit to the underlying models and the eventual reliability figures, resulting from their application. In fact the applications of the proposed methodologies are to a large extent dependent upon the assumptions underlying the methods themselves.
At the international level, for instance, IAEA recently coordinated a research project, denoted as "*Natural Circulation Phenomena, Modelling and Reliability of Passive Systems"* (2004-2008), (IAEA, 2005; IAEA, 2009), while another coordinated research project on "*Development of Methodologies for the Assessment of Passive Safety System Performance in Advanced Reactors"* (2008-2012) is currently underway: while focus of the first project has been the natural circulation and related phenomena, the objective of the latter program is to determine a common analysis-and-test method for reliability assessment of passive safety system performance.
This paper provides the insights resulting from the analysis on the technical issues associated with assessing the reliability of passive systems in the context of nuclear safety and probabilistic safety analysis, and a viable path towards the implementation of the research efforts in the related areas is delineated as well. Focus on these issues is very important since it is the major goal of the

international research activities (e.g. IAEA) to strive to reach a common consensus about the different proposed approaches. The paper is organized as follows: at first the current available methodologies are illustrated and compared, the open issues coming out from their analysis are identified and for which one of them the state of the art and the outlook is presented; the relative importance of each of them within the evaluation process is presented as well.
It must be underlined that this article is to be considered as an "update" on the current and emerging/necessary activities and issues associated with the reliability assessment of passive safety systems, to be implemented in the design of the innovative reactors. In the light of this, the objective is to provide a sort of "state of the art" related to the topic, attempting to define and consolidate the issues associated with current-day development of commercial nuclear power plants.

2. Methodologies description and comparison

A very good description of the various methodologies proposed so far and currently available in the open literature is provided by Zio and Pedroni (2009).
The earliest significant effort to quantify the reliability of such systems is represented by a methodology known as REPAS (Reliability Evaluation of Passive Systems), (Jafari and D'Auria, 2003), which has been developed in late 1990s, cooperatively by ENEA, the University of Pisa, the Polytechnic of Milan and the University of Rome, that was later incorporated in the EU (European Union) RMPS (Reliability Methods for Passive Systems) project. This methodology is based on the evaluation of a failure probability of a system to carry out the desired function from the epistemic uncertainties of those physical and geometric parameters which can cause a failure of the system.
The RMPS methodology, described by Marques et al. (2005), was developed to address the following problems: 1) Identification and quantification of the sources of uncertainties and determination of the important variables, 2) Propagation of the uncertainties through thermal-hydraulic (T-H) models and assessment of passive system unreliability and 3) Introduction of passive system unreliability in accident sequence analyses. In this approach, the passive system is modeled by a qualified T-H code (e.g. CATHARE, RELAP) and the reliability evaluation is based on results of code runs, whose inputs are sampled by Monte-Carlo (M-C) simulation. This approach provides realistic assessment of the passive system reliability, thanks to the flexibility of the M-C simulation, which adapts to T-H model complexity without resort to simplifying approximation. In order to limit the number of T-H code runs required by M-C simulation, alternative methods have been proposed such as variance reduction techniques, first and second order reliability methods and response surface methods. The RMPS methodology has been successfully applied to passive systems utilizing natural circulation in different types of reactors (BWR, PWR, and VVER). A complete example of application concerning the passive residual heat removal system of a CAREM reactor is presented in Lorenzo et al. (2011). The RMPS methodology tackles also an important problem, which is the integration of passive system reliability in a PSA study. So far, in existing innovative nuclear reactor projects PSA's, only passive system components failure probabilities are taken into account, disregarding the physical phenomena on which the system is based, such as the natural circulation. The first attempts performed within the framework of RMPS have taken into account the failures of the components of the passive system as well as the impairment of the physical process involved like basic events in static event tree as exposed by Marques (2005). Two other steps have been identified after the development of the RMPS methodology where an improvement was desirable: the inclusion of a formal expert judgment (EJ) protocol to estimate distributions for parameters whose values are either sparse on not available, and the use of efficient sensitivity analysis techniques to estimate the impact of changes in the input parameter distributions on the reliability estimates.
R&D in the United States on the reliability of passive safety systems has not been as active at least until mid 2000. A few published papers from the Massachusetts Institute of Technology (MIT) have demonstrated their development of approaches to the issue. Their technique has examined T-H uncertainties in passive cooling systems for Generation IV-type gas-cooled reactors. The MIT research on the reliability of passive safety systems has taken a similar approach but has focused on a different set of reactor technologies. Their research has examined thermal hydraulic uncertainties in passive cooling systems for Generation IV gas-cooled reactors, as described by Apostolakis (2005, 2008). Instead of post-design probabilistic risk analysis for regulatory purposes, the MIT research seeks to

leverage the capabilities of probabilistic risk assessment (PRA) to improve the design of the reactor systems early in their development life cycle.
In addition to the RMPS approach, a number of alternative methodologies have been investigated for the reliability assessment of T-H passive systems.
Three different methodologies have been proposed by ENEA. In the first methodology (Burgazzi, 2007b), the failure probability is evaluated as the probability of occurrence of different independent failure modes, a priori identified as leading to the violation of the boundary conditions or physical mechanisms needed for successful passive system operation. This approach based on independent failure modes introduces a high level of conservatism as it appears that the probability of failure of the system is relevantly high, because of the combination of various modes of failure as in a series system, where a single fault is sufficient to challenge the system performance. The correspondent value of probability of failure can be conservatively assumed as the upper bound for the unavailability of the system, within a sort of "parts-count" reliability estimation. In the second, (Burgazzi, 2002), modeling of the passive system is simplified by linking to the modeling of the unreliability of the hardware components of the system: this is achieved by identifying the hardware failures that degrade the natural mechanisms upon which the passive system relies and associating the unreliability of the components designed to assure the best conditions for passive function performance. Thus, the probabilities of degraded physical mechanisms are reduced to unreliability figures of the components whose failures challenge the successful passive system operation. If, on the one hand, this approach may in theory represent a viable way to address the matter, on the other hand, some critical issues arise with respect to the effectiveness and completeness of the performance assessment over the entire range of possible failure modes that the system may potentially undergo and their association to corresponding hardware failures. In this simplified methodology, degradation of the natural circulation process is always related to failures of active and passive components, not acknowledging, for instance, any possibility of failure just because of unfavorable initial or boundary conditions. In addition, the fault tree model adopted to represent the physical process decomposition is used as a surrogate model to replace the complex T-H code that models the system behavior. This decomposition is not appropriate to foresee interactions among physical phenomena and makes it extremely difficult to realistically assess the impact of parametric uncertainty on the performance of the system. The third approach is based on the concept of functional failure, within the reliability physics framework of load-capacity exceedance (Burgazzi, 2003, 2007c, Apostolakis 2005). The functional reliability concept is defined as the probability of the passive system failing to achieve its safety function as specified in terms of a given safety variable crossing a fixed safety threshold, leading the load imposed on the system to overcome its capacity. In this framework, probability distributions are assigned to both safety functional requirement on a safety physical parameter (for example, a minimum threshold value of water mass flow required to be circulating through the system for its successful performance) and system state (i.e., the actual value of water mass flow circulating), to reflect the uncertainties in both the safety thresholds for failure and the actual conditions of the system state. Thus the mission of the passive system defines which parameter values are considered a failure by comparing the corresponding pdfs according to defined safety criteria. The main drawback in the last method devised by ENEA lies in the selection and definition of the probability distributions that describe the characteristic parameters, based mainly on subjective/engineering judgment.
Every one of three methods devised by ENEA shares with the main RMPS approach the issue related to the uncertainties affecting the system performance assessment process. With respect to the RMPS a greater simplicity is introduced, although detrimental to the relevance of the approaches themselves: this is particularly relevant as far as the approach based on hardware components failure is concerned.
Finally a different approach is followed in the APSRA (Assessment of Passive System ReliAbility) methodology developed by BARC (Bhabha Atomic Research Centre, India), see Nayak et al. (2008). In this approach, a failure surface is generated by considering the deviation of all those critical parameters, which influence the system performance. Then, the causes of deviation of these parameters are found through root diagnosis. It is attributed that the deviation of such physical parameters occurs only due to a failure of mechanical components such as valves, control systems, etc. Then, the probability of failure of a system is evaluated from the failure probability of these mechanical components through classical PSA treatment. Moreover, to reduce the uncertainty in code

predictions, BARC foresee to use in-house experimental data from integral facilities as well as separate.
With reference to the two most relevant methodologies (i.e. RMPS and APSRA), the RMPS consists mainly in the identification and quantification of parameter uncertainties in the form of probability distributions, to be propagated directly into a T-H code or indirectly in using a response surface; the APSRA methodology strives to assess not the uncertainty of parameters but the causes of deviation from nominal conditions, which can be in the failure of active or passive components or systems.
As a result, different approaches are used in the RMPS and APSRA methodologies. RMPS proposes to take into account, in the PSA model, the failure of a physical process. This problem is treated in using a best estimate T-H code plus uncertainty approach. APSRA includes in the PSA model the failure of those components which cause a deviation of the key parameters resulting in a system failure, but does not take into account possible uncertainties on these key parameters. As the consequence, the T-H code is used in RMPS to propagate the uncertainties and in APSRA to build a failure surface. APSRA incorporates an important effort on qualification of the model and use of the available experimental data. These aspects have not been studied in the RMPS, given the context of the RMPS project.
The following table attempts to identify the main characteristics of the methodologies proposed so far, with respect to some aspects, such as the development of deterministic and probabilistic approaches, the use of deterministic models to evaluate the system performance, the identification of the sources of uncertainties and the application of expert judgment.

Methodology	Probabilistic vs. deterministic	Deterministic Analysis	Uncertainties	Expert Judgment/Experimental data
REPAS/RMPS	Merge of probabilistic and thermal hydraulic aspects	T-H code adopted for uncertainty propagation	Uncertainties in parameters modeled by probability density functions	EJ adopted to a large extent; Statistical analysis when experimental data exist
APSRA	Merge of probabilistic and thermal hydraulic aspects	T-H code adopted to build the failure surface	parameters' deviations from nominal conditions caused by failure of active or passive components (root diagnosis)	Experimental data usage; EJ for root diagnosis
ENEA methods	Only probabilistic aspects		Uncertainties in parameters	EJ adopted to a large extent (except the approach based on hardware failure)

Table 1. Main features of the various approaches

3. Open issues

From the exam of the various methodologies, which have been developed over these most recent years within the community of the safety research, and are currently available in the open literature, the following open questions are highlighted and consequently needs for research in all related areas are pointed out :

- The aspects relative to the assessment of the uncertainties related to passive system performance: they regard both the best estimate T-H codes used for their evaluation and system reliability assessment itself;

- The dependencies among the parameters, mostly T-H parameters, playing a key role in the whole process assessment.

- The integration of the passive systems within an accident sequence in combination with active systems and human actions.

- The consideration for the physical process and involved physical quantities dependence upon time, implying, for instance, the development of dynamic event tree to incorporate the interactions between the physical parameter evolution and the state of the system and/or the transition of the

system from one state to another. It's worth noticing that these two last aspects are correlated, but hey will be treated separately.

- The comparison between active and passive systems, mainly on a functional viewpoint.

All of these points are elaborated in the following, in an attempt to cover the entire spectrum of issues related to the topic, and capture all the relevant aspects to concentrate on and devote resources towards for fulfilling a significant advance.

4. Uncertainties

The quantity of uncertainties affecting the operation of the T-H passive systems affects considerably the relative process devoted to reliability evaluation, within a probabilistic safety analysis framework, as recognized in Apostolakis et al.. (2005).
These uncertainties stem mainly from the deviations of the natural forces or physical principles, upon which they rely (e.g., gravity and density difference), from the expected conditions due to the inception of T-H factors impairing the system performance or to changes of the initial and boundary conditions, so that the passive system may fail to meet the required function. Indeed a lot of uncertainties arise, when addressing these phenomena, most of them being almost unknown due mainly to the scarcity of operational and experimental data and, consequently, difficulties arise in performing meaningful reliability analysis and deriving credible reliability figures. This is usually designated as phenomenological uncertainty, which becomes particularly relevant when innovative or untested technologies are applied, eventually contributing significantly to the overall uncertainty related to the reliability assessment.
Actually there are two facets to this uncertainty, i.e., "aleatory" and "epistemic" that, because of their natures, must be treated differently. The aleatory uncertainty is that addressed when the phenomena or events being modeled are characterized as occurring in a "random" or "stochastic" manner and probabilistic models are adopted to describe their occurrences. The epistemic uncertainty is that associated with the analyst's confidence in the prediction of the PSA model itself, and it reflects the analyst's assessment of how well the PSA model represents the actual system to be modeled. This has also been referred to as state-of-knowledge uncertainty, which is suitable to reduction as opposed to the aleatory which is, by its nature, irreducible. The uncertainties concerned with the reliability of passive system are both stochastic, because of the randomness of phenomena occurrence, and of epistemic nature, i.e. related to the state of knowledge about the phenomena, because of the lack of significant operational and experimental data. For instance, as initial step, the approach described by Burgazzi (2004) allows identifying the uncertainties pertaining to passive system operation in terms of critical parameters driving the modes of failure, as, for instance, the presence of non-condensable gas, thermal stratification and so on. In this context the critical parameters are recognized as epistemic uncertainties. The same reference points out, as well, the difference between the uncertainties related to passive system reliability and the uncertainties related to the T-H codes (e.g. RELAP), utilized to evaluate the performance itself, as the ones related to the coefficients, correlations, nodalization, etc.: these specific uncertainties, of epistemic nature, in turn affect the overall uncertainty in T-H passive system performance and impinge on the final sought reliability figure.
A further step of the matter can be found in Burgazzi (2007b), which attempts to assign sound distributions to the critical parameters, to further develop a probabilistic model. As is of common use when the availability of data is limited, subjective probability distributions are elicited from expert/engineering judgment procedure, to characterize the critical parameters.
Three following classes of uncertainties to be addressed are identified:

- Geometrical properties: this category of uncertainty is generally concerned with the variations between the as-built system layout and the design utilized in the analysis: this is very relevant for the piping layout (e.g. suction pipe inclination at the inlet of the heat exchanger, in the isolation condenser reference configuration) and heat loss modes of failure.

- Material properties: material properties are very important in estimating the failure modes concerning for instance the undetected leakages and the heat loss.

- Design parameters, corresponding to the initial/boundary conditions (for instance, the actual values taken by design parameters, like the pressure in the reactor pressure vessel).

- Phenomenological analysis: the natural circulation failure assessment is very sensitive to uncertainties in parameters and models used in the thermal hydraulic analysis of the system. Some of the sources of uncertainties include but are not limited to: the definition of failure of the system used in the analysis, the simplified model used in the analysis, the analysis method and the analysis focus on failure locations and modes and finally the selection of the parameters affecting the system performance.

The first, second and third groups are part of the category of aleatory uncertainties because they represent the stochastic variability of the analysis inputs and they are not reducible. The fourth category is referred to the epistemic uncertainties, due to the lack of knowledge about the observed phenomenon and thus suitable for reduction by gathering a relevant amount of information and data. This class of uncertainties must be subjectively evaluated, since no complete investigation of these uncertainties is available.
A clear prospect of the uncertainties as shown in Table 2 (Zio and Pedroni, 2009).

Aleatory	Epistemic
Geometrical properties	T-H analysis
Material properties	Model (correlations)
Initial/boundary conditions (design parameters)	Parameters
	System failure analysis
	Failure criteria
	Failure modes (critical parameters)

Table 2. Categories of uncertainties associated with T-H passive systems reliability assessment (Zio and Pedroni, 2009)

As highlighted above, clearly the epistemic uncertainties address mostly the phenomena underlying the passive operation and the parameters and models used in the T-H analysis of the system (including the ones related to the best estimate code) and the system failure analysis itself. Some of the sources of uncertainties include but are not limited to the definition of failure of the system used in the analysis, the simplified model used in the analysis, the analysis method and the analysis focus of failure locations and modes and finally the selection of the parameters affecting the system performance. With this respect, it is important to underline, again, that the lack of relevant reliability and operational data imposes the reliance on the underlying expert judgment for an adequate treatment of the uncertainties, thus making the results conditional upon the expert judgment elicitation process. This can range from the simple engineering/subjective assessment to a well structured procedure based on expert judgment elicitation, as reported in Ricotti et al. (2002), which outlines the main aspects of the REPAS procedure.
In that (Ricotti et al., 2002), in order to simplify both the identification of the ranges and their corresponding probabilities, initially discrete values have been selected. As a general rule, a central pivot has been identified, and then the range has been extended to higher and lower values, if applicable. The pivot value represents the nominal condition for the parameter. The limits have been chosen in order to exclude unrealistic values or those values representing a limit zone for the operation demand of the passive system. Once the discrete ranges have been set up, discrete probability distributions have been associated, to represent the probabilities of occurrence of the values. As in the previous step, the general rule adopted is that the higher probability of occurrence corresponds to the nominal value for the parameter. Then lower probabilities have been assigned to the other values, as much low the probability as much wide the distance from the nominal value, as in a sort of Gaussian distribution.
Ultimately, as underlined in the previous section, the methodologies proposed in RMPS and within the studies conducted by MIT address the question by propagating the parameter and model uncertainties,

by performing Monte Carlo simulations on the detailed T-H model based on a mechanistic code, and calculating the distribution of the safety variable and thus the probability of observing a value above the defined limit, according to the safety criterion.

5. Dependencies

Similar to some other types of analyses for nuclear power plants, the documented experience with PSS reliability seems to focus on the analysis of one passive attribute at a time. In many cases, this may be sufficient, but for some advanced designs with multiple passive features, modeling of the synergistic effects among them is important. For example, modeling of a passive core cooling system may require simultaneous modeling of the amount of non condensable gases which build up along the circuit during extended periods of operation, the potential for stratification in the cooling pool, and interactions between the passive core cooling system and the core. Analysis of each of these aspects independently may not fully capture the important boundary conditions of each system. For instance, with regard to the aforementioned methodologies, the basic simplifying assumption of independence among system performance relevant parameters, as the degradation measures, means that the correlation among the critical parameter distributions is zero or is very low to be judged significant, so that the assessment of the failure probability is quite straightforward. If parameters have contributors to their uncertainty in common, the respective states of knowledge are dependent. As a consequence of this dependence, parameter values cannot be combined freely and independently. Instances of such limitations need to be identified and the dependencies need to be quantified. If the analyst knows of dependencies between parameters explicitly, multivariate distributions or conditional subjective pdfs (probability density functions) may be used. The dependence between the parameters can be also introduced by covariance matrices or by functional relations between the parameters.

As observed by Nayak (2008), both REPAS and RMPS approaches adopt a probability density function (pdf) to treat variations of the critical parameters considered in the predictions of codes. To apply the methodology, one needs to have the pdf values of these parameters. However, it is difficult to assign accurate pdf treatment of these parameters, which ultimately define the functional failure, due to the scarcity of available data, both on an experimental and operational ground. Moreover, these parameters are not really independent ones to have deviation of their own. Rather deviations of them from their nominal conditions occur due to failure/malfunctioning of other components or as a result of the combination with different concomitant mechanisms. Thus the hypothesis of independence among the failure driving parameters appears non proper.

With reference to the functional reliability approach set forth in (Burgazzi, 2003), the selected representative parameters defining the system performance, for instance coolant flow or exchanged thermal power, are properly modeled through the construction of joint probability functions in order to assess the correspondent functional reliability. A recent study shows how the assumption of independence between the marginal distributions to construct the joint probability distributions to evaluate system reliability adds conservatism to the analysis (Burgazzi, 2008a): for this reason the model is implemented to incorporate the correlations between the parameters, in the form of bivariate normal probability distributions. That study has the merit to highlight the dependence among the parameters underlying the system performance: further studies are underway, with regard, for instance to the approach based on independent failure modes. As described in the previous section 2, this approach begins by identifying critical parameters, properly modeled through probability functions, as input to basic events, corresponding to the failure modes, arranged in a series system configuration, assuming non-mutually exclusive independent events. It introduces a high level of conservatism as it appears that the probability of failure of the system is relevantly high to be considered acceptable, because of the combination of various modes of failure, where a single fault is sufficient to challenge the system performance. Initial evaluations (Burgazzi, 2009) reveal that the critical parameters are not suitable to be chosen independently of each other, mainly because of the expected synergism between the different phenomena under investigation, with the potential to jeopardize the system performance. This conclusion allows the implementation of the proposed methodology, by properly capturing the interaction between various failure modes, through modeling system performance under multiple degradation measures. It was verified that when the multiple degradation measures in a system are

correlated, an incorrect independence assumption may overestimate the system reliability, according to a recent study (Burgazzi, 2011).

6. Integration of passive system within PSA

PSA has been introduced for the evaluation of design and safety in the development of those reactors. A technology-neutral framework, that adopts PSA information as a major evaluation tool, has been proposed as the framework for the evaluation of safety or regulation for those reactors (USNRC, 2007; IAEA, 2007). To utilize this framework, the evaluation of the reliability of Passive Systems has been recognized as an essential part of PSA.

In PSA, the status of individual systems such as a passive system is assessed by an accident sequence analysis to identify the integrated behavior of a nuclear system and to assign its integrated system status, i.e. the end states of accident sequences. Because of the features specific of a passive system, it is difficult to define the status of a passive system in the accident sequence analysis. In other words, the status of a passive system does not become a robust form such as success or failure, since "intermediate" modes of operation of the system or equivalently the degraded performance of the system (up to the failure point) is possible. This gives credit for a passive system that "partially works" and has failed for its intended function but provides some operation: this operation could be sufficient to prolong the window for opportunity to recover a failed system, for instance through redundancy configuration, and ultimately prevent or arrest core degradation (Burgazzi, 2009). This means that the status of a passive system can be divided into several states, and each status is affected by the integrated behavior of the reactor, because its individual performance is closely related with the accident evolution and whole plant behavior.

Burgazzi (2008b) lays the foundations to outline a general approach for the integration of a passive system, in the form of a front line system and in combination with active ones and/or human actions, within a PSA framework.

In Marques (2005) a consistent approach, based on an event tree representation, has been developed to incorporate in a PSA study the results of reliability analyses of passive systems obtained on specific accident sequences. In this approach, the accident sequences are analyzed by taking into account the success or the failure of the components and of the physical process involved in the passive systems. This methodology allows the probabilistic evaluation of the influence of a passive system on a definite accident scenario and could be used to test the advantage of replacing an active system by a passive system in specific situations.

However in order to generalize the methodology, it is important to take into account the dynamic aspects differently than by their alone modeling into the T-H code. Indeed in complex situations where several safety systems are competing and where the human operation cannot be completely eliminated, this modeling should prove to be impossible or too expensive in computing times. It is thus interesting to explore other solutions already used in the dynamic PSA, like the method of the dynamic event trees, in order to capture the interaction between the process parameters and the system state within the dynamical evolution of the accident.

In the PSA of nuclear power plants (NPPs), accident scenarios, which are dynamic in nature, are usually analyzed with event trees and fault trees.

The current PSA framework has some limitations in handling the actual timing of events, whose variability may influence the successive evolution of the scenarios, and in modeling the interactions between the physical evolution of the process variables (temperatures, pressures, mass flows, etc.,) and the behavior of the hardware components. Thus, differences in the sequential order of the same success and failure events and the timing of event occurrence along an accident scenario may affect its evolution and outcome; also, the evolution of the process variables (temperatures, pressures, mass flows, etc.,) may affect the event occurrence probabilities and thus the developing scenario. Another limitation lies in the binary representations of system states (i.e., success or failure), disregarding the intermediate states, which conversely concern the passive system operation, as illustrated above.

To overcome the above-mentioned limitations, dynamic methodologies have been investigated which attempt to capture the integrated response of the systems/components during an accident scenario (Mercurio et al. 2009).

The most evident difference between dynamic event trees (DETs) and the event trees (ETs) is as follows. ETs, which are typically used in the industrial PSA, are constructed by an analyst, and their branches are based on success/ failure criteria set by the analyst. These criteria are based on simulations of the plant dynamics. Instead, DETs are produced by a software that embeds the models to simulate the plant dynamics into stochastic models of components failure. A challenge arising from the dynamic approach to PSA is that the number of scenarios to be analyzed is much larger than that of the classical fault/event tree approaches, so that the a posteriori information retrieval can become quite burdensome and difficult.
This is even more relevant as far as thermal hydraulic natural circulation passive systems are concerned since their operation is strongly dependent, more than other safety systems, upon time and the state/parameter evolution of the system during the accident progression.
Merging probabilistic models with T-H models, i.e. dynamic reliability, is required to accomplish the evaluation process of T-H passive systems in a consistent manner: this is particularly relevant with regard to the introduction of a passive system in an accident sequence, since the required mission could be longer than 24 h as usual level 1 PSA mission time. In fact for design basis accidents, the passive systems are required to establish and maintain core cooling and containment integrity, with no operator intervention or requirement for a.c. power for 72 h, as a grace time (R. A. Matzie and A. Worrally, 2004).
The goal of dynamic PRA is to account for the interaction of the process dynamics and the stochastic nature/behavior of the system at various stages: it associates the state/parameter evaluation capability of the thermal hydraulic analysis to the dynamic event tree generation capability approach. The methodology should estimate the physical variation of all technical parameters and the frequency of the accident sequences when the dynamic effects are considered. If the component failure probabilities (e.g. valve per-demand probability) are known, then these probabilities can be combined with the probability distributions of estimated parameters in order to predict the probabilistic evolution of each scenario outcome.
A preliminary attempt in addressing the dynamic aspect of the system performance in the frame of passive system reliability is shown in (Burgazzi, 2008c), which introduces the T-H passive system as a non-stationary stochastic process, where the natural circulation is modeled in terms of time-variant performance parameters, (as for instance mass flow-rate and thermal power, to cite any) assumed as stochastic variables. In that work, the statistics associated with the stochastic variables change in time (in terms of associated mean values and standard deviations increase or decrease, for instance), so that the random variables have different values in every realization, and hence every realization is different.

7. Comparative assessment between active and passive systems

The design and development of future water-cooled reactors address the use of passive safety systems, i.e. those characterized by no or very limited reliance on external input (forces, power or signal, or human action) and whose operation takes advantage of natural forces, such as free convection and gravity, to fulfill the required safety function and to provide confidence in the plant's ability to handle transients and accidents. Therefore, they are required to accomplish their mission with a sufficient reliability margin that makes them attractive as an important means of achieving both simplification and cost reduction for future plants while assuring safety requirements with lesser dependence of the safety function on active components like pumps and diesel generators.
On the other hand, since the magnitude of the natural forces, which drive the operation of passive systems, is relatively small, counter-forces (e.g. friction) can be of comparable magnitude and cannot be ignored as is generally the case with pumped systems. This concern leads to the consideration that, despite the fact that passive systems "should be" or, at least, are considered, more reliable than active ones - because of the smaller unavailability due to hardware failure and human error - there is always a nonzero likelihood of the occurrence of physical phenomena leading to pertinent failure modes, once the system enters into operation.
These characteristics of a high level of uncertainty and low driving forces for heat removal purposes justify the comparative evaluation between passive and active options, with respect to the accomplishment of a defined safety function (e.g. decay heat removal) and the generally accepted

viewpoint that passive system design is more reliable and more economical than active system design has to be discussed (JiYong and Golay, 2008).
Here are some of the cons and pros of the passive systems that should be evaluated vs. the correspondent active system.

Advantages

- No external power supply: no loss of power accident has to be considered.
- No human factor, implying no inclusion of the operator error in the analysis.
- Better impact on public acceptance, due to the presence of "natural forces".
- Less complex system than active and therefore economic competitiveness.
- Passive systems must be designed with consideration for ease of ISI, testing and maintenance so that the dose to the worker is much less.

Drawbacks

- Reliance on "low driving forces", as a source of uncertainty, and therefore need for T-H uncertainties modeling.
- Licensing requirement (open issue), since the reliability has to be incorporated within the licensing process of the reactor. For instance the PRA's should be reviewed to determine the level of uncertainty included in the models.
- Need for operational tests, so that dependence upon human factor can not be neglected.
- Reliability assessment in any case. Quantification of their functional reliability from normal power operation to transients including accidental conditions needs to be evaluated. Functional failure can happen if the boundary conditions deviate from the specified value on which the performance of the system depends.
- Ageing of passive systems must be considered for longer plant life; for example corrosion and deposits on heat exchanger surfaces could impair their function.
- Economics of advanced reactors with passive systems, although claimed to be cheaper, must be estimated especially for construction and decommissioning.

The question whether it is favorable to adopt passive systems in the design of a new reactor to accomplish safety functions is still to be debated and a common consensus has not yet been reached, about the quantification of safety and cost benefits which make nuclear power more competitive, from potential annual maintenance cost reductions to safety system response.

8. Criticality analysis

Based on the analysis of the criticalities related to the open points discussed in the previous section a qualitative analysis, on the basis of the author's opinion, reported in Table 3 below aims at identifying for each of the above items both the criticality with respect to the passive system reliability assessment process, in terms of the relative importance and the existing advancement, according to table 4 which ranks the relative level of both the importance and progress.

Item	Importance	Advance
Uncertainties	H	L
Dependencies	M	L
Integration within PSA	M	L
Passive vs. Active	H	L

Table 3. Importance analysis

	Grade	Definition
Importance	H	The item is expected to have a significant impact on the system failure
	M	The item is expected to have a moderate impact on the system failure
	L	The item is expected to have only a small impact on the system failure
Advance	H	The issue is modeled in a detailed way with adequate validation
	M	The issue is represented by simple modeling based on experimental observations or results.
	L	The issue is not represented in the analysis or the models are too complex or inappropriate which indicates that the calculation results will have a high degree of ambiguity

Table 4. Grade rank for importance and advancement analysis

It is clear that he worst case is characterized by “high “and “low” rankings relative respectively to the importance and the advancement aspects, thus making the correspondent item development a critical challenge.
Based on this, the results of this qualitative analysis show the relevance relative to the uncertainties and the comparison between active and passive, as most critical points to be addressed in the application of the PRA to the evaluation of the passive system performance assessment. This allows the analyst to track a viable R&D program to deal with these issues and limitations and to steer the relative efforts towards their implementation.

9. Conclusions

Due to the specificities of passive systems that utilize natural circulation (small driving force, large uncertainties in their performance, lack of data…), there is a strong need for the development and demonstration of consistent methodologies and approaches for evaluating their reliability. This is a crucial issue to be resolved for their extensive use in future nuclear power plants. Recently, the development of procedures suitable for establishing the performance of a passive system has been proposed: the unavailability of reference data makes troublesome the qualification of the achieved results. These procedures can be applied for evaluating the acceptability of a passive system, specifically when nuclear reactor safety considerations are important for comparing two different systems having the same mission and, with additional investigation, for evaluating the performance of an active and passive system on a common basis. The study while identifying limitations of the achieved results or specific significant aspects that have been overlooked has suggested areas for further development or improvements of the procedures:

- In order to get confidence in the achieved results, the reduction of the so identified level of uncertainty pertaining to the passive system behavior, and regarding in particular the

phenomenological uncertainty. In fact, it's worth noting that these uncertainties are mainly related to the state of knowledge about the studied object/phenomenon, i.e., they fall within the class of epistemic uncertainties, thus suitable for reduction by gathering and analyzing a relevant quantity of information and data.

- The determination of the dependencies among the relevant parameters adopted to analyze the system reliability.

- The study of the dynamical aspects of the system performance, because the inherent dynamic behavior of the system to be characterized: this translates into the development of the dynamic event tree.

- The comparison against the active system, also to evaluate the economical competitiveness, while assuring the same level of safety.

Future research in nuclear safety addressing this specific topic relevant to advanced reactors should be steered towards all these points in order to foster and add credit to any proposed approach to address the issue and to facilitate the proposed methods endorsement by the scientific and technical community.

References

Apostolakis G., Pagani L. and Hejzlar, P., 2005. The Impact of Uncertainties on the Performance of Passive Systems. Nuclear Technology 149, 129–140

Apostolakis G., Mackay F., and. Hejzlar P, 2008. Incorporating Reliability Analysis into the Design of Passive Cooling System with an Application to a Gas-Cooled Reactor. Nuclear Engineering & Design 238, 217-228

Burgazzi, L., 2002. Passive System Reliability Analysis: a Study on the Isolation Condenser, Nuclear Technology 139, 3-9.

Burgazzi, L., 2003. Reliability Evaluation of Passive Systems through Functional Reliability Assessment, Nuclear Technology 144, 145-151.

Burgazzi, L., 2004. Evaluation of Uncertainties related to Passive Systems Performance. Nuclear Engineering and Design 230, 93-106.

Burgazzi, L, 2007a. State of the Art in the Reliability of Thermal-Hydraulic Passive Systems. Reliability Engineering and System Safety 92, 671-675.

Burgazzi, L., 2007b. Addressing the Uncertainties related to Passive System Reliability. Progress in Nuclear Energy 49, 93-102.

Burgazzi, L. 2007c. Thermal-hydraulic Passive System reliability-based design approach, Reliability Engineering and System Safety 92 (9), 1250-1257.

Burgazzi, L., 2008a. Reliability Prediction of Passive Systems based on Bivariate Probability Distributions, Nuclear Technology 161, 1-7.

Burgazzi, L., 2008b. Incorporation of Passive Systems within a PRA Framework. Proceedings of PSAM9, 9th International Probabilistic, Safety Assessment and Management Conference, Hong Kong, 18-23 May 2008.

Burgazzi, L., 2008c. About Time-variant Reliability Analysis with Reference to Passive Systems Assessment. Reliability Engineering and System Safety 93, 1682-1688.

Burgazzi, L., 2009. Evaluation of the Dependencies related to Passive System Failure. Nuclear Engineering and Design 239, 3048-3053

Burgazzi, L., 2011. Reliability Prediction of Passive Systems with Multiple Degradation Measures, Nuclear Technology 173, 153-161.

IAEA TEC-DOC-626, 1991. Safety Related Terms for Advanced Nuclear Power Plants. September 1991.

IAEA TEC DOC-1474, 2005. Natural Circulation in Water Cooled Nuclear power Plants. Phenomena, models, and methodology for system reliability assessments, November 2005.

IAEA TECDOC-1624, 2009. Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants. November 2009

IAEA, 2007. Proposal for a technology-neutral safety approach for new designs. International Atomic Energy Agency, TECDOC-1570, Vienna.

Jafari, J., D'Auria F., et al., 2003. Reliability Evaluation of a Natural Circulation System. Nuclear Engineering and Design 224, 79–104.

Lorenzo G., et al., Assessment of an Isolation Condenser of an Integral Reactor in View of Uncertainties in Engineering Parameters, Science and technology of Nuclear Installations, Volume 2011, Article ID 827354, 9 pages

Marques, M., Burgazzi L., et al., 2005. Methodology for the Reliability Evaluation of a Passive System and its Integration into a Probabilistic Safety Assessment. Nuclear Engineering and Design 235, 2612-2631.

Matzie, R. A. and Worrally, A., The AP1000 reactor—the Nuclear Renaissance Option. Nuclear Energy, 2004, 43, No. 1, Feb., 33–45

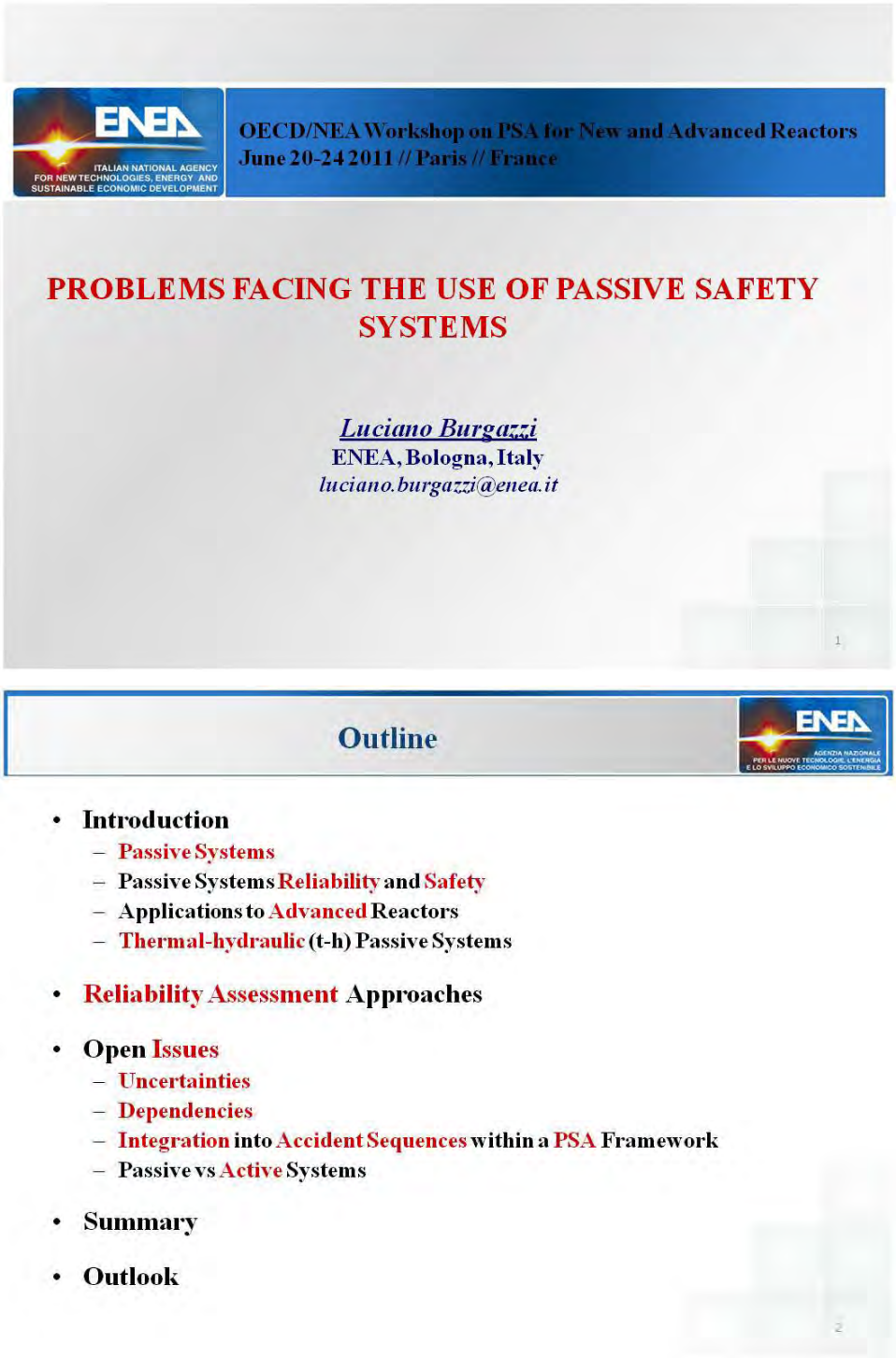
Mercurio, D., Podofillini, L., Zio, E., Identification and Classification of Dynamic Event Tree Scenarios via Possibilistic Clustering: Application to a Steam Generator Tube Rupture Event. Accident Analysis and Prevention 41 (2009), 1180–1191

Nayak, A.K., et al., 2008. Passive System Reliability Analysis using the APSRA Methodology. Nuclear Engineering and Design 238, 1430-1440. NEA CSNI/WGRISK, 2002. Workshop on Passive Systems Reliability—A Challenge to Reliability, Engineering and Licensing of Advanced Nuclear Power Plants. Cadarache, (F), 4-6/03/'02, NEA/CSNI/R (2002)10

Ricotti M.E., Zio E., D'Auria F., Caruso G., 2002. Reliability Methods for Passive Systems (RMPS) Study – Strategy and Results, in proceedings of the NEA CSNI/WGRISK Workshop on Passive System Reliability. A Challenge to Reliability Engineering and Licensing of Advanced Nuclear Power Plants, 146-163

USNRC, 2007. Feasibility study for a risk-informed and performance-based regulatory structure for future plant licensing. US Nuclear Regulatory Commission, NUREG-1860.

Zio, E., Pedroni, N., 2009. Building Confidence in the Reliability Assessment of Thermal hydraulic Passive Systems. Reliability Engineering and System Safety, 94, 268-281. JiYong Oh and Golay, M., 2008. Methods for Comparative Assessment of Active and Passive Safety Systems with respect to Reliability, Uncertainty, Economy and Flexibility. Proceedings of PSAM9, 9th International Probabilistic, Safety Assessment and Management Conference Hong Kong, 18-23 May 2008.


ENEA
ITALIAN NATIONAL AGENCY FOR NEW TECHNOLOGIES, ENERGY AND SUSTAINABLE ECONOMIC DEVELOPMENT
OECD/NEA Workshop on PSA for New and Advanced Reactors
June 20-24 2011 // Paris // France
PROBLEMS FACING THE USE OF PASSIVE SAFETY SYSTEMS
Luciano Burgazzi
ENEA, Bologna, Italy
luciano.burgazzi@enea.it
1
Outline
ENEA
AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE
• Introduction
– Passive Systems
– Passive Systems Reliability and Safety
– Applications to Advanced Reactors
– Thermal-hydraulic (t-h) Passive Systems
• Reliability Assessment Approaches
• Open Issues
– Uncertainties
– Dependencies
– Integration into Accident Sequences within a PSA Framework
– Passive vs Active Systems
• Summary
• Outlook
2

Generics

- Innovative reactors largely implement passive safety systems
- Reactivity control, decay heat removal, fission product containment
- Applications of passive systems for innovative reactors demand high availability and reliability
- PSA analysis
- Accident sequence definition and assessment
  - Event Tree and Fault Tree model
- Introduction of a passive system within an accident scenario in the fashion of a front-line system and in combination with active systems and human actions

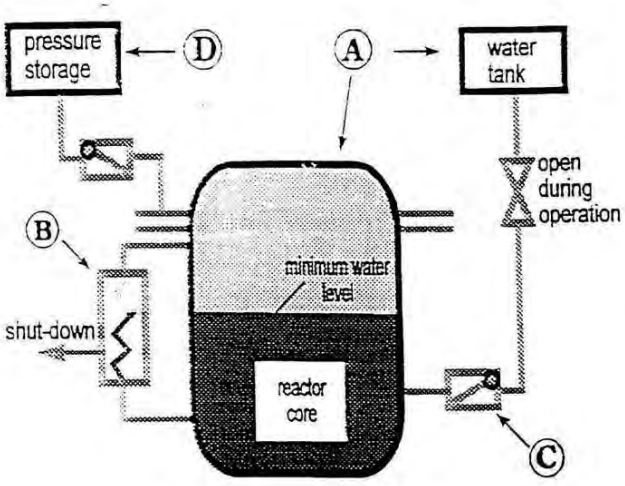
Recalls

- IAEA (*IAEA-TECDOC-626*) definitions:
  - *Passive Component*: a component which does not need any external input to operate
  - *Passive System*: either a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation
- Passive System Categorization:
  - A: physical barriers and static structures,
  - B: moving working fluids,
  - C: moving mechanical parts,
  - D: external signals and stored energy (passive execution/active initiation)

Classification of Passive Systems

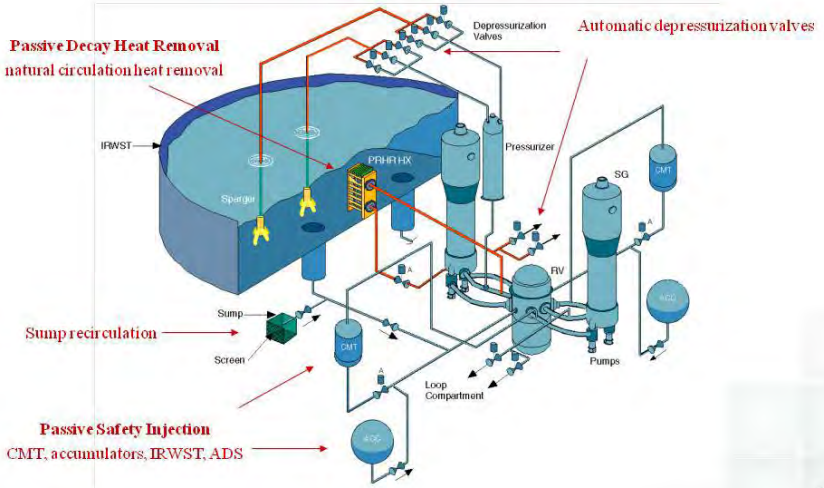
	Category-A	Category-B	Category-C	Category-D
Input Signal, External Power Sources, Forces	No	No	No	Yes
Moving Mechanical Parts	No	No	Yes	Yes
Moving Working Fluid	No	Yes	Yes/No	Yes/No
Some examples	▪ Core cooling system relying only on radiation/ conduction ▪ Physical barriers against release of fission products	▪ Reactor cooling based on natural circulation	▪ Systems consisting of accumulators or storage tanks and discharge lines equipped with check valves. ▪ Mechanical actuators such as check valves and spring loaded relief valves	▪ Emergency core cooling systems based on gravity/compress -ed Nitrogen driven flow of water activated by battery-powered valves. ▪ Mechanical Shut-Off rods

Examples



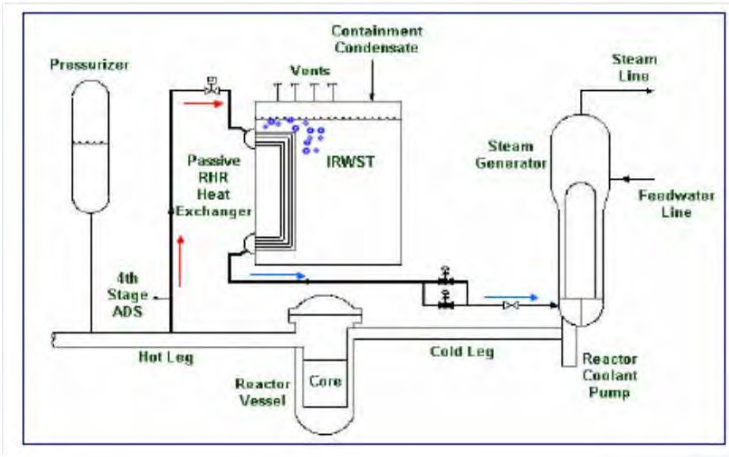
Passive Systems in Advanced Reactors

AP1000 Passive Core Cooling System



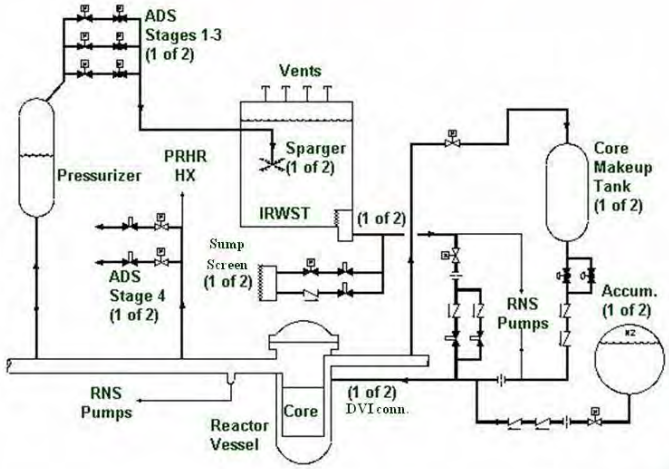
Passive Systems in Advanced Reactors

AP1000 Passive Residual Heat Removal (PRHR)



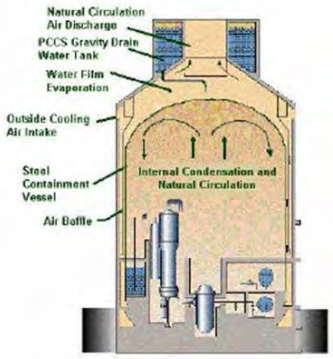
Passive Systems in Advanced Reactors

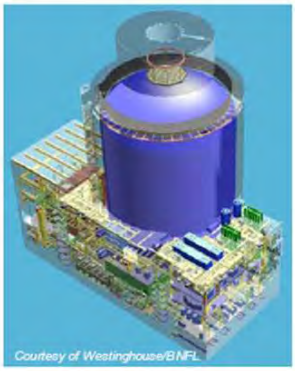
AP1000 Passive Safety Injection



Passive Systems in Advanced Reactors

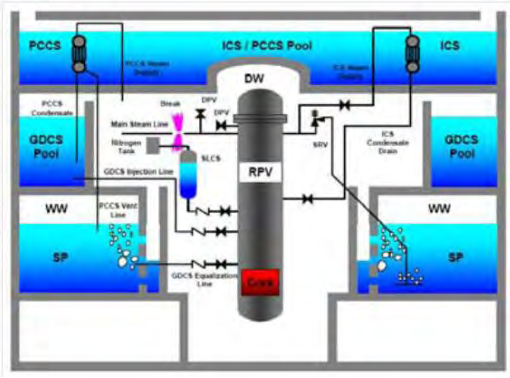
AP1000 Containment and Passive Containment Cooling System (PCCS)





Passive Systems in Advanced Reactors

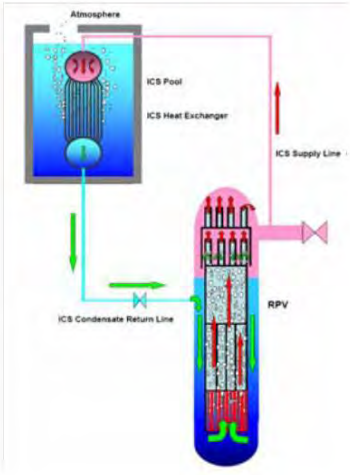
ESBWR design and passive safety systems



11

Passive Systems in Advanced Reactors

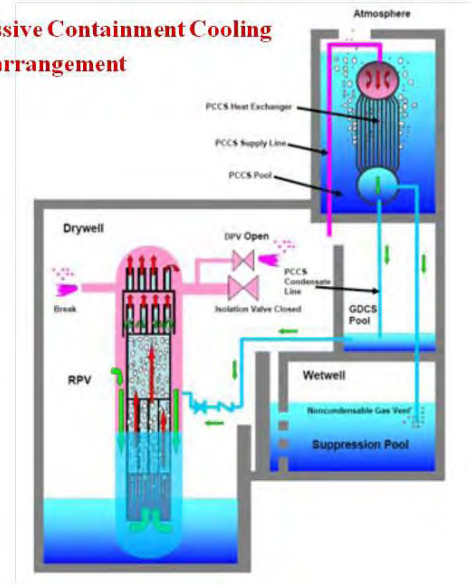
ESBWR Isolation Condenser arrangement



12

Passive Systems in Advanced Reactors

ESBWR Passive Containment Cooling Condenser arrangement



13

Passive System Reliability

- Probabilistic reliability methods for passive A safety systems have been extensively developed and applied in fracture mechanics
- For several passive C and D systems reliability figures may be derived from operating experience
- For passive B type systems basing on physical principle (natural circulation, i.e. gravity and density difference) denoted as t-h (thermal-hydraulic) passive systems, there is no agreed approach towards their reliability assessment yet
- T-h passive system reliability
  - deviations of natural forces or physical principles from the expected conditions, rather than classical component mechanical and electrical faults

14

Thermal-hydraulic Passive System Reliability

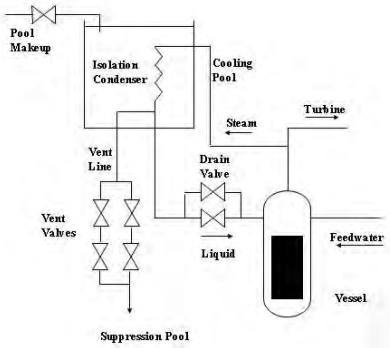
- **Natural circulation**: small engaged driving forces and thermal-hydraulic factors affecting the passive system performance (e.g. non condensable fraction, heat losses)
- System from the **predictable** nominal performance to the state of degradation of the physical principle in varying degrees up to the failure
- Occurrence of **physical phenomena** leading to pertinent **failure modes**, as:
  - non-condensable gas build-up, thermal stratification and heat transfer rate degradation
- Physical principle deterioration dependency on the **boundary conditions** and **mechanisms** needed for start-up and maintain the **intrinsic** principle
- Passive Systems for **decay heat removal** implementing in-pool heat exchangers and foreseeing the free convection (e.g. **PRHR** for AP 600 and AP 1000, **Isolation Condenser** for SBWR and ESBWR)

15

T-h Passive Systems in Advanced Reactors

Isolation Condenser (SBWR, ESBWR)

- Core Decay Heat removal from the reactor, by natural circulation following an isolation transient, including a **heat source** and a **heat sink** where **condensation** occurs via a heat exchanger
- Limit the **overpressure** in the reactor system at a value below the set-point of the safety relief valves, preventing unnecessary reactor depressurization
- Isolation Condenser **actuation** on MSIV position, high reactor pressure and low reactor level



Scheme of the Isolation Condenser

16

Thermal-hydraulic Passive System Reliability

- **System/component reliability (piping, valves, etc.)**
  - mechanical component reliability
- **Physical phenomena "stability" (natural circulation)**
  - factors impairing the performance/stability of the physical principle (gravity and density difference) upon which passive system operation is relying
  - dependency on the surrounding conditions related to accident progress, affecting system behaviour
  - this could require not a unique unreliability figure, but the reevaluation for each sequence following an accident initiator
  - thermal-hydraulic analysis is helpful to evaluate parameter evolution

17

Thermal-hydraulic Passive System Reliability

- **Difference between**
  - Passive system availability
    - probability of system start-up and natural convection inception
  - Passive system reliability
    - probability of the system to accomplish the safety function, along the designated mission time
    - conditional on natural circulation activation
- **Uncertainties related to the performance assessment**
  - aleatory, e.g., initial conditions, geometry, materials
  - subjective or epistemic, e.g. t-h correlations (both analytical and experimental) and coefficients for system t-h modeling

18

Exisiting Methodologies for Passive System Reliability Assessment

- **Reliability of passive safety systems** has been considered as an important international **standard problem exercise**
- To achieve a **consistent** methodology
  - to capture all the phenomena involved and their interactions
  - to merge **probabilistic** and **physical**, i.e. t-h, aspects (t-h simulations)
- **REPAS (REliability of PAssive Systems) (late '90s)**
  - ENEA, University of Pisa, Polytechnic of Milano, University of Rome
    - J. Jafari, F.D'Auria, H. Kazeminejd, H. Davilu, *Reliability evaluation of a natural circulation system, Nuclear Engineering and Design 224 (2003) 79–104*
- **RMPS (Reliability Methods for Passive Safety Functions)**
  - Fifth European Union Framework Programme project (2001-2004)
    - Marques M., et al., *Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment,* Nuclear Engineering and Design 235 (2005) 2612–2631
- **APSRA (Assessment of Passive System ReliAbility)**
  - Bhabha Atomic Research Centre (India)
    - Nayak A. K., et al., *Passive system reliability analysis using the APSRA methodology,* Nuclear Engineering and Design, Volume: 238, Issue: 6, June, 2008, pp. 1430-1440

19

Exisiting Methodologies for Passive System Reliability Assessment

- **RMPS**
  - **identification** and **quantification** of the sources of **uncertainties** and determination of the **important** variables
  - **propagation** of the uncertainties through a t-h model and **reliability** evaluation of the t-h passive system
  - **integration** of the t-h passive system in an **accident sequence**, as a basic event
- **APSRA**
  - **failure surface: deviations** of all critical parameters influencing the system performance through test data analysis
  - causes of deviation through **mechanical** components (as valves, control systems, etc.) failure analysis
  - **failure probability** through **classical PSA** (fault tree)

20

Exisiting Methodologies for Passive System Reliability Assessment

- Currently, the APSRA methodology developed by BARC and the RMPS methodology developed by EU are used for analyzing reliability of passive safety systems
- While in the RMPS methodology the deviation of key parameters causing the failure of the system is accounted by a probability density function based on expert judgment, on the other hand, in the APSRA methodology the functional failure due to deviation of parameters is correlated with the failure of actual components
- The APSRA methodology relies on in-house experimental data to account code and modeling uncertainties unlike that in RMPS methodology

21

Open Issues Related to t-h Passive System Reliability

- Analysis of the different methodologies proposed so far
- Uncertainties
  - Passive system performance
  - T-h code
- Dependencies
  - Relevant parameters
- Integration within an accident sequence within a Probabilistic Safety Assessment (PSA) framework, in combination with an active systems and human actions
- Passive vs active systems

22

Sources of Uncertainties related to Passive System Evaluation

- **Uncertainties related to natural circulation system behaviour prediction**
  - **deviations of the natural forces or physical principles from the expected conditions**
  - **phenomenological uncertainties, due to scarcity of operational and experimental data**
  - **best estimate code (e.g. RELAP, CATHARE) uncertainties**
    - inadequate physical models built in the codes to represent a specific phenomena;
    - absence of models to represent a particular phenomena;
    - approximation in simulating system geometry;
    - deviations of the input parameters in respect of initial and boundary conditions;
    - uncertainties in thermophysical properties and thermohydraulic relationships
- **Difficulties in performing meaningful reliability analysis and deriving credible reliability figures**
- **Expert judgment elicitation and engineering/subjective judgment**

23

Sources of Uncertainties related to Passive System Evaluation

Aleatory
Geometrical properties
Material properties
Initial/boundary conditions (design parameters)
Epistemic
T-H analysis
Model (correlations)
Parameters
System failure analysis
Failure criteria
Failure modes (critical parameters)

Categories of uncertainties associated with T-H passive systems reliability assessment

Zio, E., Pedroni, N., *Building confidence in the reliability assessment of thermal hydraulic passive systems.* Reliability Engineering and System Safety, 94 (2009), 268-281

24

Dependencies

- Assumption of independence among relevant parameters adopted in the analysis
  - safety variables
    - e.g. flow rate, exchanged heat
  - critical parameters driving the modes of failure
    - e.g. non-condensable gas
- In case of dependence (e.g. degradation measures), parameters can not be combined freely and independently
- Joint pdfs, e.g. multivariate distributions
- Conditional subjective probability distributions
- Covariance matrix
- Functional relationships between the parameters

25

Event Tree Development

- Limitations of PSA (event tree development)
  - binary representation (success or failure, intermediate states are usually not treated)
  - time treatment (chronology of events instead of actual timing)
- Need for the development of dynamic event tree in order to evaluate the interaction between the parameter evolution during the accident and the system state
- Evaluation for 72 hours grace period, compared to 24 hours in classical PSA
- Time-variant stochastic process
  - the evolution of physical parameters over time, in terms of probability distributions

26

Active vs Passive

- **Functional and economic comparison of active vs passive safety systems, required to accomplish the same mission**
- **Passive**
  - **Advantages e.g.,**
    - **no external power supply: no loss of power accident**
    - **no human factor**
    - **better impact on pubblic acceptance, due to the presence of "natural forces"**
    - **less complex system than active and therefore economic competitiveness**
  - **Drawbacks e.g.,**
    - **reliance on "low driving forces", as a source of uncertainty**
    - **licensing requirement (open issue)**
    - **reliability assessment in any case (lack of data)**

27

Criticality Analysis

Item	Importance	Advance
Uncertainties	H	L
Dependencies	M	L
Integration within PSA	H	L
Passive vs. Active	H	L

Importance analysis

	Grade	Definition
Importance	H	The item is expected to have a significant impact on the system failure
	M	The item is expected to have a moderate impact on the system failure
	L	The item is expected to have only a small impact on the system failure
Advance	H	The issue is modeled in a detailed way with adequate validation
	M	The issue is represented by simple modeling based on experimental observations or results
	L	The issue is not represented in the analysis or the models are too complex or inappropriate which indicates that the calculation results will have a high degree of ambiguity

Grade rank for importance and advancement analysis

28

Summary

- As the future reactor concept makes use of passive safety features in combination with active safety systems, the question of Natural Circulation Decay Heat Removal (NCDHR) reliability and performance assessment into the ongoing PSA constitutes a challenge
- Development of a consistent methodology for the evaluation of the reliability of the passive systems
- Difficulties in evaluation of functional failure of passive systems, i.e. the probability of the system to fail to accomplish the required safety function, e.g.,
  - lack of operational data
  - lack of sufficient experimental data from Integral Facilities or even from Separate Effect Tests in order to understand their performance characteristics not only at normal operation but also during transients and accidents
  - capability of so called "Best Estimate Codes" for such systems
    - uncertainties in prediction
  - difficulty in modeling the physical behavior of such systems, as
    - effect of non-condensable gases on condensation, etc.
  - difficulty in modeling such systems in a probabilistic framework

Path forward (1/2)

- **Future needs**

➢ *Clear rules for identification and quantification of uncertainties*
  ➢ *Formal expert judgment (EJ) protocol to estimate distributions for parameters whose values are either sparse or not available*
  ➢ *Sensitivity analysis techniques to estimate the impact of changes in the input parameter distributions on the reliability estimates*

➢ *Clear distinction between the prediction of the thermal hydraulic code and the true behaviour of the passive system under consideration*
  ➢ *Problem of model uncertainties*

➢ *The time dependence of the passive system reliability*
  ➢ *Dynamic event trees*

Path forward (2/2)

Future needs (following):

- *Evaluation of the dependencies among relevant system parameters*
- *Comparison of different methodologies*
- *Merge elements of different methodologies: RMPS, APSRA/BARC, REPAS methodologies, since high dependency of results upon the assumptions underlying the models*
- *Establish guidelines and criteria for the comparison of active and passive systems*

31

International Efforts in Progress

- **IAEA Coordinated research project (CRP) on *"Development of Methodologies for the Assessment of Passive Safety System Performance in Advanced Reactors"* (2008-2011)**
  - **the objective is to determine a common analysis-and-test method for reliability assessment of passive safety system performance**
- **IAEA CRP on "*Natural Circulation Phenomena, Modelling and Reliability of Passive Systems*" (2004-2008)**
  - **TECDOC-1474, "Natural Circulation in Water Cooled Nuclear Power Plants", November 2005**
  - **TECDOC-1624, "Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants", November 2009**
  - **TECDOC-XXXX, "Natural Circulation in Water-Cooled Nuclear Power Plants: Phenomena, Modelling, and Reliability of Passive Systems that Utilize Natural Circulation", under preparation**

32

NRC ACTIVITIES CONCERNING PSA FOR NEW AND ADVANCED REACTORS

N. Siu, NRC, USA

See the presentation enclosed in this report

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC Activities Concerning PSA for New and Advanced Reactors

Jeffery Wood, Kevin Coyne, Margaret Tobin,
Mark Caruso, Nathan Siu
U.S. Nuclear Regulatory Commission

WGRISK Workshop on PSA for New and Advanced Reactors
OECD Headquarters, Paris, France
June 20-22, 2011

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Outline

- New and Advanced Designs Considered
- Risk-Informed Guidance for New Reactors
- New Reactor SPAR Models
- Risk-Informed Framework and Licensing Reviews for Advanced Reactors
- Technical Research Programs
- Related Activities
- Summary

2

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

New and Advanced Reactor Designs Under Consideration

- "New" Reactor Designs
  - Large LWRs
  - Designs currently under review
- "Advanced" Reactor Designs
  - Integral Pressurized Water Reactors (iPWRs), sodium-cooled fast reactors, HTGRs, other non-large LWR designs
  - Currently engaging in pre-application discussions
  - No applications under review

3

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

New Reactor Designs Under Review

- Designs under review for Design Certification (DC) and Combined License (COL) applications

NPP Design	DC Applicant
Advanced Boiling Water Reactor (ABWR)	GE-Hitachi, Toshiba
Advanced Passive 1000 (AP1000)	Westinghouse
Economic Simplified Boiling-Water Reactor (ESBWR)	GE-Hitachi
U.S. EPR	AREVA
U.S. Advanced Pressurized-Water Reactor (US-APWR)	Mitsubishi Heavy Industries, Ltd.

4

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Use of PSA in NRC Licensing Process

- Applications submitted under 10 CFR 52
  - Require a description of PSA and its results
- Identify risk-informed safety insights
- Compare to Commission's goals for CDF and large release frequency
- Demonstrate risk comparison to existing operating plants
- Support regulatory programs (e.g., RAP, RTNSS, MSPI)

See Reg. Guide 1.206, part C.I.19 for more information

5

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Risk-Informed Guidance for New Reactors

- Commission direction to NRC staff
  - Existing safety goals and risk guidance are sufficient for new plants
  - Engage external stakeholders in "tabletop exercises" to test regulatory tools
- On-going tabletop exercises assessing, for example:
  - Risk-managed technical specifications
  - Application of Maintenance Rule 50.65(a)(4)
  - Reactor Oversight Process

6

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Use of Risk Insights for Advanced Reactors

- Develop a new risk-informed framework (long-term objective)
  - Pilot study on an iPWR design
  - Apply principles of NUREG-1860 approach
- Apply risk insights to licensing reviews of iPWR designs
  - See paper by M. Caruso (this workshop, ML111670023)

7

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Advanced Reactor Policy Issues

- NRC working groups assessing policy issues related to PSA, for example:
  - Multi-module facilities
  - Approach to Defense in Depth
  - Source Term analysis
  - Emergency Planning
  - Human factors and staffing
- See SECY-10-0034 (ML093290245)

8

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

New Reactor SPAR Models

- NRC's independent PSA models
  - ABWR
  - AP1000
  - US-APWR (near completion)
  - Additional new & advanced reactor designs planned
- Scope: Level 1, internal events, at-power
- Used to support:
  - New reactor tabletop exercises
  - Independent validation and risk insights for NRC staff

9

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Research Programs

- HTGR Research Plan
  - Areas addressed include: Fuel Performance, High Temperature Materials, Accident Analysis, Identifying Challenges for PSA
  - See ML110310182
- Digital System Research Plan
  - Sec. 3.1.6 of plan addresses PSA, ML100541484
  - Current focus on incorporating software failures into digital system reliability models
- Human Factors Analysis for New and Advanced Reactors
  - See HTGR Research Plan (ML110310182) and paper S. Fleger, J. O'Hara, "Updating NRC's HFE Design Review Guidance" at 2010 ANS Winter Mtg.

10

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Related Activities

- Participation in development of ASME/ANS PSA Standards
  - PSA Standards under development for
    - Advanced LWRs
    - Advanced Non-LWRs
- Participation in international activities
  - MDEP
  - CNSI / WGRISK
  - CNRA / WGRNR

11

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary

- New Reactor Designs Under Review
  - See http://www.nrc.gov/reactors/new-reactors.html
- Risk-Informed Guidance for New Reactors and Tabletop Exercises
  - See SECY-10-0121(ML102230076) and SRM to SECY-10-0121 (ML110610166)

12

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary (continued)

- Use of Risk Insights for Licensing Advanced Reactors
  - See SRM-COMGBJ-10-0004/COMGEA-10-0001 (ML102510405), SECY-11-0024 (ML110110691), and M. Caruso, et al. "Applying Risk Insights in USNRC Reviews of Integral Pressurized Water Reactor Designs" (this workshop)

13

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary (continued)

- On-going technical research programs (e.g., HTGR research, Digital I&C, etc.)
- Participation in PSA Standards development and international activities

14

ASME/ANS STANDARDS FOR ALWR AND ADVANCED NON-LWR PRA: STATUS AND SOME CHALLENGES

N. Siu, NRC, USA

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ASME/ANS Standards for ALWR and Advanced Non-LWR PRA: Status and Some Challenges

N. Siu, M. Drouin
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

D. Dube
Office of New Reactors
U.S. Nuclear Regulatory Commission

K. Fleming
KNF Consulting LLC

WGRISK Workshop on PSA for New and Advanced Reactors
OECD Headquarters, Paris, France
June 20-22, 2011

1

U.S.NRC
Protecting People and the Environment

PRA Technical Adequacy for New Reactors

- New reactor requirements:
  - Design-specific Level 1 and Level 2 PRA for design certification (DC) and combined license (COL)
  - Plant-specific Level 1 and Level 2 PRA no later than the scheduled date for initial loading of fuel
    - Cover initiating events and modes for which NRC-endorsed consensus standards on PRA exist one year prior to the scheduled date for initial loading of fuel
- RG 1.200 applicable

2

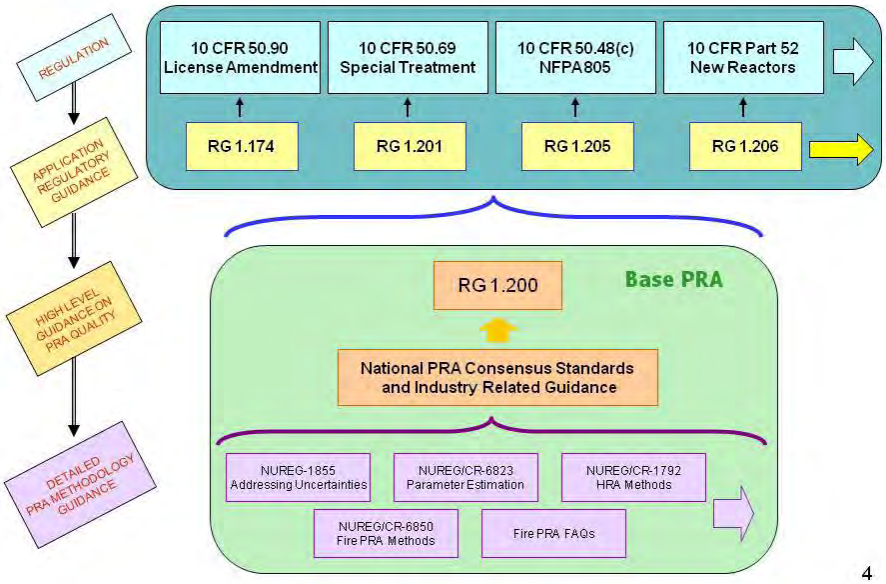
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RG 1.200 for New Reactors

- Expectations for new reactors same as for operating reactors:
  - Obviate the need for an in-depth staff review of the base PRA
  - Allow staff to focus on key assumptions and areas identified by peer reviewers as being of concern
  - Provide for a more focused and consistent review process by the staff
- Standards (and peer review guidance) required for PRA
  - Design and construction stage
  - At initial fuel loading
  - Early operational stage (after fuel loading)
- Standards need to be of sufficient specificity to support the above goals
  - Remove ambiguity with regard to the technical requirements for a PRA in design/construction and early operational stages
  - Parameters for acceptable assumptions for information not available for a PRA in design/construction and early operational stages

3

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment



4

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Content of a PRA Standard

- Standard provides requirements in four areas:
  - Risk assessment application process
    - The requirements for determining, for a given application, what hazards are relevant, and for the relevant hazards whether the requirements are applicable and whether the requirements themselves are sufficient.
  - Technical requirements
    - The requirements for a technically acceptable base PRA for each hazard. The requirements define what is needed, not how to accomplish.
  - Configuration control
    - The requirement for a configuration control of the PRA such that the base PRA represents the as-built and as-operated plant at the time of the application.
  - Peer review
    - The requirements for a peer review of the PRA to evaluate whether the base PRA meets the intent of the technical and configuration control requirements.
- Web-based training will be available

5

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Status of PRA Standard for Advanced LWRs

- Maximum use of existing ASME/ANS PRA Standard for operating units (Level-1 at power)
- Emphasis has evolved from an issue of "advanced" LWR to an issue of "pre-operational" LWR
  - Early design/pre-construction, construction phase, early stages of commercial operation
  - Lack of operating experience, written procedures, and simulator/operator training
  - Inability to 'walkdown' systems pre-construction
- Several approaches considered, no early consensus

6

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Status of PRA Standard for Advanced LWRs (cont'd)

- Proposed approach now a "hybrid" of several alternatives
  - Propose to develop a tabulation with alternative language for those Supporting Requirements (SRs) where changes would be appropriate for a preoperational plant
  - Propose changes to main body language of Standard
  - Harmonize with non-LWR work, as appropriate

7

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Example - Approach to Challenges

HLR-IE-A: The initiating event analysis shall provide a reasonably complete identification of initiating events

IE-A9	CC1	CC2	CC3
ASME/ANS RA-Sa-2009	No requirement for precursor review	REVIEW plant-specific operating experience for initiating event precursors, for identifying additional initiating events. **For example, plant-specific experience with intake structure clogging might indicate that loss of intake structures should be identified as a potential initiating event.**	REVIEW plant-specific and industry operating experience for initiating event precursors, for identifying additional initiating events
Potential Alternative (ALWR, adapted from non-LWR)	CAN BE MET	REVIEW available operating experience from similar plants for initiating event precursors, for the purposes of identifying additional initiating events. Note: Document basis for similarity	REVIEW available operating experience from similar plants **and relevant industry** operating experience for initiating event precursors, for the purposes of identifying additional initiating events. Note: For plants without industry operating experience, the SR is not applicable. Note: Document basis for similarity and relevance.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Example - Approach to Challenges

HLR-IE-C: The initiating event analysis shall estimate the annual frequency of each initiating event or initiating event group

IE-C6	CC1	CC2	CC3
ASME/ANS RA-Sa-2009 and Potential Alternative (ALWR)	Alternative: USE as screening criteria no higher than the following characteristics (or more stringent characteristics as devised by the analyst) to eliminate initiating events or groups from further evaluation: *(a)* the frequency of the event is less than ~~1E-7 per reactor year (/ry)~~ **two orders of magnitude lower than the internal hazards core damage frequency**, and the event does not involve either an ISLOCA, containment bypass, or reactor pressure vessel rupture *(b)* the frequency of the event is less than ~~1E-6 per reactor year (/ry)~~ **one order of magnitude lower than the internal hazards core damage frequency**, and core damage could not occur unless at least two trains of mitigating systems are failed independent of the initiator, or *(c)* the resulting reactor shutdown is not an immediate occurrence. That is, the event does not require the plant to go to shutdown conditions until sufficient time has expired during which the initiating event conditions, with a high degree of certainty (based on supporting calculations), are detected and corrected before normal plant operation is curtailed (either administratively or automatically). If either criterion (a) or (b) above is used, then CONFIRM that the value specified in the criterion meets the applicable requirements in Data Analysis (2-2.6) and Level 1 Quantification (2-2.7).		

9

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Status of PRA Standard for Advanced Non-LWRs

- Approach
  - Self-contained, technology neutral, all sources, scenarios out to release, all hazards, all phases (design, licensing, and operation)
  - Build off of existing and ongoing standards work
- Draft issued Fall, 2008 for public review and comment; ~600 comments received
- PBMR cancelled, withdrew support; NGNP increased support (2010)
- Revised draft completed; potential issuance for ballot review (as trial use standard?) in late summer
- JCNRM to decide whether to move forward (pending review)

10

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Technical Elements

- Plant Operational States Analysis (POS):
- Initiating Events Analysis (IE):
- Event Sequence Analysis (ES):
- Success Criteria (SC):
- Systems Analysis (SY):
- Human Reliability Analysis (HR):
- Data Analysis (DA):
- Internal Flooding Analysis (FL):
- Internal Fire Analysis (FI)
- Seismic Events Analysis (S)
- Other Hazards Screening Analysis (EXT)
- Other Hazards Risk Analysis (X)
- High Winds Analysis (W)
- External Flooding Analysis (XF)
- Event Sequence Quantification (ESQ)
- Mechanistic Source Term Analysis (MS)
- Radiological Consequence Analysis (RC)
- Risk Integration (RI)

11

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Development Challenges

- Technical
  - Design-stage requirements
  - Intermediate states (e.g., "core damage")
  - Multiple modules
- Alignment
  - Existing standards
  - Draft standards and other developments (e.g., ALWR)
- Resources

12

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Example - Approach to Challenges

HLR-IE-B: The initiating event analysis shall group the initiating events so that events in the same group have similar mitigation requirements (i.e., the requirements for most events in the group are less restrictive than the limiting mitigation requirements for the group) to facilitate an efficient, but realistic estimation of ~~CDF~~ the frequency of each modeled event sequence, event sequence family, and release category. (HLR-IE-B).

IE-B1	CC1	CC2	CC3
ASME/ANS RA-Sa-2009	COMBINE initiating events into groups to facilitate definition of accident sequences in the Accident Sequence Analysis (Section 2.2.2) and to facilitate quantification in the Quantification (2.2.7).		
Non-LWR Proposal	GROUP initiating events to facilitate definition of event sequences in the Event Sequence Analysis element (Section 4.5.3) and to facilitate quantification in the Event Sequence Quantification element (Section 4.5.15). Do not GROUP initiating events that impact different combinations of reactor units or modules for plants with multiple reactor units or modules. It is acceptable given the large number of configurations that might be encountered to subsume and screen cases provided that the events and end-states that remain capture the subsumed or screened event adequately.		

13

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Concluding Remarks

- Writing groups are continuing their work
- Challenges remain
  - Technical
  - Alignment
  - Process and schedule
  - Resources
- Further developments this summer?

14

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Additional Examples

15

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Example - Approach to Challenges

HLR-IE-A: The initiating event analysis shall provide a reasonably complete identification of initiating events

IE-A8	CC1	CC2	CC3
ASME/ANS RA-Sa-2009	No requirement for interviews	INTERVIEW plant personnel (e.g., operations, maintenance, engineering, safety analysis) to determine if potential initiating events have been overlooked.	INTERVIEW plant operations, maintenance, engineering, and safety analysis personnel to determine if potential initiating events have been overlooked.
Potential Alternative (ALWR, adapted from non-LWR)	CAN BE MET	Alternative: For PRAs performed prior to plant operation, PERFORM interviews and detailed reviews (e.g., table top reviews, computerized walk-throughs) with engineering to confirm that potential initiating events have not been overlooked. CONFIRM with plant personnel as they become trained using interviews and detailed reviews.	

16

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Example - Approach to Challenges

HLR-IE-C: The initiating event analysis shall estimate the annual frequency of each initiating event or initiating event group

IE-C6	CC1	CC2	CC3
ASME/ANS RA-Sa-2009 IE-C6 and **Potential Alternative (Non-LWR IE-C7)**	USE as screening criteria no higher than the following characteristics (or more stringent characteristics as devised by the analyst) to eliminate initiating events or groups from further evaluation: (a) the frequency of the event is less than 1E-7 per reactor year (/ry) and the event does not involve either ~~an ISLOCA,~~ a containment, confinement, or reactor building bypass, or reactor pressure vessel rupture (b) the frequency of the event is less than 1E-6/ry and ~~core damage~~ a release of radioactive material could not occur unless at least two ~~trains of mitigating systems~~ means of mitigation (means include system trains, inherent reactor features, or barriers to release) are failed independent of the initiator, or (c) the frequency of the event is sufficiently low to ensure that, when combined with a demonstrably conservative assessment of event consequences, the event does not result in a significant contribution to any modeled event sequence, event sequence family, or release category frequency. (d) the resulting reactor shutdown is not an immediate occurrence. That is, the event does not require the plant to go to shutdown conditions until sufficient time has expired during which the initiating event conditions, with a high degree of certainty (based on supporting calculations), are detected and corrected before normal plant operation is curtailed (either administratively or automatically). If either criterion (a) or (b) above is used, then ENSURE that the value specified in the criterion meets the applicable requirements in the Data Analysis section (Section 4.5.7) and the ~~Level 1~~ Event Sequence Quantification section (Section 4.5.15).		

17

INSIGHTS FROM RECENT ACTIVITIES ON PSA BEING PURSUED BY THE IAEA

Irina Kuzmina, IAEA

See the presentation enclosed in this report

International Atomic Energy Agency

Insights from Recent Activities on PSA Being Pursued by the IAEA

Presented by: Irina Kuzmina, Safety Officer
Safety Assessment Section/ Division of Nuclear Installation Safety/
Department of Nuclear Safety and Security/ IAEA
i.kuzmina@iaea.org

Workshop on PSA for New and Advanced Reactors
OECD Conference Centre, Paris, France
20-22 June 2011

OBJECTIVES

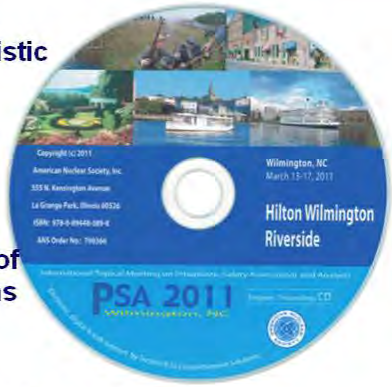
- **To provide a summary of the outcomes and insights from recent activities relating to PSA being pursued by the IAEA:**
  - I. Paper at PSA-2011 Conference in Wilmington, March 2011, "An Approach for Holistic Consideration of Defence in Depth for Nuclear Installations Using Probabilistic Techniques"
  - II. IAEA Technical Meeting on Safety Goals in Application to Nuclear Installations, April 2011
  - III. Guidance on Risk Informed Decision Making
- **To provide a brief overview of IAEA Safety Review Services**

I. IAEA PAPER AT PSA-2011

ANS PSA-2011 Conference

International Topical Meeting on Probabilistic Safety Assessment and Analysis

- Wilmington NC, USA
- March 13-17, 2011



Title of the Paper:

An Approach for Holistic Consideration of Defence in Depth for Nuclear Installations Using Probabilistic Techniques

Authors:

I. Kuzmina, M. El-Shanawany, M. Modro, and A. Lyubarskiy
International Atomic Energy Agency (IAEA)

Paper presents some results of an internal research

IAEA PAPER AT PSA-2011

HIGHLIGHTS

1. **OVERVIEW OF DEFENSE-IN-DEPTH (DiD) SAFETY CONCEPT**
   - **Development**
   - **IAEA publications**
   - **Elements of DiD**
2. **USE OF EVENT TREE TECHNIQUES FOR DiD REPRESENTATION**
3. **DISCUSSION ON DETERMINATION OF REQUIREMENTS FOR RELIABILITY OF PLANT SYSTEMS**
4. **REQUIREMENTS TOWARDS PSA TECHNICAL QUALITY**
5. **CONCLUSIONS**

IAEA PAPER AT PSA-2011

OVERVIEW OF THE DiD SAFETY CONCEPT

- DiD provides a hierarchical deployment of different independent levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials, the workers, public, and the environment, during normal operation and potential accident conditions

KEY OBJECTIVES OF DiD

- To compensate for potential human and component failures
- To maintain the effectiveness of the barriers by averting damage to the plant and to the barriers themselves
- To protect people and the environment from harm in the event that these barriers are not fully effective

IAEA PAPER AT PSA-2011

DEVELOPMENT OF DiD CONCEPT IN IAEA PUBLICATIONS

1988 – INSAG-3, Basic Safety Principles for Nuclear Power Plants: *concept of DiD outlined*

1996 – INSAG-10, DiD in Nuclear Safety: *objectives, strategy, and implementation*

1999 – INSAG-12 (update of INSAG-3): *central concept is DiD*

2000-2005 – IAEA Safety Standards*: DiD emphasized*

2005 – Safety Reports Series No. 46, Assessment of DiD for NPPs: *method for assessing the defence in depth capabilities*

2006 – an extensive program on revision of the existing and development of new IAEA Safety Standards started: *DiD reemphasized*

IAEA PAPER AT PSA-2011

STRUCTURE OF DiD

Levels of DiD	Objective
Level 1: Prevention of abnormal operation and failures	The objective of the first level of protection is the prevention of abnormal operation and system failures.
Level 2: Control of abnormal operation and detection of failures	If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection.
Level 3: Control of accidents within the design basis	Should the second level fail, the third level ensures that safety functions are further performed by activating specific safety systems and other safety features.
Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials.
Level 5: Mitigation of radiological consequences of significant releases of radioactive materials	The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response. The efficacy of the mitigation measures will depend on their overall effectiveness and the speed of their implementation.

International Atomic Energy Agency

IAEA PAPER AT PSA-2011

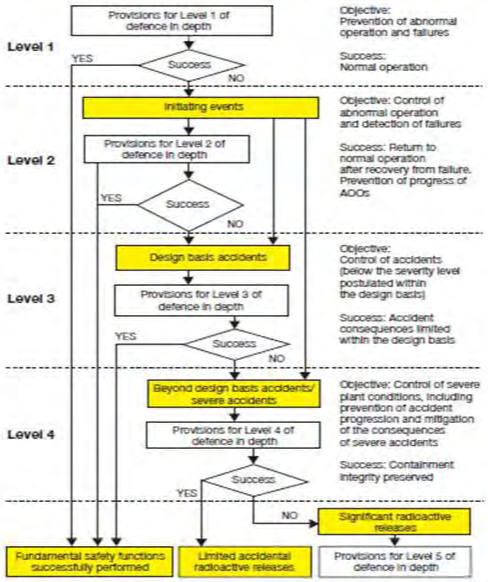
INITIATING EVENTS CONSIDERED IN DiD (Based on SSG-2)

Event and Definition	Frequency Range
Deviation – an event *expected during the calendar year* resulting in insignificant allowable change in plant parameters requiring adjustment by normal operation system	**Mean frequency:** $1 < F$ *Note: Deviations to be dealt with at Level 1 of DiD*
Anticipated Operational Occurrences (AOO) - an event *expected over the lifetime of the plant* resulting in a substantial change in plant parameters due to malfunction or failures of normal operation system or external grid failures requiring operation of control systems to prevent reactor scram and/or engineered safety features actuation	**Mean frequency:** $10^{-2} < F < 1$ *Note: AOOs to be dealt with at Level 2 of DiD*
Design Basis Accident (DBA) – an *infrequent event* leading to reactor scram, for which engineered safety features are provided by the design to prevent core damage (CD)	**Mean frequency:** $10^{-4} < F < 10^{-2}$ *Note: DBAs to be dealt with at Level 3 of DiD*
Beyond Design Basis Accident (BDBA)	
1) **BDBA NOT directly leading to CD** - an *unlikely event*, for which protection is not considered explicitly in the design, but which may be mitigated (CD avoided) due to the existing safety margins not credited in the design basis	**Mean frequency:** $10^{-6} < F < 10^{-4}$ *Note:* *- BDBAs not resulting in CD can still be dealt with at Level 3 of DiD* *- BDBAs resulting in CD to be dealt with at Level-4 of DiD*
2) **BDBA directly leading to CD** – a *remote event* representing a severe accident for which it is not demonstrated that CD can be prevented even considering the existing safety margins	**Mean frequency:** $F < 10^{-6}$ *Note: BDBAs directly leading to core damage to be dealt with at Level 4 of DiD*

International Atomic Energy Agency

IAEA PAPER AT PSA-2011

ILLUSTRATION OF DiD IN IAEA SAFETY REPORT #46

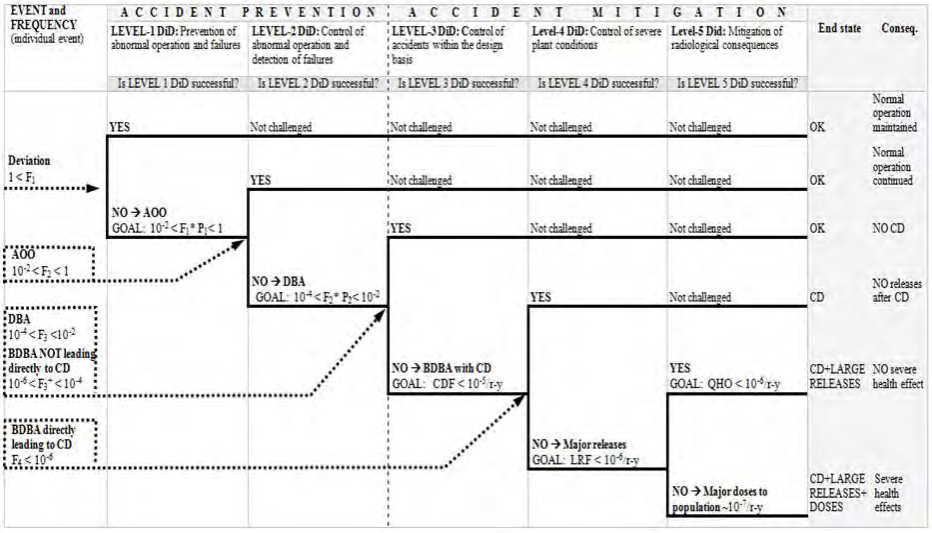


International Atomic Energy Agency

9 of 34

IAEA PAPER AT PSA-2011

CONCEPT OF DiD ILLUSTRATED BY THE EVENT TREE TECHNIQUE



International Atomic Energy Agency

10 of 34

IAEA PAPER AT PSA-2011

DETERMINATION OF REQUIREMENTS FOR RELIABILITY OF PLANT SYSTEMS

- **Determination of requirements for reliability of normal operation, control, and engineered safety features of an NPP require holistic consideration of different levels of DiD in conjunction with deterministic and probabilistic success criteria**
  - ✓ This is especially important in the process of designing new NPPs
- **Example: Level-2 of DiD**
  - Requirements for reliability of control systems
    - ✓ Probability P_2 of failure of the function of control system when AOO (with the frequency F_2) occurs should satisfy:

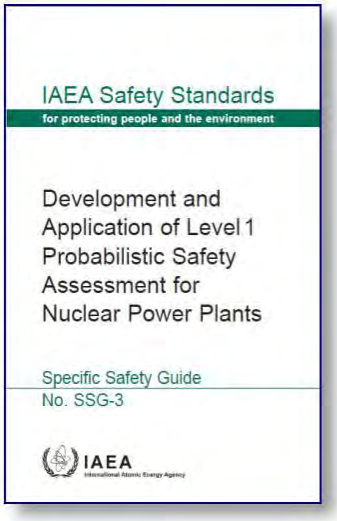
      $10^{-4} < F_2 * P_2(\text{control system fail} \mid \text{AOO}) < 10^{-2}$
    - ✓ Explanation:
      - **If control system fails, the AOO turns into a DBA**
      - **The frequency of DBA should fall in the range of event frequencies F_3 specified for DBAs: $10^{-4} < F_3 < 10^{-2}$**
  - Knowing F_2 for an AOO, the probability of failure of the associated control system and the associated reliability parameters can be specified

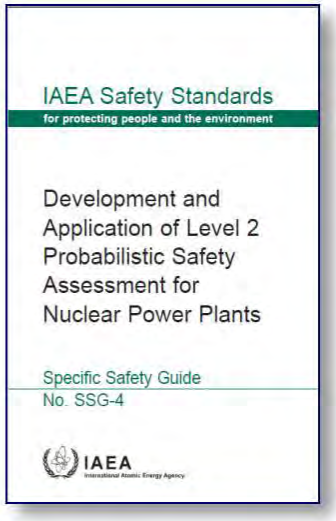
IAEA PAPER AT PSA-2011

REQUIREMENTS FOR PSA QUALITY

- **PSA used in the process of assessing compliance with DiD and determining the requirements for reliability of normal operation and safety systems, should be of sufficient scope and follow current state of the art in PSA technology**
  - **A full scope PSA including all operational modes and events (i.e. internal initiating events caused by component failures and human errors, internal hazards, and external hazards) is usually required**
  - **A quality PSA should comply with contemporary PSA standards - examples are:**
    - ✓ *ASME/ANS PRA Standard*
    - ✓ *Recently issued IAEA Specific Safety Guides on Level-1 and Level-2 PSA and Applications (SSG-3 and SSG-4 issued in 2010)*
- **An independent peer review is utmost important**

IAEA SAFETY GUIDES ON PSA





II. TECHNICAL MEETING ON SAFETY GOALS IN APPLICATION TO NUCLEAR INSTALLATIONS

OBJECTIVE:

To provide an international forum for presentations and discussions on the current practices in the area of establishing and use of safety goals for nuclear installations

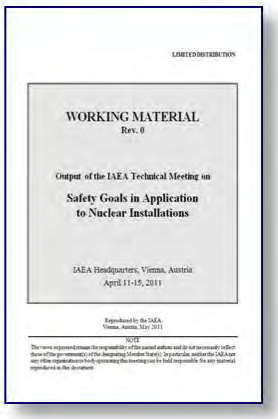
- Need to analyze the experience accumulated, summarize the achievements
- Outline the way forward
- Identify emerging and important issues to be addressed in relation to the topic of Safety Goals for NPPs and other nuclear installations

MEETING SUMMARY

- Some 40 attendees from 20 countries and 4 international organizations
- 30 presentations and papers
- A mix of regulators, operators, designers and consultants, organisations etc.
- Two working groups considering General Framework for Safety Goals and Specification of Safety Goals
- Questionnaire on national framework for Safety Goals with 20 responses
- TM contributed to review of current thinking on safety goals and assisted IAEA in determining what additional work it should sponsor

OUTCOME OF THE TECHNICAL MEETING

- Presentations and papers by the participants
- Summaries of WG discussions
- A formal technical report comprising the background information, papers by participants, collated questionnaires with observations, discussions held, supporting information, and conclusions and recommendations is being finalized


LIMITED DISTRIBUTION

WORKING MATERIAL
Rev. 0

Output of the IAEA Technical Meeting on

Safety Goals in Application to Nuclear Installations

IAEA Headquarters, Vienna, Austria
April 11-15, 2011

Reproduced by the IAEA
Vienna, Austria, May 2011

NOTE

SOME GENERAL CONCLUSIONS

- Safety is not defined by a single attribute
- Integration of Safety Goals is necessary (cf INSAG-25)
- Safety is achieved by a balanced approach to the various hazards and risks that exist on a nuclear installation
- Nuclear Installation Safety is not only achieved by a good design, but requires a sound operational approach
- At all lifecycle stages good leadership and management is essential to maintain safety

SOME AGREEMENTS

- General agreement that Safety Goals should cover all safety issues: normal operation and accidents, workers and the public and all sources of risk
- Safety Goals should be considered in an integrated decision-making process to produce a balanced level of safety
- Consideration of external hazards needs to be dealt with in such a way that internal faults are not masked
- General agreement that high level safety goals should be technology neutral as far as possible
- Recognition that public involvement, as the prime stakeholder, is important.

  This means that the goals need:
  - to be formulated so they were understandable to the public
  - to be clearly related to the more technological goals

HIERARCHY OF SAFETY GOALS

- To develop an approach to safety that can encompass all technologies and that is applicable to all types of installation, Safety Goals need to be founded on a philosophy that consists of a hierarchy
- The hierarchy should start with the technology neutral high level goals (eg IAEA Fundamental Safety Objective), and
  - derive lower-tier goals from higher tier ones;
  - more technology specific goals that are consistent and coherent, can then be determined
- Examples of possible hierarchical structures (eg MDEP) were proposed, but no methodology to derive lower tier goals was proposed
  - This is an area which needs development.

INTERPRETATION OF SEMI-QUANTITATIVE/QUALITATIVE TERMS

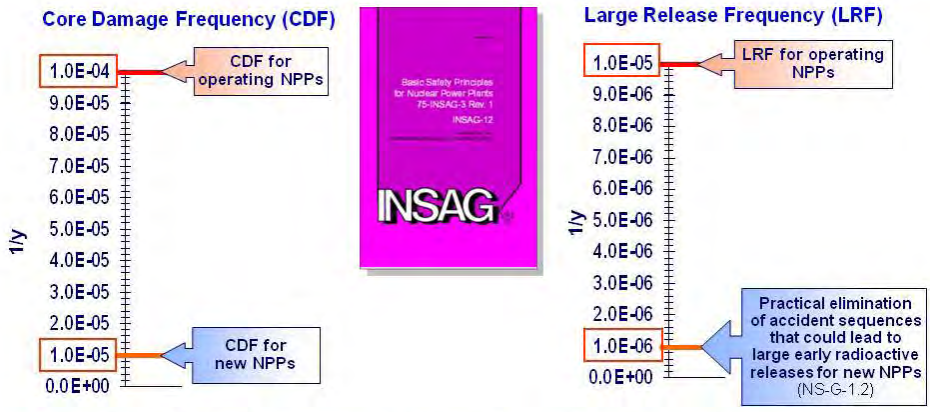
- Overwhelming agreement that clear definitions are needed eg:
  - "safety goals"
  - "practical elimination"
  - "reasonably practicable"
  - "very unlikely"
  - "core" & "damage" as in "core damage"
  - "large" & "early" as in "large early release"
  - etc.

QUALITATIVE/QUANTITATIVE GOALS

More contentious was the qualitative/quantitative balance:

- All agreed that the higher level goals would tend to be qualitative or semi-quantitative: the difficulties IAEA, WENRA and MDEP had encountered in considering quantitative goals were noted
- Most attendees felt that quantitative goals were needed to measure achievement
- Most attendees felt that numerical values should be targets rather than mandatory limits
- It was noted that if goals are used for comparison of different designs/regulatory requirements (or even the same designs operated by different operators) it was important to ensure consistency of the modelling, assumptions, data and depth of review of the analysis

CONCEPT OF NUMERICAL SAFETY GOALS CONSIDERED IN INSAG-12 & NS-G-1.2/ SSG-3



- INSAG-12 does not provide a detailed explicit consideration of qualitative and quantitative goals on health effects (early and latent cancer fatalities) and impact to the environment

NEW/EXISTING FACILITIES

- Much discussion about applying new standards to existing facilities, which reflected concern about operating older reactors whilst arguing future reactors should be safer
- General view was that the safety of facilities should be reviewed periodically with new standards used as the benchmark and improvements should be implemented where possible
- There was no support for allowing facilities to operate without consideration of the need for upgrading safety where this was determined to be reasonably practicable

TECHNICAL ISSUES TO BE ADDRESSED

- Application of Safety Goals to multi-unit sites
- Application to all sources of radioactivity at a facility/site:
  - e.g. spent fuel ponds, waste treatment systems
- How to integrate safety and security requirements
- How to deal in detail with the issue of external natural hazards:
  - if compounded with internal analyses the basic scale and uncertainties involved can mask the potential for improvements to internal fault safety

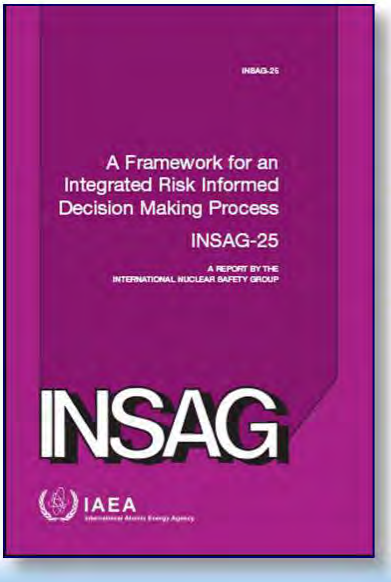
FUTURE IAEA WORK

- Five areas were recommended where IAEA should consider producing guidance:
  - Develop a hierarchical approach for safety goals (such as proposed by MDEP and other organisations) – now is the time to influence future designs using different technologies
  - Clarify interfaces between the Fundamental Safety Objectives, Safety Principles, Safety Requirements and the proposed framework for Safety Goals
  - Develop a methodology to derive lower-tier goals in a consistent and coherent manner
  - Develop guidance on methods and approaches to assess the degree of compliance with the full spectrum of safety goals and a comprehensive review methodology
  - Develop an approach to using safety goals, in a meaningful way, to compare different designs/regulatory requirements and operating philosophies

FUTURE IAEA WORK (Cont.)

- Work on how to communicate with the public is also a possible future area to consider
- It was suggested that IAEA should take account of lessons learnt from the Fukushima event in finalising its work in this area
- The report of the TM is now virtually finalised and should be available in a couple of months: all presentations etc are on an IAEA website

III. GUIDANCE ON RISK INFORMED DECISION MAKING



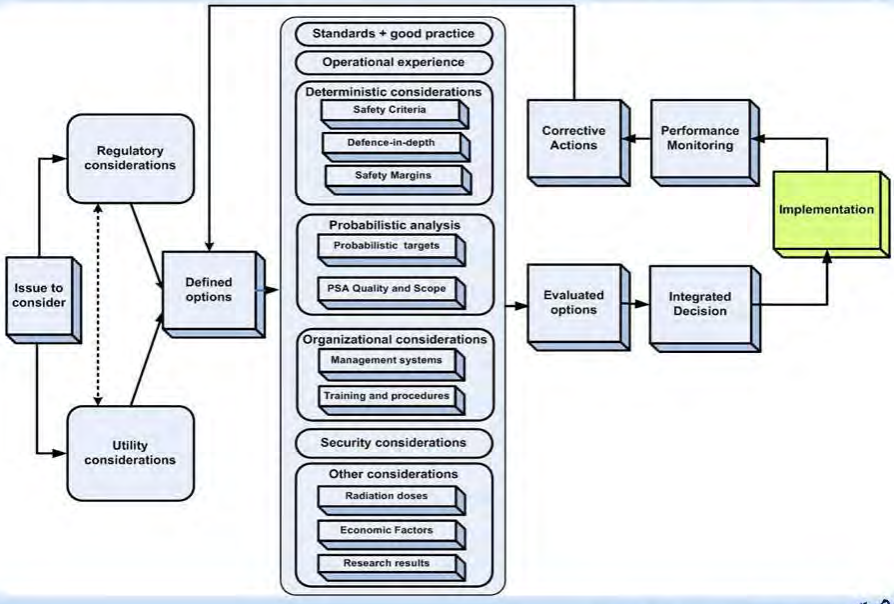
INSAG-25 - OBJECTIVES:

- To identify the framework, principles and key elements for IRIDM
- To describe the interrelationship between the key elements, and the integration of their inputs
- The need for documentation, communication and follow-up on the implementation of the decisions, including performance monitoring and corrective action, is emphasized

International Atomic Energy Agency

27 of 34

INSAG-25: THE BASIC FRAMEWORK AND KEY ELEMENTS OF IRIDM



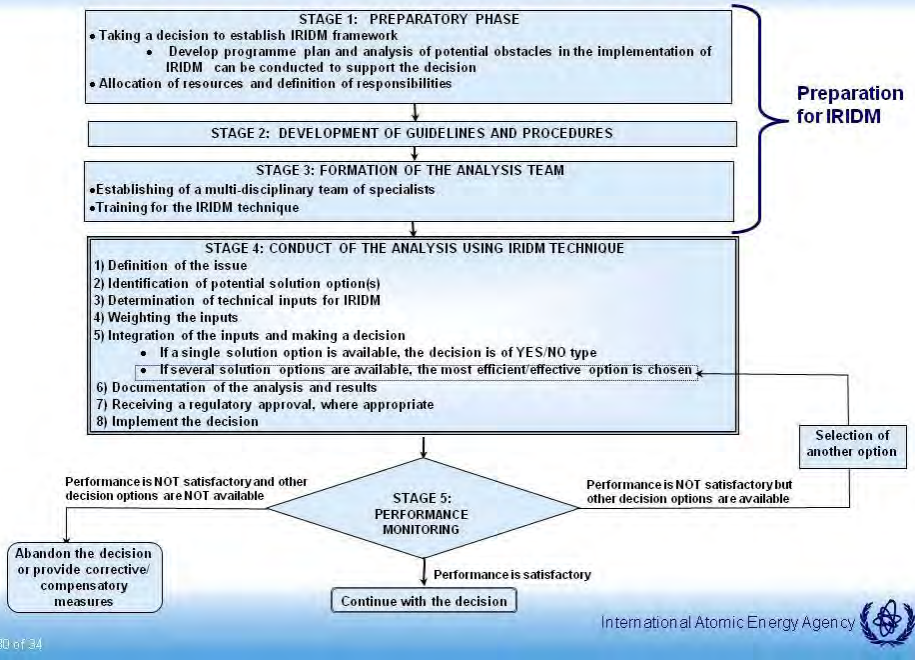
International Atomic Energy Agency

26 of 34

TECDOC ON IRIDM

- **To provide principles and suggest approaches to integrate the results of DSA and PSA as well as other important aspects to make sound, optimum, and safe decisions**
  - Follows main principles listed in INSAG-25 report "A Framework for an Integrated Risk-informed Decision Making Process"
  - Provides detailed information/guidance on the key elements of IRIDM and weighting factors
  - Provides examples illustrating how the decisions can be made or have been made using structured IRIDM process
- **The first CS was held in Oct. 2009, the second in May 2010, and the third in May 2011**
  - Experts from Armenia, Germany, Hungary, Korea Japan, UK, Ukraine, US NRS

TECDOC ON IRIDM: IMPLEMENTATION STAGES



NSNI SAFETY REVIEW SERVICES

Division of Nuclear Installation Safety - NSNI

Operational Safety Section	Safety Assessment Section	Regulatory Activities Section	Research Reactor Safety Section	International Seismic Safety Centre
• Operational Safety Assessment Review Team - OSART • Peer Review of Operational Safety Performance Experience - PROSPER • Incident Reporting System - IRS • Safety Aspects of Long Term Operation of Water Moderated Reactors Peer Review Service - SALTO • Safety Culture Assessment Review Team - SCART	• Integrated Safety Review - ISR ➢ Periodic Safety Review Service - PSR ➢ International Probabilistic Safety Assessment Review Team - IPSART ➢ Review of Accident Management Programmes - RAMP • Generic Reactor Safety Review - GRSR • Safety Assessment Capacity & Competency Review - SAC	• Integrated Regulatory Review Service - IRRS	• Integrated Safety Assessment for Research Reactors – INSARR • Safety Evaluation of Fuel Cycle Facilities During Operation - SEDO	• Site and Seismic Safety Review Services

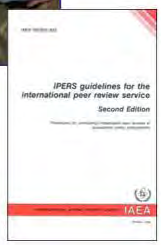
International Atomic Energy Agency

31 of 34

IPSART Service

International Probabilistic Safety Assessment Review Team

- **Peer reviews by teams of carefully selected independent international experts of Probabilistic Safety Assessments studies performed in MSs**

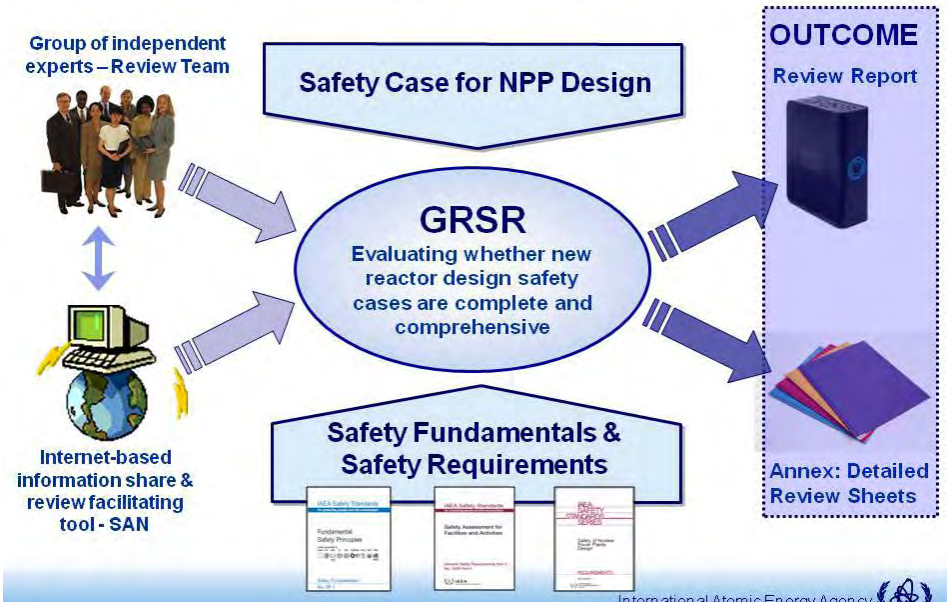


- **Conducted in accordance with the dedicated Guidelines**

International Atomic Energy Agency

32 of 34

IAEA GENERIC REACTOR SAFETY REVIEW SERVICE



International Atomic Energy Agency

33 of 34

SUMMARY

- **IAEA is further pursuing holistic consideration of the DiD concept**
  - A paper was presented at PSA-2011 (March 2011) discussing the use of ET technique to promote a more holistic representation of DiD
- **The issue of developing a new framework for Safety Goals is in focus of current IAEA activities**
  - A Technical Meeting on Safety Goals was held in April 2011 - the outcome will be used as a basis for future activities
- **Development of guidance on IRIDM is in progress**
  - INSAG-25 issued
  - TECDOC on IRIDM is in advanced stage
- **Safety Guides on Level-1 and Level-2 PSA produced in 2010**
- **IAEA Safety Review Services (including PSA review) are a valuable resource for independent peer review of safety assessments for NPPs and other nuclear installations**

International Atomic Energy Agency

34 of 34

ASSURING PSA TECHNICAL ADEQUACY FOR NEW ADVANCED LIGHT WATER REACTOR DESIGNS

Robert J. Lutz, Jr., Westinghouse Electric Company, USA

Heather L. Detar, Westinghouse Electric Company, USA

Raymond E. Schneider, Westinghouse Electric Company, USA

Abstract

The Probabilistic Safety Assessment (PSA) for an Advanced Light Water Reactor (ALWR) must exhibit a high level of technical adequacy, or technical quality, in order to be used as a reliable tool for making risk informed decisions concerning design and eventual operation of the plant. During the design phase, decisions on some design features may use the PSA as an input. Also, the PSA may be used as input to other operational decisions during plant design and construction including the development of procedures, development of technical specification limiting conditions for operation and scheduling of preventive maintenance activities.

For the existing fleet of light water reactors (LWRs), PSA technical adequacy can be judged from wide ranging acceptance criteria such as the PRA Standard in the United States of America that was developed jointly by the American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS). However, the requirements for PRA technical adequacy in this PRA Standard assumes that the plant is built and has operation experience. Some of the requirements cannot be met for ALWRs in the design or construction phase and with no operational history. Key elements of a high level of technical adequacy include procedures, operator interviews, plant walkdowns and equipment reliability histories.

The ability to include these key elements into the ALWR PSA to improve technical adequacy will progress as the ALWR progresses from the design stage through the construction stage and finally to the fuel load / pre-operational stage. As the technical adequacy becomes more robust, more confidence can be placed on risk-informed decisions that are made with the PSA.

To assist in using the PSA as input to design and operational decisions in the design and construction stages of an ALWR, an addition to the ASME/ANS PRA Standard is being developed. The intent of this addition to the Standard is to provide alternative methods of addressing the requirements in the PRA Standard. This addition to the PRA Standard will provide a method of addressing PSA Technical adequacy for pre-operational ALWR plants and permit risk-informed decisions on design and operation to be made with high confidence.

Keywords: PSA, PRA, ALWR, Technical Adequacy

1. Introduction

The Probabilistic Safety Assessment (PSA) is a tool used to assess the integrated safety of nuclear power stations by identifying risk important systems structures and components as well as potential vulnerabilities. It is also an excellent tool for assessing defense in depth for low probability events. In the USA, the PSA has also become part of the fabric of plant design and operation. It is used in daily decision making regarding the alignment of systems and scheduling test and preventive maintenance to minimize potential challenges to plant safety should an upset condition occur. The PSA is also used to modify the plant design and licensing basis, such as risk-informed technical specification changes and equipment additions to support operational flexibility. To support this aggressive use of the PSA, it is imperative that the technical adequacy of the PSA is at a very high level.

For the existing fleet of light water reactors (LWRs), the technical adequacy of the PSA can be judged from wide ranging acceptance criteria such as the PRA Standard (ASME, 2009) in the United States of America that was developed jointly by the American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS). The Standard contains hundreds of detailed requirements called Supporting Requirements (SRs) that specify the minimum set of considerations in the development of the PSA. The SRs detail what should be included in the PSA as opposed to how to accomplish it. For example, an SR requirement is "For each modeled initiating event, IDENTIFY the key safety functions that are necessary to reach a safe, stable state and prevent core damage." However, it does not specific how to identify the safety functions.

Each SR may have varying levels of considerations that correspond to the minimum requirements for the various applications that the PSA my support. For example, conservative analyses and generic assessments may be acceptable for PSA uses that only involve risk ranking applications, but plant specific assessments would be required for use of the PSA to support plant design and operational changes.

The PRA Standard was developed for the existing fleet of plants based on experience in developing PSA studies and assumes that the plant has been built and operating for many years. The PRA Standard assumes that the plant is physically built, procedures are well developed and a significant body of previous operating experience is available to identify important elements of the PSA.

2. ALWR PSA challenges

The NRC's 10 CFR Part 52 regulations, as further developed in Regulatory Guide 1.206, require that a PRA be developed to support the review of the Standard Plant Design Certification and to support initial operation of the plant. When this Standard is applied to the PRA for the advanced light water reactors currently being licensed and soon to be constructed, there are a number of requirements in the Standard that cannot be fully met due to the stage of plant development. Plant walkdowns to confirm modeling details, interviews with plant personnel on system operating experience (a.k.a. system health) and incorporation of operating experience are just a few of the Supporting Requirements (SRs) that cannot be met for a plant that is still in the design stages. However, as the plant design and construction progresses toward initial operation, some of these SRs can be met (e.g., plant walkdowns). Therefore the Standard needs to address alternative means if possible to address the SRs for plants still in the design stage and as it progresses toward operation.

For the purposes of applying this Standard to ALWRs, it is proposed that four distinct stages be considered. The concept of stages is needed because the PRA should mature along with the design. Reviews or assessments of PRA adequacy should be conducted at certain stages to ensure that the PRA meets specific requirements that are commensurate with the design maturity. This will help ensure that the technical adequacy for risk informed applications developed before plant operation are properly dispositioned. It is only necessary to consider the four stages in the context of risk-informed applications that are initially developed using the PRA in any of the four stages and maintaining the validity of those applications as the design progresses. That is, if there are no risk-informed applications prepared based on the PRA at one of the four stages, then the stage becomes irrelevant for the purposes of technical adequacy of the PRA to support the application. The four stages are:

- Design Certification Stage (incorporation of insights) – In this stage, there is no construction started, procedures may be in a very rudimentary stage of development, there are no designated plant personnel, and there is no operating history. Procedures are meant to include:
    - Accident response procedures that define operator actions for the various accident scenarios identified in the PSA,

- Test and maintenance procedures that define pre-initiator operator errors that can impact equipment availability for an initiating event,
- Procedures that can be used to define equipment unavailability for test and maintenance.

An assessment (either self assessment or peer review) against the PRA Standard should be conducted at this stage to support technical adequacy for identifying design and operational insights. Some SRs must therefore be addressed by alternate means if possible.

- Construction Stage (development of risk-informed programs) – In this stage, construction has only started. Procedures have likely been developed but not validated, a plant operational staff has been identified and is being trained but there is no operating history. An assessment against the PRA Standard should be conducted at this stage to support technical adequacy for developing risk informed applications. The design is more robust at this point, but some SRs must still be addressed by alternate means.

- Pre-Operational Stage (completion of risk-informed programs) – In this stage, construction should be nearly complete, procedures have been validated, the plant operational staff has been trained but there is still no operating history. An assessment against the PRA Standard should be conducted at this stage to support technical adequacy for implementing risk informed programs when operation begins. The design and construction should be complete, but some SRs, such as operating history, must still be addressed by alternate means.

- Operational Stage (completion of risk-informed programs) – In this stage, initial plant operation has begun and operating history is beginning to be collected. Based on experience, the initial fuel cycle of operation of a new plant is not typical of later operation as issues are identified and resolved. Only after the completion of the second fuel cycle can operating history begin to be incorporated into the PRA and risk-informed programs. An assessment against the PRA Standard according to the guidance provided in Section 1-6 of the Standard should be conducted at this stage to support technical adequacy for adjusting risk informed programs as necessary after operation begins. From this point forward, no alternate means of addressing the SRs should be necessary.

Some of the requirements cannot be met for ALWRs in the design or construction phase and with no operational history. Key elements of a high level of technical adequacy include procedures, operator interviews, plant walkdowns and equipment reliability histories.

3. Use of PSA for ALWRs

In developing alternative means to address SRs, consideration needs to be given to the decisions that will be made using input from the PSA. There are two distinct regulatory decisions that rely, in part, on the PSA:

- Is the Standard Plant PSA for which a design certification is being sought technically adequate to support incorporation of PSA insights into the proposed design and operation of the plant?
- Is the plant specific PSA technically adequate to support the development of risk-informed applications that will be used to govern initial operation of the plant?

After initial startup of the plant, operating experience will be gained that can be factored into the PRA and used to adjust risk informed programs that govern the long term operation of the plant. Therefore, the technical adequacy of the PSA, as judged by the Supporting Requirements in the PRA Standard, needs to change as the plant progresses from a design stage to the pre-operational stage and finally into the post-operational stage.

During the design phase, decisions on some design features should use the PSA as an input. The adequacy of the design and proposed operation can be assessed by reviewing the PSA for vulnerabilities, defense in depth and the risk significance of key components

During the construction phase, the PSA should be used as input to development of procedures, development of technical specification surveillance intervals and limiting conditions for operation and scheduling of test and preventive maintenance activities. It can also be used for the development of in-service inspection programs that will be initially used when the plant begins operation.

In the pre-operational stage, the risk-informed applications that were developed during earlier stages need to be validated using the updated PSA. Risk important components need to be identified and included in relevant operational programs such as the Maintenance Rule in the U.S. Also, a final search for vulnerabilities should be conducted using the pre-operational PSA.

Once operation has begun, data collection becomes very important so that the PSA can be updated to reflect actual operating history including component reliability and availability and initiating event frequencies.

The ability to include these key elements into the ALWR PSA to improve technical adequacy will progress as the ALWR progresses from the design stage through the construction stage and finally to the fuel load / pre-operational stage. As the technical adequacy becomes more robust, more confidence can be placed on risk-informed decisions that are made with the PSA.

4. A modified PSA standard for ALWRs

Alternative actions for ALWRs to satisfy the RA-Sa-2009 Supporting Requirements that cannot be satisfied for a pre-operational plant could be developed as described below. Rather than describe alternative actions for each individual SR that cannot be satisfied, the alternative actions could be developed for topical areas. For example, alternative actions for any SR that requires a walkdown to confirm equipment placement, spatial effects, etc. are described under the topic of walkdowns. These alternative actions would be applicable at each stage of plant development. The alternative actions are a guide; assessors of the technical adequacy of the PRA at any stage need to consider the state of plant development in determining the appropriate alternative actions.

Only one full peer review of the PRA model, as described in this Standard, should be performed and that could occur at any stage of the PRA model development. After the initial peer review, self assessments may be sufficient at succeeding stages of model development for those changes that can be categorized as model updates as defined in Section 1-6 of the Standard. Focused peer reviews may be required for model upgrades as discussed in Non-Mandatory Appendix 1-A of the Standard. A single peer review of the PRA is considered to be sufficient because the peer review examines the methods used to build and quantify the PRA and updates are permitted without additional peer review. For example, during the design stage of a new plant, spatial effects would be addressed from 3-D models, layout drawings, etc. A peer review at this stage would ensure that all spatial effects are addressed. Subsequently, as the plant construction progresses, the spatial effects identified from the 3-D models and layout drawings would be validated and the PRA model updated to reflect any discrepancies identified. However, this should not be considered an upgrade because the same spatial effects are being assessed – only by different methods as the plant goes from design to finish of construction.

- **Walkdowns** - Confirmation of design features using walkdowns will not be possible until construction is completed for the relevant design features. ALWR Alternative Actions include:
  - Design Certification Stage: USE drawings (e.g., layout and isometric) and/or 3-D digital simulations to CONFIRM design features prior to placement of all equipment.
  - Construction Stage: USE drawings (e.g., layout and isometric) and/or 3-D digital simulations to CONFIRM design features prior to construction and placement of all equipment. Initial cable routings should also be reviewed at this stage to minimize risk of multiple spurious shorts.
  - Pre-Operational Stage: PERFORM walkdowns to confirm design features, component layout and cable routings after placement of all equipment and before fuel load.
  - Post-Operational Stage: SRs satisfied at Pre-Operational Stage; No additional actions required. Periodic review to ensure any design changes are properly implemented consistent with the intent of the initial design. Confirm integrity of seals, penetrations and barriers credited or assumed available in the PRA.

- **Interviews** - Interviews with plant personnel to obtain relevant operating experience will not be possible until plant operation has begun. ALWR Alternative Actions include:
  - Design Certification Stage: USE interviews with system designers and procedure developers.
  - Construction Stage: USE interviews with plant personnel from existing plants who have knowledge of the ALWR design and proposed operation. Review LERs or manuafacturers reports for operating experience on similar key components at other plants
  - Pre-Operational Stage: USE interviews with plant personnel who will be operating the plant. If this is not the first plant, consider experience of similar units.
  - Post-Operational Stage: CONFIRM model assumptions are consistent with operating experience after two cycles of operation are completed.

- **Procedures, Operating Philosophy and Talk-Throughs** - Final plant specific operating, emergency, abnormal, test and maintenance procedures may not be available. Procedure users may not have been trained on the procedure usage. ALWR Alternative Actions include:
  - Design Certification Stage: USE draft procedures supplemented by REVIEW of safety analysis for operator actions.
  - Construction Stage: USE procedures that have been developed at that time, including interviews with operators and simulator trainers.
  - Pre-Operational Stage: USE procedures that have been validated through trial usage, including operator training exercises.

- Post-Operational Stage: CONFIRM model assumptions are consistent with operating experience after two cycles of operation are completed.

- **Generic Data** - Generic data may not be applicable for the ALWR design features. Generic data may not be available if equipment has not previously been used in nuclear plant applications. ALWR Alternative Actions include:

  - Design Certification Stage: EVALUATE the applicability of generic data to the ALWR design, operational features and environment. Where applicable, USE generic data from nuclear applications when possible. USE generic data from other applicable data sources and testing data if available.

  - Construction Stage: EVALUATE the applicability of generic data to the ALWR design, operational features and environment. Where applicable, USE generic data from nuclear applications. Otherwise, USE generic data from other applicable data sources.

  - Pre-Operational Stage: EVALUATE the applicability of generic data to the ALWR design,

  - operational features and environment. Where applicable, USE generic data based on components being used for nuclear applications. Otherwise, USE generic data from other applicable data sources.

  - Post-Operational Stage: SRs satisfied at Pre-Operational Stage; No additional actions required.

- **Similar Plants** - For ALWR PRAs for a reference plant design, there may not be similar plants available for comparison. ALWR Alternative Actions include:

  - Design Certification Stage: EVALUATE the applicability of data and results from existing plants taking into account differences in design, operational features and environment.

  - Construction Stage: EVALUATE the applicability of data and results from existing plants, including sister plants, taking into account differences in design, operational features and environment.

  - Pre-Operational Stage: EVALUATE the applicability of data and results from existing plants, including sister plants, site specific PRAs taking into account differences in site specific factors that impact the PRA.

  - Post-Operational Stage: COMPARE data and results from operating plants taking into account differences in site specific factors that impact the PRA.

- **Plant- Specific Operating Experience and Data** - Plant-specific operating experience and data may not be available. ALWR Alternative Actions include:

  - Design Certification Stage: USE generic data when plant specific data does not exist. ENSURE that data is applicable to the application in the ALWR (environment and functional requirements).

- Construction Stage: INCORPORATE applicable utility operating experience as appropriate to the ALWR.
- Pre-Operational Stage: INCORPORATE applicable utility operating experience as appropriate to the ALWR. USE plant specific operating experience from existing plants, including sister plants.
- Post-Operational Stage: USE plant operating experience from the first two fuel cycles of operation and sister plants. Early operating experience may be screened based on expected future operation.

- **Assumptions and Uncertainty** - For PRAs performed prior to initial plant operation, there are assumptions that are made to develop the PRA because design and operational information are preliminary. There are uncertainties in the details of the as-built and as-operated plants. ALWR Alternative Actions include:
  - Design Certification Stage: USE best available information. IDENTIFY unverified assumptions based on the stage of design. IDENTIFY unique uncertainties related to the stage of the plant design. CHARACTERIZE uncertainty with regard to their use in the PRA model and potential impacts. Pay particular attention to risk significant assumptions.
  - Construction Stage: USE best available information. VALIDATE unverified assumptions as information becomes available.
  - Pre-Operational Stage: USE final design information. VALIDATE unverified assumptions to the extent possible.
  - Post-Operational Stage: USE as-built information. VALIDATE all remaining unverified assumptions.

To assist in using the PSA as input to design and operational decisions in the design and construction stages of an ALWR, an addition to the ASME/ANS PRA Standard is being developed. The intent of this addition to the Standard is to provide alternative methods of addressing the requirements in the PRA Standard. This addition to the PRA Standard will provide a method of addressing PSA Technical adequacy for pre-operational ALWR plants and permit risk-informed decisions on design and operation to be made with high confidence.

5. Conclusions

The use of the PRA for ALWRs must consider the stage of completion of the design and construction of the plant and should include steps to validate the earlier PRA models and assumptions as plant design and construction moves toward operation. The proposed modification to the ASME/ANS PRA Standard is a step in this direction.

6. References

ASME (2009), Addenda to ASME/ANS RA-S–2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sa-2009, American Society of Mechanical Engineers, 2009.

NRC (2007), Combined License Applications for Nuclear Power Plants (LWR Edition), Regulatory Guide 1.206, U.S. Nuclear Regulatory Commission, 2007.

Assuring PSA Technical Adequacy for New Advanced Light Water Reactor Designs

Bob Lutz, Heather Detar and Ray Schneider
Westinghouse Electric Co, LLC

OECD / NEA Workshop on
PSA for New and Advanced Reactors
June 20 – 22, 2011
Paris, France

Westinghouse

1

Background

- Probabilistic Safety Assessment (PSA) is an integral part of the design and regulatory licensing of the new and advanced reactors
- Traditional PSA analyses are done for operating plants where equipment and procedures are well known and an operating history is available.
- For new advanced reactors, this information may not be available, depending on the stage of design, construction and early operation.

Westinghouse

2

The Challenge

- How to assure that the decisions being made that are based on the PSA related to the design and operation of the plant are based on a robust PSA
  - *From a regulatory perspective, consider*
    - Regulatory approvals for the design certification
    - Regulatory approvals for risk informed applications prior to plant operation
    - Regulatory approvals for approval of plant operation
  - *From a designer perspective, consider*
    - Choices between design alternatives
    - Development of test and maintenance schedules and procedures
    - Development of emergency procedures

Westinghouse

3

General Adequacy Basis

- The ASME/ANS PRA Standard, RA-Sa-2009, provides requirements for judging the technical adequacy of the PSA
  - This is used by the U.S. NRC for determining the capability of the PSA to support various risk-informed decisions
  - European regulators may have similar country specific standard or guidance on a country specific basis
- The ASME/ANS PRA Standard is a consensus standard approved by all stakeholders in the US, including the NRC (with limited clarifications and exceptions)
  - It has evolved through several editions based on trial usage at operating plants

Westinghouse

4

Applying the PRA Standard to Advanced Plants

- Some SRs in the PRA Standard cannot be addressed for ALWRs prior to operation
  - **Walkdowns** for consequential damage, fire, flooding, etc.
  - **Interviews** with plant personnel to validate design and operational assumptions
  - **Procedures** to characterize operator actions and error likely situations
  - **Generic Data** to model component reliability and initiating events
  - **Comparison** to similar plants for reasonableness of results
  - **Plant Specific Data** to reflect the actual plant operating philosophy
  - **Assumptions and Uncertainty** to assess the confidence in risk decisions

Westinghouse

5

Progression of the Advanced Plants

- As the plant progresses from a paper design to an operating plant these SRs can be fully addressed
  - Prior to operation, an alternate means of considering the requirements needs to be identified
- There are four distinct stages of plant progression that can be used to identify
  - The degree to which requirements can be met
  - The possible risk informed decisions

Westinghouse

6

Stages of the Advanced Plants

- Design Stage
  - This is the paper plant stage
- Construction Stage
  - This is the stage where actual construction and placement of equipment is taking place
- Pre-Operational Stage
  - This is the complete plant just prior to operation
- Early Operation Stage
  - This is the early operation stage where design issues are being addressed.

Westinghouse

7

Risk-Informed Decisions

- Design Stage
  - PSA is used to assess vulnerabilities and determine whether the basic design represents a high level of safety; later details should not alter these basic decisions
- Construction Stage
  - PSA is used to for equipment procurement, procedure development, technical specification development and initial training of plant personnel; later details should only result in refinements to these activities

Westinghouse

8

Risk-Informed Decisions (2)

- Pre-Operational Stage
  - PSA is used to develop regulatory oversight programs such as reliability assurance, configuration risk management etc. Plant operation should only result in refinements to these programs
- Early Operation Stage
  - PSA is used to validate the design assumptions. Subsequent plant operation will continue to refine the PSA model and risk-informed decisions.

Alternative Methods for PSA Adequacy

- Alternative methods for addressing SRs can be effective in assuring PSA technical adequacy prior to operation
  - **Walkdowns** – Use of drawing and 3-D models
  - **Interviews** – Use designers and procedure writers
  - **Procedures** – Use safety analyses
  - **Generic Data** - Use applicable data from other sources
  - **Comparison** – Use existing plants with engineering judgments
  - **Plant Specific Data** – Use similar plants if applicable
  - **Assumptions and Uncertainty** – Identify and document assumptions and uncertainties
- Validate the PSA as the plant progresses from design to operation

Peer Review and Self Assessments

- Peer reviews and self assessments are an integral part of judging technical adequacy
  - The PSA is a massive effort that cannot be easily verified by independent reviews of the entire model
  - Self Assessments and peer reviews have been shown to be an effective means of identifying systemic deficiencies that could impact risk-informed decisions
    - Experience has shown that they can be successfully performed at the design stage using surrogates for some requirements
  - Using the PRA Standard philosophy, a full peer review might only be required once during the plant development
    - Focused peer reviews and self assessments can be used for PSA model upgrades

Westinghouse

11

Conclusion

- The ALWR PRA Standard currently being developed provides an effective means to assess the technical adequacy of the PSA for risk informed decision-making during plant design, construction and early operation.
  - The ALWR PRA Standard provides a consistent method for judging PSA technical adequacy across the different ALWR designs
- The ALWR PRA Standard is currently in the writing stage
  - Subsequent approvals through established ANS and ASME processes will be required before it can be issued as a Standard

Westinghouse

12

LESSONS LEARNT FROM PSAS FOR NEW AND ADVANCED REACTORS IN RUSSIA

V. Morozov, G. Tokmachev
Atomenergoproekt, Moscow, Russia
morozov@aep.ru

Abstract

The Atomenergoproekt company has been performing probabilistic safety assessments (PSA) for six nuclear power plants (NPP) in design. They belong to different plant generations constructed or planned to construct in Russia, Iran, India, Turkey and Bulgaria including Generation 3+ plants. Now a PSA for a Generation 4 plant is started. The plants have new inherent safety features that are addressed in terms of their influence on PSA development.

The paper is aimed at sharing some issues and experience gained from the PSA development for new and advanced plants.

First of all, Customer requirements to probabilistic safety targets are usually stronger than existing Regulatory or IAEA ones. It appears that industry takes the lead over regulation in this case and forces the designer to find and implement appropriate means to enhance safety, which sometimes have no reference to practical experience. On the other hand, regulatory documents and the existing PSA methodology are mainly oriented to operating plants. This creates problems when developing a PSA as well as performing regulatory reviews.

Secondly, the scope of the PSA may be different depending on a design stage such as the development conceptual, basic or detailed design. In addition, the base case PSA is usually performed for NPP in design. However, a customer may require additional PSA applications to consider, for instance, risk monitoring. In this case the scope of the PSA should be extended to implement special attributes of the application needed that often requires specific information not available at the design stage.

Thirdly, lack of design information affecting PSA development may be associated with incompleteness of the design that is typical for interim design stages and communication problems caused by the involvement of many different companies in the deign activity. To deal with this issue bounding technologies and the iterative PSA development are used. However this sometimes contradicts to the “best estimate” approach recommended by regulatory guides.

Fourthly, the PSA development for advanced NPPs has raised some issues originated from unknown new components, processes and technologies incorporated into the design of an advanced plant. This is a challenge to PSA developers.

The paper addresses some issues resolved while carrying out PSAs for advanced NPPs. They include the reliability estimation for new components, long-term mission time modeling, assessment of defense against common cause failures, software reliability treatment, etc.

Finally, some PSA results for new advanced VVER plants under construction and the first lessons learnt from the Fukushima accident are discussed.

Background

JSC Atomenergoproekt is an engineering company, general designer of nuclear power plants. They belong to different plant generations constructed or planned to construct in Russia, Iran, India, Turkey and Bulgaria including Generation 3+ plants. Now a PSA for a Generation 4 plant is going to be started. The new plants have new inherent safety features that are addressed in terms of their influence on probabilistic safety assessment (PSA) studies which have been performed by Atomenergoproekt since 1988.

One of the new plants under construction is the Kudankulam nuclear power plant (NPP) in India. Its design is developed on the basis of serial power units with VVER-1000/V-320 reactor plants, which have been in operation in Russia and East European countries for many years. The main design features are a unique combination of active and passive safety systems and accommodation to tropical climatic conditions. This design is referred to Generation 3 advanced pressurized water reactors class and complies with international requirements to the nuclear power plants commissioned after the year 2000.

The Kudankulam NPP design developed by Atomenergoproekt has enhanced safety characteristics. The qualitative upgrading of the safety level is attained due to the maximum use of the following passive safety features:

- Eight additional hydraulic accumulators for long-term passive core flooding for 24 hours or longer
- Twelve air cooled heat exchangers for passive decay heat removal for an unlimited time period without operator interference
- New passive fast acting boron injection system to transfer the reactor in a sub-critical state
- Double containment shell of the reactor building with passive filtering of the annulus
- Hydrogen recombiners installed in different compartments inside the containment
- Core melt catcher for catching core debris generated when the core melts and corium penetrates the reactor pressure vessel

The main advantage of the NPP with the new generation reactor compared with Russian designs of previous generations is the use of advanced equipment and introduction of additional passive safety systems in a combination with conventional active systems. Implementation of diversity increases likelihood of safety function fulfillment (see Fig.1).

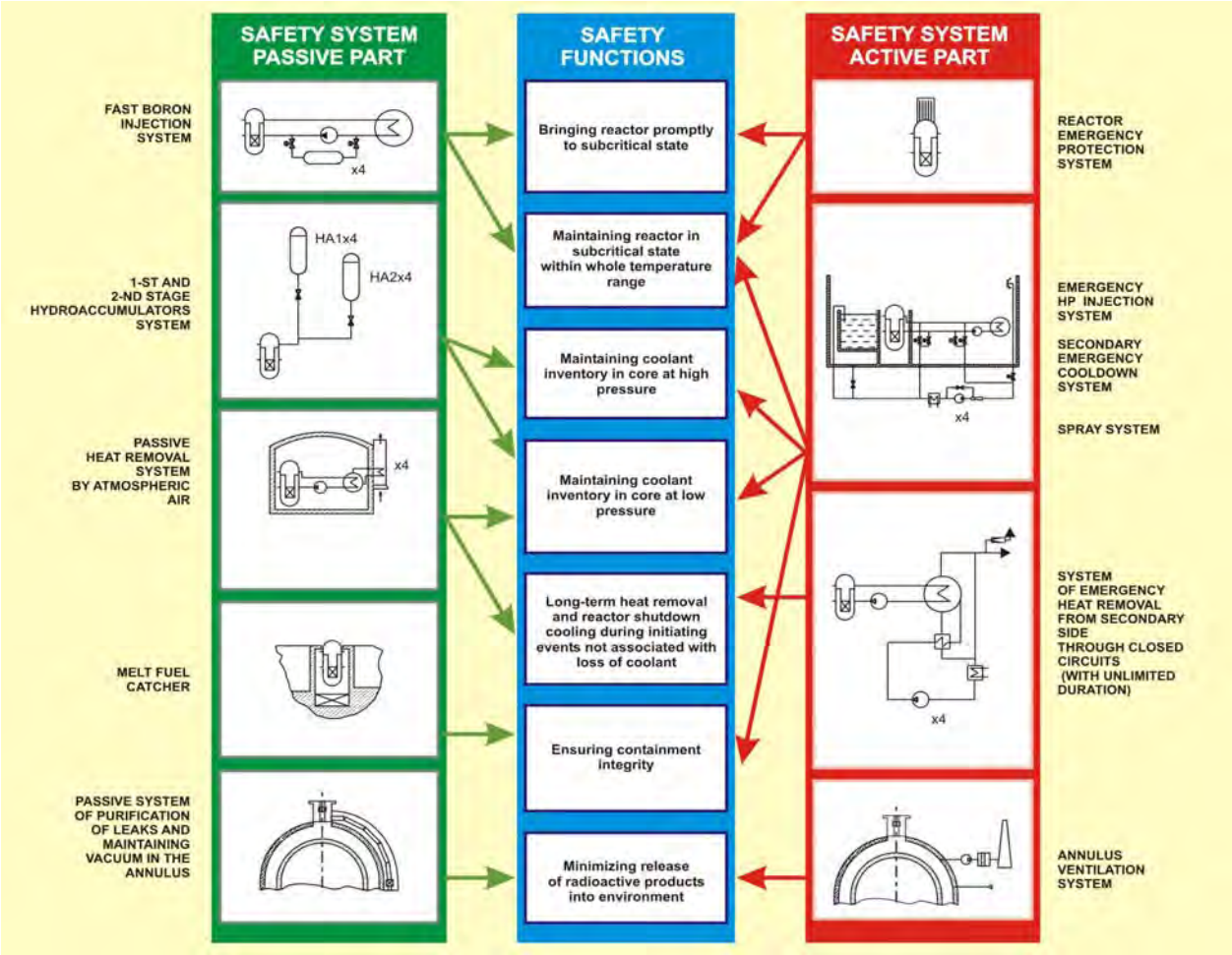


Fig. 1. Diversity in design of new plants

Another new plant under construction is the Novovoronezh NPP-2 in Russia. Atomenergoproekt was selected as the general contractor for both designing and construction of this plant. The Novovoronezh NPP-2 is the prototype nuclear power plant of the new generation AES-2006 design with VVER-1200 reactor type. It is based on the technical solutions of the AES-92 design, which is officially certificated for compliance with the European Utility Requirements (EUR). Unique technologies, used in the AES-2006 design not only increase the service life of the main nuclear power plant equipment up to 60 years, but also enhance safety characteristics and competitiveness on the electric power markets. The main design feature is the compliance with modern and prospective safety requirements. The AES-2006 design is characterized by a broad use of passive and active safety systems, which are similar to those at the Kudankulam plant, as well as low sensitivity to human errors. All these features increase safety level and improve the design performance.

For newer plants specific features have been incorporated into the design to provide protection for severe accidents. These pre-planned severe accident management measures includes:

- providing cooling to the core by any means when it is still in the pressure vessel, e.g. using feed-and-bleed procedure
- using depressurisation of the primary circuit to prevent high pressure melt ejection
- removing hydrogen from containment volume by means of passive recombiners that have the capacity to deal with the rate and volume concentration produced during a severe accident
- adding water to the containment to provide a means of heat removal from the molten core material after it has exited the pressure vessel

The planned development of nuclear energy in Russia in the nearest future is going to be mainly based on the AES-2006 design with either VVER-1200 or VVER-1300 reactor (VVER-TOI). Atomenergoproekt is also the general designer of Seversk, Central and South-Ural NPPs in Russia. All three plants are supposed to be constructed as per the AES-2006 design.

Last but not least the company has started the development of a power plant based on module lead-bismuth fast neutron reactor — SVBR-100. Its design has integral layout of the entire primary circuit equipment in a robust casing covered with protective housing. The advantage of this reactor technology is the modular design which allows creating nuclear power plants of different capacity multiple of 100 MW (e) based on a standardized reactor module which is completely manufactured at machinery works and practically ready-made is delivered to the NPP site.

At the moment the Atomenergoproekt company has been performing PSAs for six NPPs in design. The paper is aimed at sharing some issues and experience gained from the PSA development for new and advanced plants.

Special features of PSA for new plants

Requirements to probabilistic safety targets

Customer requirements to probabilistic safety targets are usually stronger than existing Regulatory or IAEA ones. It appears that industry takes the lead over regulation in this case and forces the designer to find and implement appropriate means to enhance safety, which sometimes have no reference to practical experience. For example, an industry requirement to the core damage frequency estimated for the AES-2006 family plants is defined as 1E-6 per reactor year taking into account contribution from all plant operating states, internal initiating events, internal and external hazards. This is an order of magnitude stronger that the Russian regulatory requirement [1] and INSAG-12 [2] recommendation.
On the other hand, the existing PSA methodology and regulatory documents are mainly oriented to existing operating plants. This creates problems when developing a PSA as well as performing regulatory and IAEA reviews [3]. For example, according to some national standards NPP shall be designed to sustain safe shutdown earthquake with frequency of 1E-4 per year. In the plant design such a seismic level is associated with the most stringent safety requirements, i.e. the target probability levels defined for the plant. The expected frequency of occurrence of the associated seismic scenarios is too high for input to a seismic probabilistic safety assessment because the nuclear power plant has a very low core damage frequency for innovative plants in relation to both seismic and non-seismic initiating events as it was mentioned above.

Another example is that PSA rules and standards say nothing about the scope and methodology of a preliminary PSA when it is carried out at the conceptual or basic design stage given lack of important information (equipment location, cable routing, operating procedures, characteristics of specific site, etc.). Our experience from IAEA IPSART missions to review preliminary PSAs shows that any expert initially provides many comments, especially on internal/external hazard PSAs. Following a discussion the expert is usually faced with the necessity of allocating his requirement among design stages (see next Section).

Scope of PSA

The scope of the PSA may be different depending on a design stage and PSA applications required. The design process can be split into three general phases:

- Conceptual design
- Basic design
- Detailed design

The scope of the PSA depends on what stage of the design the PSA is used for its evaluation. For a new plant, the PSA is usually started during the conceptual design aimed at evaluation whether the level of redundancy and diversity in the safety related systems is adequate. After that, the PSA is

improved at the basic design stage to assess more detailed design issues, including evaluation of protection against internal hazards. Finally, the full-scope PSA is used for design verification against probabilistic safety criteria at the detailed design stage.

At the conceptual design phase the PSA usually addresses the contribution to risk arising from all internal initiating events and possibly all the modes (power, low power and shutdown) of operation of the plant.

During the basic design phase the design of the plant may be not site specific. To verify that the plant design complies with the probabilistic safety targets during the basic design phase, the scope of the PSA includes a Level-1 and Level-2 type analyses for internal events and internal/external hazards which are simplified. The last is optional.

The full scope PSA, including a Level-1 and Level-2 type analyses for all plant operating modes, internal initiators, internal and external hazards, needs to be developed during the detailed design phase to provide a basis for demonstrating compliance with quantitative safety targets [4].

When using a PSA as a support to design, making decision about safety features to be incorporated into the design based on the PSA results is an iterative process to ensure that the insights gained from the PSA are fed back into the design process. The designers, based on research results as well as operational experience and PSA results for reference plants, make initial judgment. After that, any modification being incorporated into the plant layout, system diagrams, descriptions, and operating modes, duration of plant operating states, lists of signals, etc. based on the previous version of the PSA requires producing a new version of the PSA, which, in turn, can provide new findings and insights being used as input for new design modifications. The design process can involve several iterations. Therefore, this should be a much more living PSA than a PSA for operating plants.

Actually, the PSA and design are developed in parallel. When performing the next revision of the PSA the plant design can potentially be modified because of the fact that the PSA is a time consuming task. Therefore, special attention is given to these living features of the plant design being developed and PSA being conducted at the stage of the plant design development.

The base case PSA is usually performed for NPP in design. However, a customer may require additional PSA applications to consider, for instance, risk monitoring. In this case the scope of the PSA is extended to implement special attributes of the application needed that often requires specific information not available at the design stage.

Uncertainty of PSA findings

A specific point that should be addressed for any plant in design is a lack of some design/operating information, especially for a PSA performed during the conceptual or basis design stage. Such a PSA may contain substantial uncertainties.

First of all using operating failure data from reference plants may lead to extra uncertainties for new ones even in the case when components of similar types are used.

The lack of design information affecting PSA development may also be associated with incompleteness of the design development that is typical for interim design stages and communication problems caused by the involvement of many different companies in the deign activity. The extra uncertainties related to the areas of insufficient information may come from incomplete design information, inapplicable data, rough thermal-hydraulic analyses, lack of operating procedures, engineering judgement, etc. It is important to note that the non-quantifiable uncertainties associated with modelling, assumptions and completeness of the study are much higher when performing a PSA for an advanced plant in design than those for operating plants.

To deal with this issue bounding technologies are used. However this approach sometimes contradicts to the “best estimate” one recommended by regulatory guides.

It is also very important to manage the iterative PSA development. The PSA should address the actual or intended design of the plant that should be clearly identified as a starting point for any revision of the PSA.

Within the design process all necessary systematic actions to provide adequate confidence that the PSA documentation will satisfy given requirements for quality are established, included in the procedures, followed by the PSA team, and controlled from independent experts to exclude root causes of possible discrepancies [5]. These actions include:

- *Coordination of deadlines between the PSA team and different groups of designers both within the design company and with subcontractors.* The establishment of an effective project work control process is very important. The overall work plan that addresses all the efforts required for the performance of activities by all the parties involved in the design process, including PSA development, is developed and carried out for the entire design development.
- *Good information exchange between designers, including deterministic analysts, and the PSA team.* Establishing of an electronic archive of valid design documentation is very useful. A good example is an extensive, detailed 3D computer model being developed for the VVER-TOI nuclear power plant. Although the model is developed over several years, using inputs from a number of design participants from a variety of companies, is labour consuming, it is very useful for the PSA, especially for fire and flood analyses.
- *Internal check and approval of the PSA documentation by designers.* It can help to reveal last changes incorporated into the design of the plant, but not considered in the PSA model.
- *Good communication with manufactory experts responsible for equipment reliability evaluation.* Due to lack of operational experience for new plants, the PSA is often forced to involve manufactory data that should be treated carefully. A typical example is the inconsistency between definitions of the boundaries and failure modes used in system and data analyses, in particular for new components if manufacturer data is applied. The PSA component boundaries in the system analysis typically extend beyond the equipment, failure modes, and failure causes specifically defined by manufacturer. For instance, the PSA boundary for a «pump» typically includes the pump mechanical components, motor, circuit breaker, and local control circuits. The manufacturer's data for "pump" failures may include only the mechanical parts of the pump because other vendors are responsible for the other subcomponents.
- *Coordination between PSA analysts performing different PSA subtasks.* Detailed procedures are developed for each PSA subtask with an emphasis on subtask interfaces, especially when incorporating the design changes into the PSA model and documentation.
- *Tracking changes in the PSA documentation in both paper and electronic form correlating with the actual design status, etc.* A special QA procedure is established to assure that the models and data used are good representation of the actual plant design. It is taken into account that a considerable information exchange is conducted in a paperless form.

In order to succeed in developing a PSA of high quality, an iterative approach to performance, modification, consistent PSA tracking, permanent interaction among PSA team members, and effective communication with designers from organizations involved in the design process are carefully established and maintained.

New methodological issues

The PSA development for advanced NPPs has raised some issues originated from unknown new components, processes and technologies incorporated into the design of an advanced plant. This is a challenge to PSA developers.

Mission time

Much longer mission times for components of, at least, three days need to be considered in the PSA for a new plant design in comparison with the usual time of 24 hours. For instance, Russian advanced VVERs [6] have low pressure passive hydroaccumulators, called the second stage, with capability of more than 24hours depending on a size of a primary leak. During this time the active emergency core cooling is unnecessary. Therefore, in this case a 24-hour mission time is inadequate to quantify actual contribution to the core damage frequency from loss-of-coolant-accidents (LOCA). In general, the

calculations for accident sequences should be extended beyond the time point when the reactor has been tripped and other safety systems actuated, until a long term stable state has been reached. On the other hand, a greater mission time can be used for recovery actions and repair usually ignored in the PSA for existing plants [7].

Safe end states

A safe end state is a long term stable state when all the safety functions have been fulfilling such as criticality control, residual heat removal from the reactor facility and the containment, and localization of radioactive products within the boundary envisaged in the plant design, plant parameters are well below the design limits for components and structures.

There is a tendency not to consider end states as safe if parameters are not stable and no heat removal from the reactor fuel is maintained via a closed circuit, i.e. actions have to be taken for replenishment of water sources.

Error probabilities for long-term human actions

Safety philosophy for non-power operating modes of new Russian reactors is based on long-term passive residual heat removal using considerable water inventory. In this case a problem of human error probability estimation within a long time window exists because the current methodologies are limited to smaller time values.

Common cause failures

Methodology adopted in the Atomenergoproekt Company distinguishes weak and strong coupling factors [8]. Depending on that common cause failure models are chosen. There are some aspects we would like to discuss:

- The use of diversity in Russian new designs is an effective defense against necessary s. One of the approaches to minimizing the impact of common causes is to apply diversity in operating modes when some trains are standby and the others are in operation before an accident. That affects common cause failure model parameters.
- The extensive use of digital systems in the design of a new plant poses methodological problems in a PSA since there is less experience in modelling computer based systems. In particular, there seems to be potentially high contribution of common cause failures and software faults (recurrent errors in redundant software modules) [9]. Issues associated with receiving fault data from software developers should also be resolved. The Russian approach is to apply diversity to redundant software based redundant modules. It should be mentioned that the main Russian regulatory document [1] prescribes the fulfillment of a software reliability analysis.
- It is usual practice not to model inter-system common cause failures for existing plants because they are believed to be negligible contributors to core damage frequency, large early release frequency, etc. However, for future reactors involving inherent safety features and demonstrating compliance with reduced safety target values special consideration seems to be given to inter-system common cause failures and common cause failures associated with similarity in active subcomponents (motors, circuit breakers, etc.).

Reliability estimation for new components

New design decision made for new plants are sometimes based on using new unique equipment. This raises an issue of its reliability estimation because operational experience may be inapplicable. In our opinion the design companies should encourage and press on manufactures to assure a good experimental and scientific support to justify reliability values, including passive equipment, e.g., based on fracture mechanics analysis.

Reliability methods being used for the analysis of natural circulation systems

The development of the reliability assessment methodology for passive systems that utilize natural circulation, including evaluation of an uncertainty range of the system performance, is very important.

The existing methods are generally based on Monte-Carlo simulations which require a large number of thermo-hydraulic calculations. As a result, these calculations can be extremely time consuming ones. To avoid this problem, an internationally accepted methodology should be developed.

Interpretation of PSA results for new plants

There are a number of ways that the results of the PSA are used to evaluate the design of a new plant, to identify weaknesses in the design and to assess and rank potential options for improving the design. Generally, these include [10]:

- *Safety metrics/indicators such as safety system reliability, core damage frequency, large early release frequency, etc.* Safety metrics/indicators show whether the overall risk from the plant is low enough to start a license process.
- *Lists of minimal cut-sets.* The integrated list of top minimal cut-sets and lists of minimal cut-sets generated for separate initiating event groups for different plant operating modes are reviewed. Both internal initiators and hazard-induced initiating events are considered. If a single order minimal cut-set representing an independent failure, e.g. a failure of a common support system component, appears in the list of minimal cut-sets provided within the internal event PSA, then, hence, the single failure criterion is not met, and redundancy of the system concerned has to be increased. If a similar finding is found in the internal hazard (e.g., fires and floods) PSA, then separation and segregation of safety related components is insufficient and needs to be improved.
- *Importance functions for basic events, groups of basic events, safety systems, initiating event groups.* High importance of an independent failure event may indicate insufficient redundancy of the system in some plant operating modes and the need for improvement. In this case, either system redundancy needs to be increased or limiting conditions for operation of the system should become tougher for this particular plant operating mode, if possible. High importance of a common cause failure may indicate insufficient diversity applied to some safety function. In this case a considerable change in the design basis might potentially be required. High importance of a human error may indicate a poor man-machine interface. Increasing automation of the plant can be considered as an additional design measure in this case.

These results are used to determine whether the design is balanced or additional measures need to be incorporated to reduce risk.

As an example, the history of the AES-92 conceptual design development in Russia can be considered. The concept of this advanced VVER was developed taking into account findings of PSA studies conducted for operating VVERs, for example, it was found that both failure of residual heat removal systems and common cause failures together with human errors have a relatively high contribution to the core damage frequency. Therefore, special measures using passive and diverse technology for residual heat removal were incorporated into the design of new plants in order to reduce their contribution. After that, results of a new PSA showed that a LOCA contribution became relatively high. That required new measures to be applied like long-term operating hydroaccumulators to reduce the LOCA contribution and create a balanced design. It was an iterative design process. Of course, the concept is supported by a large number of research and experimental studies.

Where the PSA has been used to identify weaknesses in the safety systems that prevent core melt or mitigate severe accidents it can also be used to compare options for improvements to remove the weakness. The options for improvement would depend on the origin of the weakness and the stage in the plant design development when the weakness was identified. Our experience shows that the considerable changes are usually possible at the conceptual design stage and might include:

- making significant improvements to safety systems used at a reference plant – for example, by adding redundant trains, incorporating diversity, etc. An example is the replacement of a tree-train configuration of safety systems typical for existing VVER-1000 plants by a four-train configuration of VVER-1000 plants being constructed now in several countries [6, 11,12];

- incorporating additional safety systems – for example, by adding diverse safety systems to prevent core melt, provide protection for a severe accident, etc. For instance, in the design of the Kudankulam plant the emergency residual heat removal is fulfilled by two diversified long-term redundant systems, one of which operates in a passive mode [11, 13];
- incorporating additional fire protection systems, fire barriers, separation, segregation, fire retardant cables, water lubricating in bearings, etc. As it was shown in paper [13], although the numerical results of the fire PSA at the preliminary design stage are associated with high uncertainties, the fire PSA including fire hazard assessment can provide an extremely cost-effective approach to fire protection improvement. The fire PSA performed in a highly iterative manner was recognized as a valuable tool that can provide insights into plant design and identify important fire-induced dependencies;
- incorporating additional flood barriers of drain facilities;
- replacing key old components with similar components of a more modern design. For instance, it is a well known VVER problem related to containment sump plugging by primary pipe thermal insulation in case of a LOCA. That was eliminated by the block structure of primary thermal insulation and a new design of the containment sump filters in the advanced VVERs [14];
- incorporating additional seismic protection;
- applying pre-planned severe accident management measures; etc.

It is important to note that a comprehensive analysis of any option to be incorporated into the design needs to be carried out involving all the parts of the PSA study. It should be done to avoid missing potential negative aspects of the option considered, for instance:

- an additional train connected to the primary circuit may increase a LOCA frequency;
- an additional water-based fire suppression system needs to be considered as an additional flood source;
- any new fluid system should also be considered as a potential flood source;
- any additional system could be dependent on the same support system as the old one that may neglect benefit of the option proposed;
- any new AC/DC powered system needs to be considered as both additional fire load and potential source of fire-induced dependencies; etc.

The results of the PSA are being used as one of the inputs to a risk informed decision making process with respect to the option to be incorporated into the design. The PSA is used to estimate the reduction in the risk for each of the options identified. This information is used together with the costs of applying the change, the deterministic requirement and other factors in decision making.

Integral PSA results for the Novovoronezh-2 plant (new advanced VVER) under construction are presented in Table1 and discussed below. To bring into adequate comparison the results are given for internal initiating events.

Table 1. Comparison between PSA results for Novovoronezh-2 and VVER-1000/320 operating unit

Core damage frequency, 1/a		**Large early release frequency, 1/a**	
VVER-1000/B-320	Novovoronezh-2	VVER-1000/V-320	Novovoronezh-2
4.5 E-5 [7] 1.5 E-5[8]	6.1E-7[9]	4.0 E-6[10]	1.8 E-8

[7] Balakovo Unit 4, Russia, internal initiating events, power and shutdown operating states

The comparison of PSA results obtained for the last family of operating VVER and advanced VVER in design shows that core damage and large early release frequencies for internal initiating events are approximately two orders of magnitude less at the Novovoronezh-2 NPP. This dramatic reduction in the cumulative frequencies is mainly caused by incorporation of passive systems and diversity principles into the design of the advanced VVER.

It should be noted that the passive systems are also very beneficial in case of internal hazards like fires and floods. These hazards may mainly cause transients, loss of off-site power or blackout. The use of diversity in the design to provide an alternative path of residual heat removal based on a passive mode is a very effective tool to cope with such hazards. That was evaluated when performing PSA for the Kudankulam plant in India. Although the fire PSA was performed in a conservative manner the extremely low value of the core damage frequency obtained shows that passive safety features incorporated into the design of the Kudankulam NPP assure reliable fire resistance of the plant. The overall fire-induced core damage frequency for Kudankulam NPP was quantified to be six times lower than the core damage frequency addressed in the internal event PSA [13].

Lessons learnt from the Fukushima accident in Japan

Following the Fukushima accident in Japan the main attention has to be paid to external hazards especially for the plants having safety features. This work has been done before the accident and is extended after that. For example, the Kudankulam NPP is located on the seacoast. Certainly the Kudankulam plant design was checked against the conditions occurred during the Fukushima accident in Japan when the earthquake had caused major damage to the power grid and the subsequent tsunami flooded the plant, knocking out emergency generators needed to run pumps which cool the reactors. It is demonstrated that the Kudankulam plant is designed to cope with the Fokushima like long-term blackout because the passive decay heat removal system can start in a passive mode in case of blackout and run for an unlimited time period removing residual heat from steam generators to atmosphere.

Our main task now is to elaborate the seismic PSA methodology already applied to analyze the design of new plants constructed in seismic regions like India, Turkey and Bulgaria. For instance, some delayed consequences such as a seismically induced loss of diesel fuel pumps may become important when considering a long-term loss of off-site power.

Other lessons learnt from the Fukushima accident are to direct additional efforts to the following points within the PSA development:

- *Investigation of multi-unit accidents.* Some dependencies such as shared diesels, switchyards, transformers, heat exchangers, etc. are evident and usually analyzed while performing a PSA. Particularly important are subtle interactions that have the potential to result in the simultaneous unavailability of safety systems at adjacent units following a long-term accident. Common cooling water and diesel fuel inventory is of utmost importance. Other important points are manager reliability analysis in case of multiple accidents as well as availability of spare parts and repair staff for several units simultaneously. Allocation of available resources may be a very useful PSA application. For a multi-unit site, the potential spreading of a hazard like seismically induced fire to other units should also be considered in the analysis.
- *Spent fuel pool analysis*. For new designs that provide the features to delay spent fuel damage, consideration of a long-term mission time is necessary. It is clear that following a loss of off-site power spent fuel cooling pumps need to be powered by essential diesel generators even if water inventory is sufficient to remove residual heat for several days by evaporation. Other important items may be resources shared between the spent fuel pool and reactor core or among several units in case of a long-term or/and multi-unit accident.

[8] Temelin NPP, the Czech Republic, internal initiating events, power operation [15]

[9] Internal initiating events, power and shutdown operating states

[10] Temelin NPP, internal initiating events, power operation [15]

- *Analysis of combined internal/external events.* Consequences of the Fukushima accident show that combinations of hazards may be significant for risk. As a matter of fact, a multiple hazards analysis should involve a systematic check of the dependencies between all internal and external hazards. It is evident that combinations of hazards may have a significantly higher impact on plant safety than each individual hazard considered separately. On the other hand, the frequency of combined events may be comparable to that of the individual hazards. Regarding experience from Japan accidents, at least, three types of hazard dependencies can be found. First, a seismic hazard induced another one (tornado). Secondly, a fire (internal hazard) occurred in the turbine section of the Onagawa NPP following the earthquake (external hazard). Thirdly, flooding caused by recovery actions discharging a large amount of water kept safety system pumps disable at the Fukushima plant. The analysis of combined internal/external events is definitely supposed to be extremely time consuming.

References

1. Gosatomnadzor of the Russian Federation. General Rules of Ensuring Nuclear Power Plant Safety. OPB-88/97. PNAE G-01-011-97. Moscow, 1997 (in Russian)

2. International Atomic Energy Agency. Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1 INSAG-12, Vienna, 1999

3. G.V. Tokmachev. Special features of development and review of probabilistic safety assessment carried out for new NPP in design. // Nuclear and Radiation Safety, Moscow, 2010, No.4(58), pages 3-10 (in Russian)

4. Federal Authority of Nuclear Regulation of the Russian Federation. Main recommendations for performing PSAs for NPPs, RB-032-02, Moscow, 2004 (in Russian)

5. G. Tokmachev, A. Lyubarskiy. Lessons Learnt from Review of PSA Studies for VVER-type Reactors. // In: Proceedings of PSAM7-ESREL'04 Conference, 14-18 June 2004, Berlin, Germany, Vol.1, pages 32-38

6. Yu.V. Svyriaev, V.B. Morozov, G.V. Tokmachev, E.V. Baykova, V.R. Chulukhadze, M.V. Fedulov. Use of probabilistic analysis in safety validation of AES-2006 designed for the Novovoronezh nuclear power plant site. // Atomic Energy, Vol. 106, Number 3, pages 155-161, Moscow, 2009

7. V.B. Morozov, G.V. Tokmachev, E.V. Baykova, V.R. Chulukhadze, M.V. Fedulov. Estimation of NPP Probabilistic Safety Characteristics for Long-Term Mission Time. // Izvestiya VUZov. Nuclear Power Engineering. No.2, pages 78-89, Obninsk, 2010

8. V.B. Morozov, G.V. Tokmachev. Approach to Common Cause Failure Modeling in Probabilistic Safety Assessments for New Designs of NPPs with VVER-1000 Reactors. // Izvestiya VUZov. Nuclear Power Engineering. No 4, pages 31-41, Obninsk, 2008

9. G.V. Tokmachev, L.V. Podkolzina, O.I. Lobanok. Estimation of Reliability of Information Computing System with Function of Presenting the Safety Parameters of Balakovo NPP. // Nuclear Measurement & Information Technologies, No 4, pages 52-63, Moscow, 2006

10. G.V. Tokmachev. Approach to the use of the PSA in designing NPPs with VVER reactors of a new generation. // Izvestiya VUZov. Nuclear Power Engineering. Volume 3. Issue 1, pages 44-53, Obninsk, 2007

11. A. Mishra, A. Chauhan. Probabilistic Safety assessment of KK-NPP. // In: Proceedings of International Conference ICRESH05 "Reliability, Safety and Hazard", Ed. P.V.Varde et al, pages 339-345, Mumbai, India, 2005

12. G. Ershov, A. Sobolev. Plant Status and PSA of Tianwan NPP. // International Workshop "SAFETY OF VVER-1000 NUCLEAR POWER PLANTS", 7-12 April 2003, Piestany, Slovakia

13. G. Tokmachev. Fire Probabilistic Safety Assessment for Kudankulam NPP in India. // In: Proceedings of International Conference ICRESH05 “Reliability, Safety and Hazard”, Ed. P.V.Varde et al, pages 375-380, Mumbai, India, 2005

14. V.M. Berkovich, I.I. Kopytov, Y.V. Shvyryaev. Design Solutions on Safety for NPP Units with WWER Reactors of New Generation – Short Description of NPP Power Units with New Generation WWER Reactors. // In: Proceedings of International Conference ICRESH05 “Reliability, Safety and Hazard”, Ed. P.V.Varde et al, pages 403-409, Mumbai, India, 2005

15. L. Kučera. Temelin PSA Level 2. // IAEA Regional Workshop on Harmonization of Level 2 PSAs for VVER Reactors, Sofia, Bulgaria, 20-24 October 2003

Abstract

Atomenergoproekt (AEP) company is the designer for NPP series with VVER reactors (analogue to western PWR plants). They belong to different generations (from old 1-st to newer 3-rd and 3+). AEP has experience in performing probabilistic safety assessments (PSA) for these NPPs at design and construction phases since 1990s

Now AEP is constructing or plan to construct NPPs in Russia, Iran, India, Turkey and Bulgaria

The new plants have safety features that are addressed in terms of their influence on probabilistic safety assessment (PSA)

The paper is aimed at sharing some issues gained from the PSA development for new and advanced plants

Layout sketch of the 1-st generation VVER-440 unit

АТОМЭНЕРГОПРОЕКТ

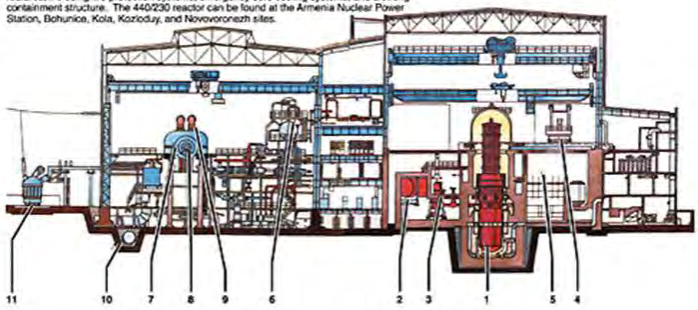
VVER-440 Model 230 Plant Layout

The VVER reactor is a pressurized, light-water cooled and -moderated reactor similar to Western pressurized water reactors (PWRs). There are three predominant models in operation, the VVER-1000 and two versions of the VVER-440.

The VVER-440/230 reactor was the initial civilian model of the Soviet PWR. It is similar to Western PWRs in that it uses low-enriched uranium oxide fuel, placed in thin metal-clad rods, to generate heat. The fuel rods are cooled by pressurized light water. The steam to run the turbine generator is produced when pressurized, heated water from the reactor is pumped through steam generators where it transfers its heat to a separate secondary coolant.

The steam is routed to the turbine generator, which produces about 440 megawatts of electricity. The VVER-440/230, although similar to Western PWRs, lacks a number of safety features, including fire protection systems, emergency core cooling systems, and a strong containment structure. The 440/230 reactor can be found at the Armenia Nuclear Power Station, Bohunice, Kola, Kozloduy, and Novovoronezh sites.

1. Reactor
2. Steam generator
3. Main circulation pump
4. Refueling machine
5. Spent fuel cooling pond
6. Deaerator
7. Steam turbine
8. Generator
9. Steam pipelines
10. Cooling water pipelines
11. Transformer

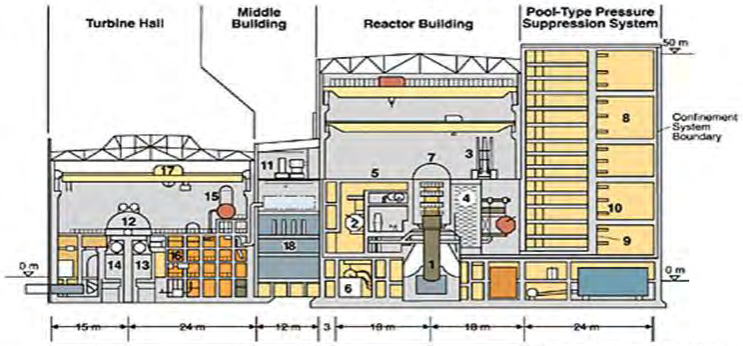


3

Layout sketch of operating VVER-440 unit

АТОМЭНЕРГОПРОЕКТ

VVER-440/213 Plant Layout



1. Reactor pressure vessel
2. Steam generator
3. Refuelling machine
4. Spent fuel pit
5. Confinement system
6. Make-up feedwater system
7. Protective cover
8. Confinement system
9. Sparging system
10. Check valves
11. Intake air unit
12. Turbine
13. Condenser
14. Turbine block
15. Feedwater tank with degasifier
16. Preheater
17. Turbine hall crane
18. Electrical instrumentation and control compartments

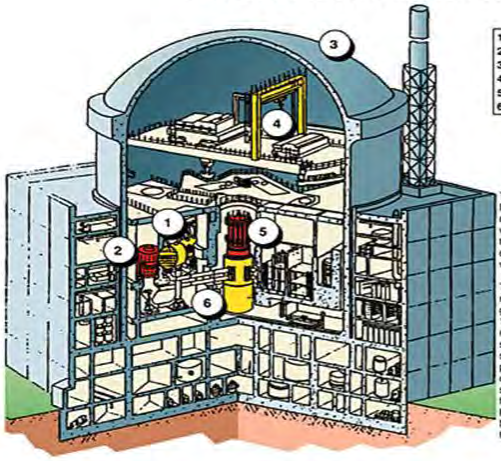
This illustration shows a vertical "cut" through containment with bubble condenser tower.

4

Layout sketch of operating VVER-1000 (V-320) unit

АТОМЭНЕРГОПРОЕКТ

VVER-1000 Plant Layout



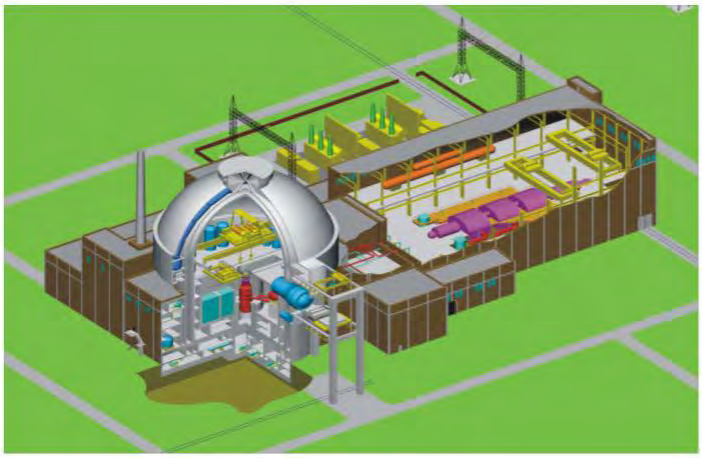
The VVER reactor is a pressurized, light-water-cooled and -moderated reactor similar to Western pressurized water reactors (PWRs). There are three predominant models in operation, the VVER-1000 and two versions of the VVER-440.

The VVER-1000 is the largest and newest of the VVERs. This third-generation design produces about 1000 megawatts of electricity and meets most international safety standards. The VVER-1000 employs safety systems common in Western plants, including emergency core cooling systems and a containment structure. The VVER-1000 can be found at the Balakovo, Kalinin, Khmelnytskyy, Kozloduy, Novovoronezh, Rivne, South Ukraine, and Zaporizhzhya sites.

5

Layout sketch of New VVER-1000 (1200) unit

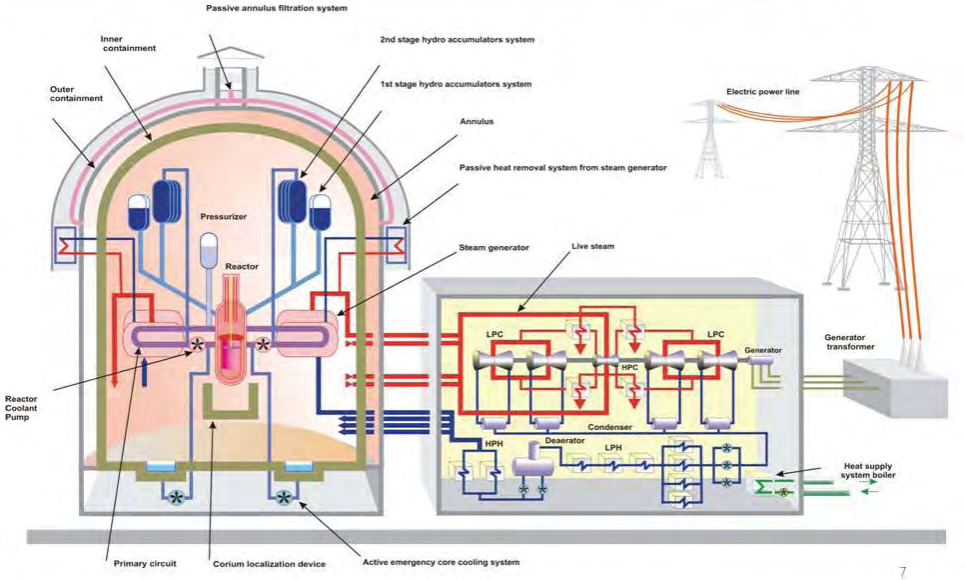
АТОМЭНЕРГОПРОЕКТ



6

Scheme of main systems for new VVER-1000 (AES-92)

АТОМЭНЕРГОПРОЕКТ



7

Passive safety systems implemented in new VVER-1000

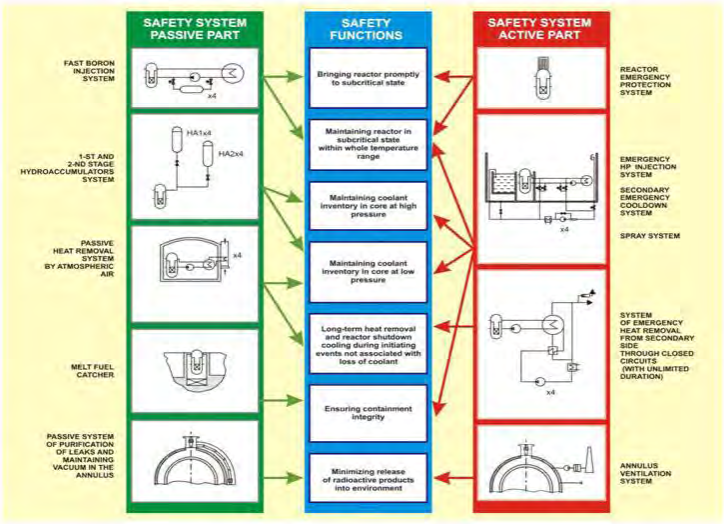
АТОМЭНЕРГОПРОЕКТ

The new VVER-1000 NPP design developed by Atomenergoproekt has enhanced safety characteristics. The qualitative upgrading of the safety level is attained due to the maximum use of the following passive safety features:

- ✓ Eight hydraulic accumulators for long-term passive core flooding for 24 hours or longer (2nd stage hydro-accumulators system)
- ✓ Twelve air cooled heat exchangers for passive decay heat removal
- ✓ New passive fast acting boron injection system to transfer the reactor in a sub-critical state
- ✓ Double concrete containment of the reactor building with passive filtering of the annulus
- ✓ Hydrogen recombiners installed in different compartments inside the containment
- ✓ Core melt catcher

The main advantage of the NPP with the new generation reactor compared with Russian designs of previous generations is the use of additional passive safety systems in a combination with conventional active systems. Implementation of diversity increases likelihood of safety function fulfillment

Diversity in safety functions in new VVER-1000



9

Comparison between PSA results for Novovoronezh-2 and VVER-1000/320 operating unit

Core damage frequency, 1/a		Large early release frequency, 1/a	
VVER-1000/V-320	Novovoronezh-2	VVER-1000/V-320	Novovoronezh-2
4.5 E-5 1.5 E-5	6.1E-7	4.0 E-6	1.8 E-8

[1] Balakovo Unit 4, Russia, internal initiating events, power and shutdown operating states
[2] Temelin NPP, the Czech Republic, internal initiating events, power operation
[3] Internal initiating events, power and shutdown operating states
[4] Temelin NPP, internal initiating events, power operation

10

Special issues of concern related to PSA for new plants

Adequacy/applicability of regulatory approaches

Probabilistic safety targets

Scope of PSA

Uncertainty of PSA findings

Methodological issues

Interpretation of PSA results

Lessons learnt from the recent accidents

11

Adequacy of regulatory approaches

PSAs for NPPs under design and construction phases typically are not stand-alone studies (a part of design process and documentation) and therefore, should accept design data and conditions that are parts of contract terms

PSAs for new designs are iterative because of their nature, however there is no specifications related to their scope and level of detail at different stages (siting, technical design, detail design, equipment mounting and testing)

The regulatory documents are mainly oriented to existing operating plants though this is not declared explicitly and not touch enough these peculiarities of design phase PSA

This creates problems when developing a PSA as well as performing regulatory and IAEA reviews as experts often follows the requirements applicable to final stage only

13

Probabilistic safety targets

Customer requirements to probabilistic safety targets are usually stronger than existing Regulatory or IAEA ones (for example, CDF frequency for the AES-2006 family plants is defined as 1E-6 per reactor year taking into account contribution from all plant operating states, internal initiating events, internal and external hazards).

Customers often takes the lead over regulation, forces the designer to find and implement appropriate means to cope with some pre-conditioned events, which sometimes have no reference to practical experience.

On the contrary, according to many national standards NPPs shall be designed to sustain external hazards with frequency of 1E-4 per year (for example SL2 earthquake). In the plant design such a probability level is associated with the maximum load to structures and equipment (the expected CDF frequency of the associated hazard initiated scenarios is too high to meet mentioned above PSA target).

Therefore, harmonization of requirements in this area is necessary

The scope of PSA

The scope of the PSA may be different depending on a design stage and PSA applications required. The design process can be split into three general phases:

- ✓ Conceptual design
- ✓ Basic design
- ✓ Detailed design

PSA rules and standards say nothing about the scope and methodology of a PSA when it is carried out at the conceptual or basic design stage given lack of important information (equipment location, cable routing, operating procedures, characteristics of specific site, etc.).

During the basic design phase the design of the plant is not site specific. To verify that the plant design complies with the probabilistic safety targets during the basic design phase, the scope of the PSA includes a Level-1 and Level-2 type analyses for internal events and (sometimes) internal/external hazards which are simplified.

Consistency problem

When using a PSA as a support to design, making decision about safety features to be incorporated into the design based on the PSA results is an iterative process.

The designers make initial judgment. After that, any modification being incorporated into the plant layout, system diagrams, descriptions, and operating modes, duration of plant operating states, lists of signals, etc. requires producing a new version of the PSA, which, in turn, can provide new findings and insights being used as input for new design modifications. Therefore, the design process can involve several iterations and should be a much more "living PSA" than a PSA for operating plants.

Actually, the PSA and design are developed in parallel. Therefore, special attention is given to these living features of the plant design being developed and PSA being conducted.

15

Uncertainty of PSA findings

A specific point in design phase is a lack of some design/operating information, especially for the basis design stage. Such a PSA may contain substantial uncertainties.

The lack of design information affecting PSA typically associated with incompleteness of the design and communication problems caused by the involvement of many companies and expert groups in the activity.

The extra uncertainties may come from inapplicable data, rough thermal-hydraulic analyses, lack of operating procedures, etc. The non-quantifiable uncertainties associated with modeling assumptions and completeness of the study are much higher when performing a PSA in design than those for operating plants.

To deal with this issue technologies that apply bounding (conservative approach) can be used. However this sometimes contradicts to the "best estimate" one recommended by regulatory guides.

16

Methodological issues – mission time

Much longer mission times of, at least, three days need to be considered in the PSA for a new plant design in comparison with usual 24 hours.

For instance, Russian advanced VVERs have low pressure passive hydro-accumulators, with capability of more than 24hours depending on a size of a primary leak. During this time the active emergency core cooling is unnecessary. Therefore, in this case a 24-hour mission time is inadequate to quantify actual contribution to the core damage frequency from LOCAs.

In general, the calculations for accident sequences should be extended until a long term stable state has been reached. However, a greater mission time should credit for recovery actions and repair, which usually ignored in the PSA methodology and not used for existing plants.

The necessity of modeling CCF at long mission period is also questionable

.

Methodological issues – safe end states

A safe end state is a long term stable state when all the safety functions are fulfilling without necessity of short-term actions (like changes of component states) within the boundary envisaged in the plant design, plant parameters are well below the design limits for components and structures.

These safety functions are: criticality control, residual heat removal from the reactor facility and the containment, and localization of radioactive products

There is a tendency not to consider end states as safe if parameters are not stable and no heat removal from the reactor fuel is maintained via a closed circuit, i.e. actions have to be taken for replenishment of water sources.

.

Methodological issues – human error probabilities

Safety philosophy for non-power operating modes of new reactors is often based on long-term passive residual heat removal using considerable water inventory.

In this case a problem of human error probability estimation within a long time window exists because the current methodologies are limited to smaller time values.

.

Methodological issues – CCF modeling

Methodology adopted in the Atomenergoproekt Company distinguishes weak and strong coupling factors. Depending on that common cause failure models are chosen. There are some aspects we would like to discuss:

- ✓ The use of diversity in is an effective defense against common cause failures. One of the approaches to minimizing the impact of common causes is to apply diversity in operating modes when some trains are standby and the others are in operation before an accident. That affects common cause failure model parameters
- ✓ The extensive use of digital systems in the design of a new plant poses methodological problems in a PSA since there is less experience in modeling computer based systems. In particular, there seems to be potentially high contribution of common cause failures and software faults (recurrent errors in redundant software modules)
- ✓ It is usual practice not to model inter-system common cause failures for existing plants because they are believed to be negligible contributors to core damage frequency, large early release frequency, etc. However, for future reactors involving inherent safety features and demonstrating compliance with reduced safety target values special consideration seems to be given to inter-system common cause failures and common cause failures associated with similarity in active subcomponents (motors, circuit breakers, etc.).

Methodological issues – using statistical data

Using operating failure data from reference plants may lead to extra uncertainties for new ones even if components of similar types are used. This can be explained by differences in age of equipment at different units, maintenance culture, criteria used for event selection as well as modernization performed.

All these factors result in inhomogeneity when pooling data in a sample. The issue should be correctly addressed in the methodology and practical analyses.

Methodological issues – reliability data for new components

New design decision made for new plants are sometimes based on using new unique equipment. This raises an issue of its reliability estimation because operational experience may be inapplicable.

In our opinion the design companies should encourage and press on manufactures to assure a good experimental and scientific support to justify reliability values, including passive equipment, e.g., based on fracture mechanics analysis.

Methodological issues – analysis of natural circulation systems

The development of the reliability assessment methodology for passive systems that utilize natural circulation, including evaluation of an uncertainty range of the system performance, is very important.

The existing methods are generally based on Monte-Carlo simulations which require a large number of thermohydraulic calculations. As a result, these calculations can be extremely time consuming ones. To avoid this problem, an internationally accepted methodology needs to be developed.

Interpretation of PSA results for new plants (1/2)

There are a number of ways how the results of the PSA are used to evaluate the design of a new plant, to identify weaknesses in the design and to assess and rank potential options for improving the design. Generally, these include:

- ✓ Safety metrics/indicators such as safety system reliability, core damage frequency, large early release frequency, etc.
- ✓ Lists of minimal cut-sets
- ✓ Importance functions for basic events, groups of basic events, safety systems, initiating event groups

PSA at design phase can be used to compare options for improvements to remove the weakness. These options would depend on the origin of the weakness and the design stage when the weakness was identified. Our experience shows that the considerable changes are usually possible at the conceptual design stage and might include:

- ✓ making significant improvements to safety systems used at a reference plant
- ✓ incorporating additional systems
- ✓ incorporating additional fire protection elements
- ✓ incorporating additional flood barriers and drain facilities
- ✓ replacing key old components with similar type of a modern design
- ✓ incorporating additional seismic protection;
- ✓ applying pre-planned severe accident management measures; etc.

Interpretation of PSA results for new plants (2/2)

It is important to note that a comprehensive analysis of any option to be incorporated into the design needs to be carried out involving all the parts of the PSA study. It should be done to avoid missing potential negative aspects of the option considered, for instance:

- ✓ an additional train connected to the primary circuit may increase a LOCA frequency
- ✓ an additional water-based fire suppression system needs to be considered as an additional flood source;
- ✓ any new fluid system should also be considered as a potential flood source;
- ✓ any additional system could be dependent on the same support system as the old one that may neglect benefit of the option proposed;
- ✓ any new AC/DC powered system needs to be considered as both additional fire load and potential source of fire-induced dependencies; etc.

The results of the PSA are being used as one of the inputs to a risk informed decision making process with respect to the option to be incorporated into the design. Therefore, the PSA can be used to estimate the reduction in the risk for each of the options identified.

35

Lessons learnt from the recent accidents (1/7)

A number of events observed last years (one of them – Fukushima accident went to severe phase) showed high importance for PSA adequately represent in the analysis the external and site hazards:

- ✓ Fires (both site specific and external
- ✓ Floods (inside buildings and external
- ✓ Seismic (including secondary effects like tsunami)
- ✓ Hurricanes and tornado
- ✓ Extreme weather conditions, etc.

These events affect on the plant as a whole and may result in collapses of plant equipment and structures and therefore, lead to long-term blackout conditions in combination with partial or complete loss of critical safety functions.

The analysis shows that one of the most probable consequence in this case is loss of essential service water (ultimate hit sink)

Some examples that show the way how these events may act are given in few next slides

Lessons learnt from the recent accidents (2/7)

АТОМЭНЕРГОПРОЕКТ

Liquefaction and foundations and underground communications damage in seismic event

27

Lessons learnt from the recent accidents (3/7)

АТОМЭНЕРГОПРОЕКТ

External flooding (Fort Calhoun NPP)

28

Lessons learnt from the recent accidents (4/7)

АТОМЭНЕРГОПРОЕКТ

Tsunami followed seismic event (Fukushima NPP)

29

Lessons learnt from the recent accidents (5/7)

АТОМЭНЕРГОПРОЕКТ

Volumetric fire at thermal plant

30

Lessons learnt from the recent accidents (6/7)

In new VVERs the main purpose initially was to provide core cooling in black-out conditions based on PSA results for operating VVER plants.

This was resolved by implementation of air PHRS that provides diversity in hit sink and at the same time works in passive mode

After Fukushima accident Kudankulam NPP, which is located on the seacoast and was checked against the conditions occurred during in Japan when the earthquake and subsequent tsunami had caused damage to the power supply systems.

It is demonstrated that the Kudankulam plant will be able to cope with the Fukushima like long-term blackout because the PHRS can start in a passive mode in case of blackout and run for an long time period removing residual heat from steam generators to atmosphere (with account for RCP sealing capacity).

Same conclusion is applicable for many other external hazards and their combinations like extreme weather conditions, draught, tornado, etc.

Lessons learnt from the recent accidents (7/7)

The main task now is to update the PSA methodology as a whole, including seismic PSA already applied to analyze the design of new plants constructed in seismic regions like Armenia, Turkey and Bulgaria. For instance, some delayed consequences such as a seismically induced loss of diesel fuel pumps may become important when considering a long-term loss of off-site power.

This can affect on spent fuel pool cooling when main cooling system is seriously damaged

Therefore, long-term factors need to be carefully addressed in PSA in order to avoid core and spent fuel damage frequency underestimation.

Probably to perform such analysis we need tool that is different from event tree / fault tree models

Other lessons learnt from the Fukushima accident are to direct additional efforts to the following points within the PSA development:

- ✓Investigation of multi-unit accidents
- ✓Analysis of combined internal/external events
- ✓Availability of an extended list of the procedures for severe accident management

Thank you for attention!

RISK-INFORMED, PERFORMANCE-BASED SAFETY-SECURITY INTERFACE

Bruce Mrowca, Information System Laboratories, Inc., United States of America

Farouk Eltawila, Federal Authority for Nuclear Regulation, United Arab Emirates

Abstract

Safety-security interface is a term that is used as part of the commercial nuclear power security framework to promote coordination of the many potentially adverse interactions between plant security and plant safety. Its object is to prevent the compromise of either. It is also used to describe the concept of building security into a plant's design similar to the long standing practices used for safety therefore reducing the complexity of the operational security while maintaining or enhancing overall security. With this in mind, the concept of safety-security interface, when fully implemented, can influence a plant's design, operation and maintenance. It brings the approach use for plant security to one that is similar to that used for safety.

Also, as with safety, the application of risk-informed techniques to fully implement and integrate safety and security is important. Just as designers and operators have applied these techniques to enhance and focus safety, these same techniques can be applied to security to not only enhance and focus the security but also to aid in the implementation of effective techniques to address the safety-security interfaces.

Implementing this safety-security concept early within the design process can prevent or reduce security vulnerabilities through low cost solutions that often become difficult and expensive to retrofit later in the design and/or post construction period. These security considerations address many of the same issues as safety in ensuring that the response of equipment and plant personnel are adequate. That is, both safety and security are focused on reaching safe shutdown and preventing radiological release. However, the initiation of challenges and the progression of actions in response these challenges and even the definitions of safe shutdown can be considerably different.

This paper explores the techniques and limitations that are employed to fully implement a risk-informed, safety-security interface.

Keywords: security, safety-security interface, risk-informed, performance-based

1 Introduction

The term safety-security interface addresses the concept of optimizing the sometimes complementary and sometimes competing objectives of plant safety and security. Ideally this optimization is risk-informed and considered early in the design process, included in the site evaluation, and continued into plant operation.

Design, in its simplest form is a plan used to satisfy a set of requirements. In nuclear power plant design, the regulated portion has long been focused on safety. Specifically, its focus has been on the actions to prevent nuclear and radiation accidents, or to limit their consequences. The classic approach is to identify a set of postulated accidents, typically referred to as design-basis accidents, for which a nuclear facility must be designed and built to withstand. This approach also includes the identification of the minimum requirements for the mitigating response to these design-basis accidents using design rules informed by operating experience, testing and analysis.

A parallel approach, although much more operationally focused, has occurred for security. The plant challenges in this case are referred to as design basis threats and the design focus is on providing physical protection (or physical security) equipment and necessary response forces to protect against acts of radiological sabotage or to prevent the theft of nuclear material.

The interaction between the safety objectives focused on plant system structures and components, and the security objectives focused on physical security has been evolving due to the greater application of risk-informed techniques for both safety and security, and due to the complexity and the resulting cost of providing a safe and secured plant in a world where there is an increasing understanding of the complexity of these challenges and of the potential severity of the consequences if these challenges are not successfully mitigated.

2 Probabilistic versus deterministic

The classic design approach discussed above is often referred to as deterministic and the risk-informed approach as probabilistic. Although these two approaches appear distinctive, the real difference is the degree of emphasis and formality in which the frequency and consequences of the accident progression is considered. Consider the following table which compares key attributes used in both methods.

Attribute	Deterministic	Probabilistic
Event Selection	Limited and bounding set typically determined by expert judgment	Large set determined by failure modes and effects and operating experience
Scope of Prevention Systems	Safety-grade systems	All systems
Operator Response	Limited credit based on deterministic rules	Probabilistically determined through human reliability analysis
Number of failures	Worst-case single failure assumed	Includes multiple failures including common cause failures
Accident Duration	Analyzed until the limiting parameter(s) is demonstrated successful	Typically 24 hours

Attribute	Deterministic	Probabilistic
End Condition	Demonstrates success based on explicit criteria	Event sequences of interest end in core damage or release
Frequency of End Condition	Not Calculated	Provided in terms of core damage frequency or large early release frequency
Uncertainties	Includes margins	Includes reduced margins. Uses probabilistic distributions – best estimate.
Quality Assurance	Formalized process with well-established guidance	Improving process with several recently issued standards

As can be seen from the above table, the application of risk-informed techniques results in a broadening of events and the broadening of the mitigation alternatives considered. This in of itself increases the likelihood of these two seemingly independent objectives, safety and security, to interact. Risk informing also brings a greater realism to the construction of the sequence of events through the use of event tree and fault tree modeling techniques. Therefore, it more clearly exposes potential interactions that may have been previously unidentified. It also reduces the limitations that may result from what is sometimes a stylized scenario used in deterministic analyses and the use of risk-informed techniques typically result in a larger variety of accident scenarios.

3. Safety-security interface

Both safety and security consider a set of challenges, the associated responses and seek the achievement of a safe-stable endstate (i.e., safe shutdown). Although the initiating challenges for safety and security are very different in both frequency of occurrence and impact on the plant systems, there is considerable overlap with regard to the plant response in that no matter what the challenge is, plant operators and equipment are required in both cases to reach a safe shutdown condition.

Considering the safety-security interactions early in the design process can prevent or reduce security vulnerabilities through low cost solutions that often become difficult and expensive to retrofit later in the design and/or post construction period. As much consideration should be given to security as to safety in the evaluation of the physical site, the layout and access of the facility, the structural capacity of critical components and structures, and the degree of redundancy and physical diversity of these components. Just as redundancy and diversity are used to limit single point failures in response to design basis events, similar techniques should be used in the design process to maximize the effectiveness of the security operational programs.

In addition to the equipment and operator response in mitigating a challenges, physical protection is also concerned with detection and delay of a potential adversary and the security response in order to prevent an adversary from reaching their objectives, often referred to as targets. A plant's physical protection program typically includes features such as access control and the associated physical barriers and sensors to enable the identification and mitigation of an attacked.

As a result, safety and security have both complementary and competing elements. Both safety and security benefit from a robust design that has redundancy, diversity and margin. For these complementary elements, coordination between the programs is needed to ensure that design decisions optimize the benefits of both programs. For example, the present of redundant storage tanks which perform a critical function may be a good safety decision but a good safety/security decision would be to ensure that these redundant tanks are protected with adequate barriers (i.e., location, structural capacity, controlled access, etc.) such that the security challenges are also effectively mitigated.

The security objectives to control access and to delay intruders can sometimes compete with operational needs which are often more focused on maximizing the operator's timely action in response to a plant challenge. A balance needs to be achieved such that the adverse impacts of these competing objectives are minimized.

The following table summarizes some of the key security attributes that require coordination between safety and security.

Attribute	Type	Design Objective	Interface
Stand-off Distance from Public Access	Site	Security – adequate to ensure necessary security response prior to adversary engaging targets	Large stand-off distances may limit or eliminate sites that otherwise have excellent safety and environmental characteristics including seismicity, climatology, hydrology, population density, and external hazards.
Defensible Terrain	Site	Security – geography does not present unacceptable security challenge	Terrain that is highly defensible with respect to its topography and configuration of nearby roads, railroads and waterways will need to be balanced with desired safety and environmental characteristics.
Hardened Structures	Design	Security – critical structures defensible against design bases threat	Complementary – structures hardened for external hazards such as seismic and high winds will also aid in achieving defensible structures that meet security objectives.
Equipment Placement	Design	Security – maximize delay to reach equipment	Equipment placement both internal to buildings and within the site could compete with operational and safety objectives that may benefit from other design consideration (e.g., short piping and cable runs, and centralized access).
Separation of Redundant Functions	Design	Security – limits single point failures	Complementary – separation will typically benefit both safety and security as safety also requires separation for external hazards such as fire and flooding.
Building Access	Design	Security – restricts access to ensure locations are monitored, controlled and defensible	Security controls may delay operator access to remote or local control points.
Secured Pathways	Design	Security – ensures expected operator pathways are protected	Security controls may delay operator access to remote or local control points.

Attribute	Type	Design Objective	Interface
Choke Points	Design	Security – ensures adversary pathways are limited	Security controls may delay operator access to remote or local control points.
Defensive Positions	Design	Security – ensures adversary pathways are defended with hardened positions	Security controls may delay operator access to remote or local control points.
Plant Modes	Operations	Operations – changing plant modes is necessary for maintenance and refueling Security – security response may require adjustments to reflect plant configuration	Requires additional coordination to ensure that proposed changes do not unacceptably degrade the safety or security response.
Maintenance of Safety Equipment	Operations	Safety - required to maintain reliability of safety function. Unavailability typically limited by technical specifications Security - Most safety equipment is required to support achieving high assurance of the security function. Some maintenance activities may require changes to the security response.	Complementary – Although maintenance is required in order to meet the safety and security objectives, careful coordination is required to ensure that maintenance activities do not unacceptably degrade the safety or security response.
Maintenance of Security Equipment	Operations	Security - required to maintain reliability of physical protection function. Unavailability typically limited by technical specifications	May compete with other production and/or safety objectives by restricting some activities (e.g., additional access delays) due to the presence of compensatory actions.

For each attribute listed above where security and safety may compete, the designer, operator and regulator will need to determine the optimal solution. The challenge is how to achieve optimization between these sometime competing objectives. This is where performance-based, risk-informed techniques become important.

4. Risk-informed

Risk-informing security and safety regulations is the process of determining what can go wrong, how likely is it and what are the consequences.

A fundamental issue in risk-informing security is the difficulty in determining a frequency of the adversary challenge (i.e., the initiating event frequency) in order to answer the question of how likely is it, or more specifically, how likely is a specific type of security challenge. This frequency determination is a typical element of performing probabilistic safety assessments, but is not common in security assessments as this determination is fraught with uncertainty, sensitive information and is

extremely dynamic. The lack of an initiating event frequency and the resulting lack of scenario frequencies limits the direct comparison of safety events with security events. Without this formality, such comparisons and the resulting optimization can only be performed subjectively. This limitation can be easily solved through the use of standard threat frequencies which could be promulgated by the appropriate national authority. These frequencies may not necessarily reflect the actually likelihood of a particular security event but could reflect the degree of importance placed by the national authority on protecting against a threat. Its determination becomes more a policy decision informed by the threat environment than an intelligence analysis.

An alternate approach is to assume an initiating event frequency of one and to compare the conditional core damage frequency of security-related events to that of the safety risk. Although such an approach avoids the direct determination of attack frequencies, it still requires some characterization of this frequency in order to select the type of safety sequences that are to be used in the comparison. That is, there are low frequency high consequence events and high frequency low consequence events. Which ones do you compare against? One needs to select the type of event that will be compared to and inherent in this selection is a judgment as to the attack frequency. Therefore, whether this frequency is directly or indirectly determined, it is necessary if safety and security risks are to be compared.

Other aspects of a security risk analysis could be developed by augmenting the probabilistic safety analysis with security-related features addressing response/adversary pathway analysis and adversary interdiction analysis. Risk-informed techniques can be used to support the identification of adversary targets and the overall performance assessment of a security plan. These techniques can identify the set of target elements which may be of interest to the adversary in a similar fashion to the techniques used to identify cutsets where the building blocks know as target elements, would be similar to basic events, the building block of cutsets, and the grouping of target elements resulting in failure of the top event, target sets, would be similar to cutsets. The tools and techniques used for the development of a plant's PSA could be leverage to construct a sabotage model which could be used to identify the combination of events that may prevent safe shutdown and that may be of interest to an adversary.

Risk assessment techniques can also be used to assess the ability of the proposed protective measures to meet the security objectives. That is, probabilities can be determined for each protective measure (e.g., failure to detect, failure to respond given detection, failure to neutralize the adversary given successful response, etc.) and a set of sequences can be developed for each target set for each design basis threat. Included in this assessment should be a timeline analysis associated with the adversary pathway between the point of detection at the facility's parameter to the disruption of all targets within a target set and the security response that is initiated at the same time as the point of detection and continues to the planned interdiction point. This framework assumes that security objectives are characterized in a similar manner to the risk objectives of achieving a core damage frequency and large release frequency target similar to that used on the safety side.

A risk assessment tool that fully integrates the assessment of safety and security would support sensitivity analyses that could assess the security benefit and safety cost, or vise versa, in order to achieve true optimization. This tool could also support operational decisions that may require adjustments to a plant's security postured as the result of maintenance or changes in the plant's mode of operation.

5. Performance-based

The performance-based aspect of this framework is in how the effectiveness of the program is assessed in both its development and later during the operational phase of the plant. An effective performance-based program focuses on the overall program effectiveness as opposed to many intermediate prescriptive requirements. It also requires a well-defined performance objective or objectives, the ability to verify these objectives through regulatory oversight, and the ability to take appropriate corrective action prior to unacceptable consequences.

The development of a risk-informed security program provides measurable objectives to support a performance-based framework. The explicit modeling of the many protective measures can be periodically tested in order to determine if the overall security objectives are being maintained.

Testing should include the assessment of both hardware and personnel. Integrated tests that verify detection capability, adversary and response force timelines for key target sets would help to provide regulatory confidence that the in-place protection measures are effective.

6. Conclusion

A well-developed security program should optimize safety and security through the use of an integrated risk-informed framework. Such a framework would fully support a performance-based oversight process, and would enable changes and any emergent deficiencies to be assessed and characterized. Although the technical methods to develop such a framework are available and similar to that used on the safety side, the formality of performing this type assessment requires careful planning and execution. However, the application of these techniques not only enhance and focus the implementation and maintenance of the necessary security measures but also aid in the implementation of effective techniques to address the safety-security interfaces.

AUTOMATIC FAULT TREE GENERATION IN THE EPR PSA PROJECT

Nathalie VILLATTE (1), Philippe NONCLERCQ (1), Sandrine TAUPY (2)

(1) EDF, R&D Division, Industrial Risks Management Department

F-92140 Clamart, France
nathalie.villatte@edf.fr

(2) EDF, CNEN

173 Avenue Pierre Brossolette, 92120 Montrouge, France
sandrine.taupy@edf.fr

Abstract

Tools (KB3 and Atelier EPS) have been developed at EDF to assist the analysts in building fault trees for PSA and importing them into RiskSpectrum® (RiskSpectrum® is the tool used at EDF for PSA).

System modelling is performed using KB3 software with a knowledge base describing generic classes of components with their behaviour and failure modes. Using these classes of components, the analyst can describe (using a graphical system editor): a simplified system diagram from the mechanical system drawings and functional descriptions, the missions of the studied system (in a form of high level fault trees) and its different configurations for the missions. He can also add specific knowledge about the system.

Then, the analyst chooses missions and configurations to specify and launch fault trees generations. From the system description, KB3 produces by backward-chaining on rules, detailed system fault trees.

These fault trees are finally imported into RiskSpectrum® (they are converted by Atelier EPS into a format readable by RiskSpectrum®).

KB3 and Atelier EPS have been used to create the majority of the fault trees for the EDF EPR Probabilistic Safety Analysis conducted from November 2009 to March 2010. 25 systems were modelled, and 127 fault trees were automatically generated in a rather short time by different analysts with the help of these tools.

A feedback shows a lot of advantages to use KB3 and Atelier EPS: homogeneity and consistency between the different generated fault trees, traceability of modelling, control of modelling and last but not least: the automation of detailed fault tree creation relieves the human analyst of this tedious task so that he can focus his attention on more important tasks: modelling the failure of a function.

This industrial application has also helped us gather an interesting feedback from the analysts that should help us improve the handling of the tools. We propose in this paper indeed some improvements that should all the more facilitate the PSA analyst's work.

Key Words: KB3 – PSA – EPR – Fault tree generation

1. Introduction

The tool used to model PSAs in EDF is the Swedish code RiskSpectrum® (© ScandPower). A first version of the EPR Flamanville 3 PSA was built in 2008-2009. Most of the fault trees describing failures of system missions were generated by KB3 (© EDF) (Pillière, 1999) and transferred into the RiskSpectrum® project by Atelier EPS (© EDF). KB3 and Atelier EPS are two tools developed by EDF.

Since mid-90s EDF sees KB3 and Atelier EPS as reference tools for the drawing up of its PSAs (Gallois, 1999).

2. Fault tree generation with KB3

KB3 assists analysts in building reliability models. KB3 is used together with knowledge bases describing generic behaviour and failure modes of components. These knowledge bases are written in a modelling language FIGARO (Bouissou, 1991) developed by EDF.

At EDF, KB3 is used since the mid-1990s to produce fault trees for PSAs. Three knowledge bases are used: one is dedicated to thermal-hydraulic systems, one is dedicated to electrical systems and the last one is dedicated to instrumentation and control. Figure1 illustrates the use of KB3 for EPR PSA Project.

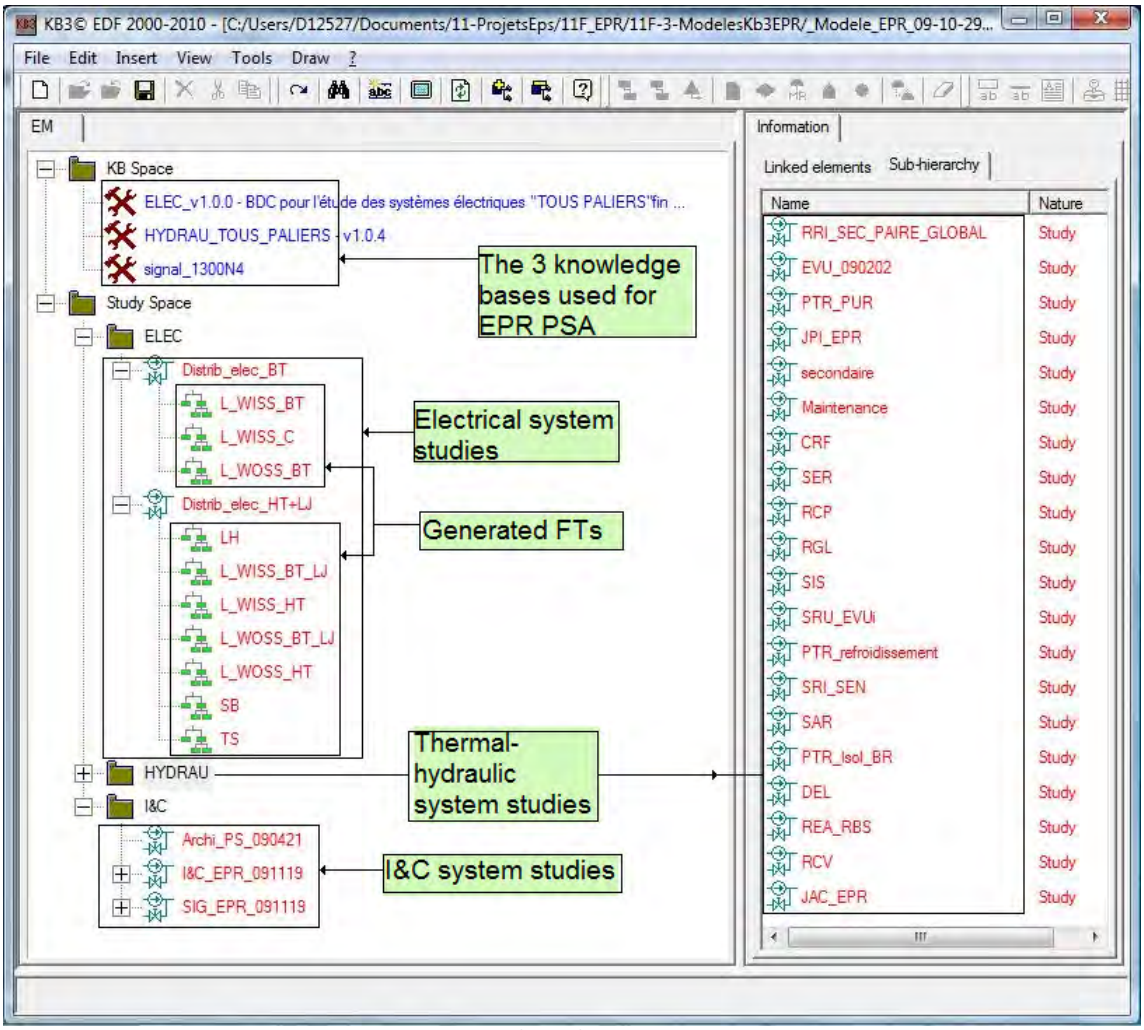


Figure 1. Use of KB3 for EPS PSA Project

2.1 First step: drawing the system diagram

KB3 provides the analyst with a graphical editor linked to a chosen knowledge base so the analyst can choose a component from a list of icons and add it to the diagram of the studied system. The icons correspond to the generic components of the chosen knowledge base. The analyst can draw the diagram on several pages.

Figure2 is an extract of the Safety Injection System diagram for the EPR PSA.

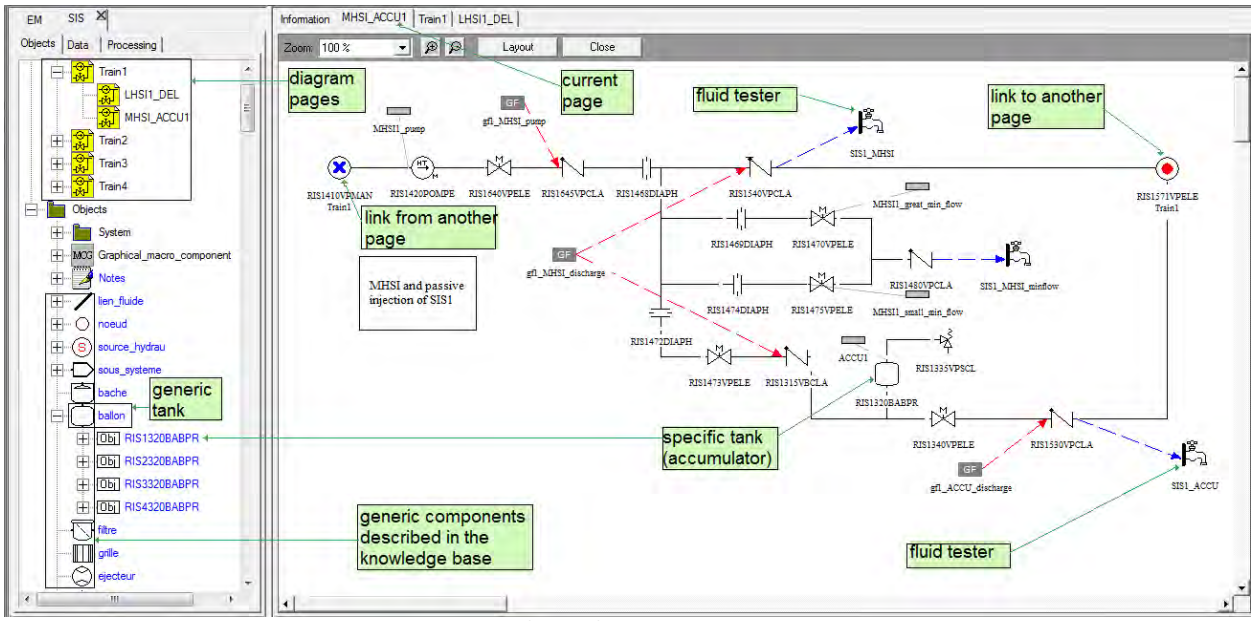


Figure 2. Extract of the Safety Injection System diagram

The analyst creates I&C and supply components. The links between operated components and I&C and power or cooling supplies is done by editing the components and filling their "interfaces" with I&C and supply components. Remark: At this stage of the PSA, I&C has not been related to components.

Figure3 shows power and cooling supplies for the motor-operated pump RIS1420POMPE.

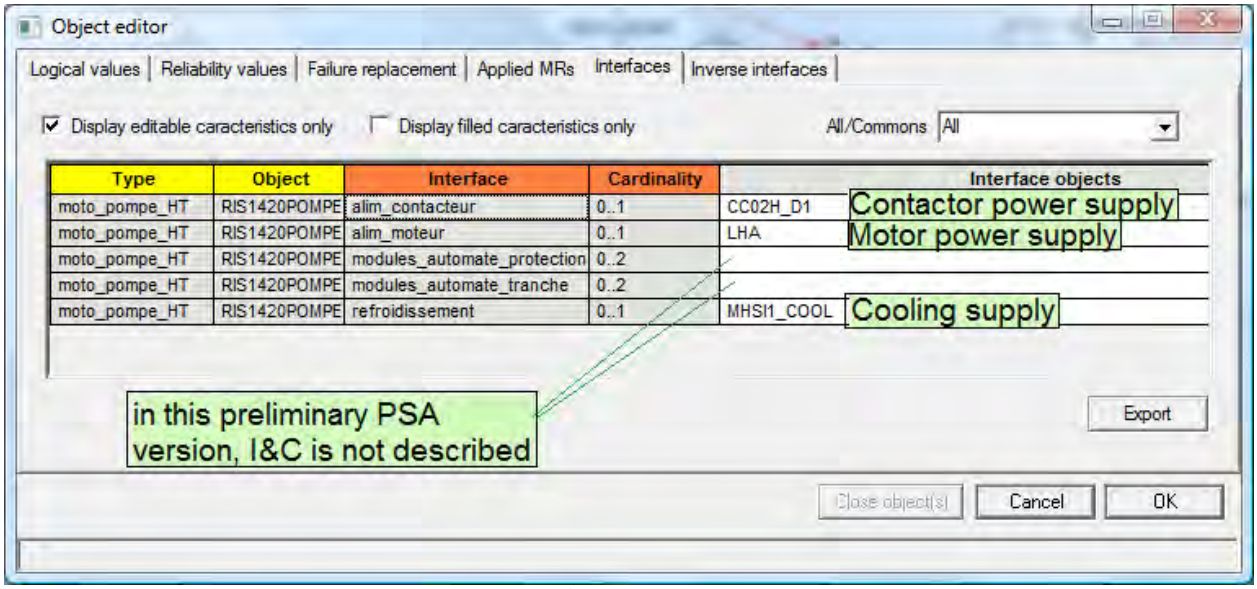


Figure 3. Power and cooling supplies for the motor-operated pump RIS1420POMPE

2.2 Second step: description of mission failures

KB3 provides the analyst with a graphical interface to describe mission failures (undesirable events). These undesirable events will correspond to the top events of the generated fault trees. Usually the analyst connects mission failures to the loss of fluid testers (special tool predefined in the knowledge base).

Figure4 is the description of the top event "**failure** of 2 out of 4 MHSI injections in states A or B" extracted from the Safety Injection System study.

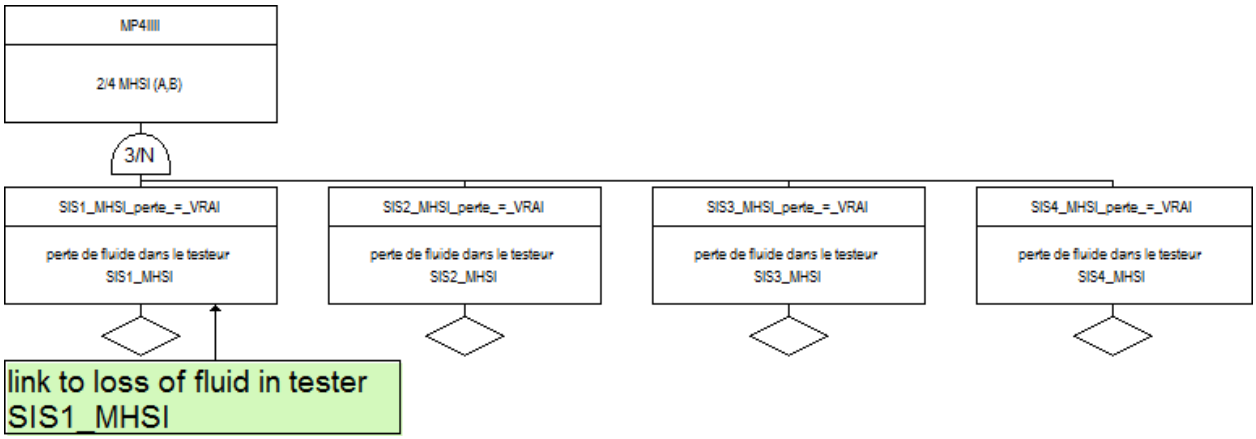


Figure 4. Top event "failure of 2 out of 4 MHSI injections in states A or B"

2.3 Third step: addition of specific knowledge

The analyst can add the description of specific behaviour (not described in the knowledge base) by using the same interface as for the undesirable events description. For example; he can add new failure modes or specific interactions between components.

Figure5 shows two manual rules: the first one indicates that maintenance on MHSI Train1 leads to the loss of RS1420POMPE, the second one indicates that loss of minimal flow leads to the loss of RS1420POMPE.

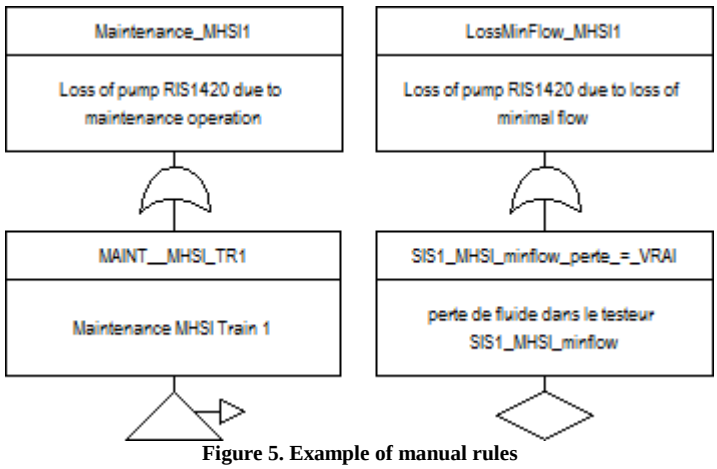


Figure 5. Example of manual rules

2.4 Fourth step: definition of configurations

Characterization of components (initial state, mission state, I&C) may be different depending on the system missions, e.g. a pump already runs or has to start. The analyst can define several configurations by modifying component characteristics. These configurations will be used for fault tree generation. The "PSA" knowledge bases provide a few verification tools. Figure6 shows one mean of verification of the state A-B configuration, by automatic display of flow.

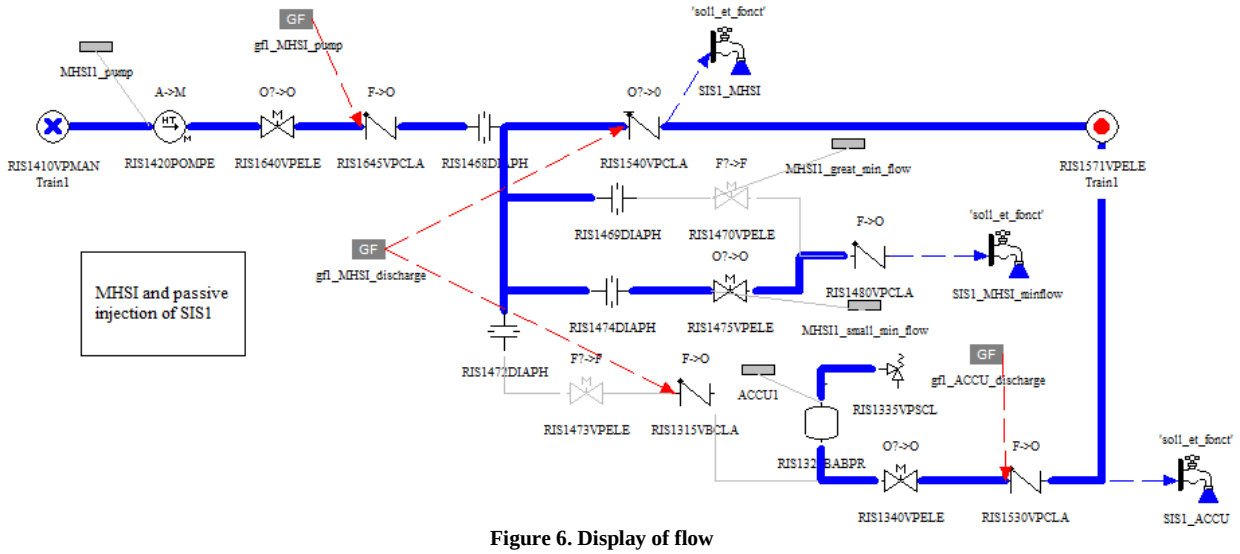


Figure 6. Display of flow

2.5 Fifth step: fault tree generation

The analyst chooses a prefix-name for the RS fault tree pages, the top event(s) to be modelled and the system configuration to be considered, then he launches the fault tree generation. See Figure7.

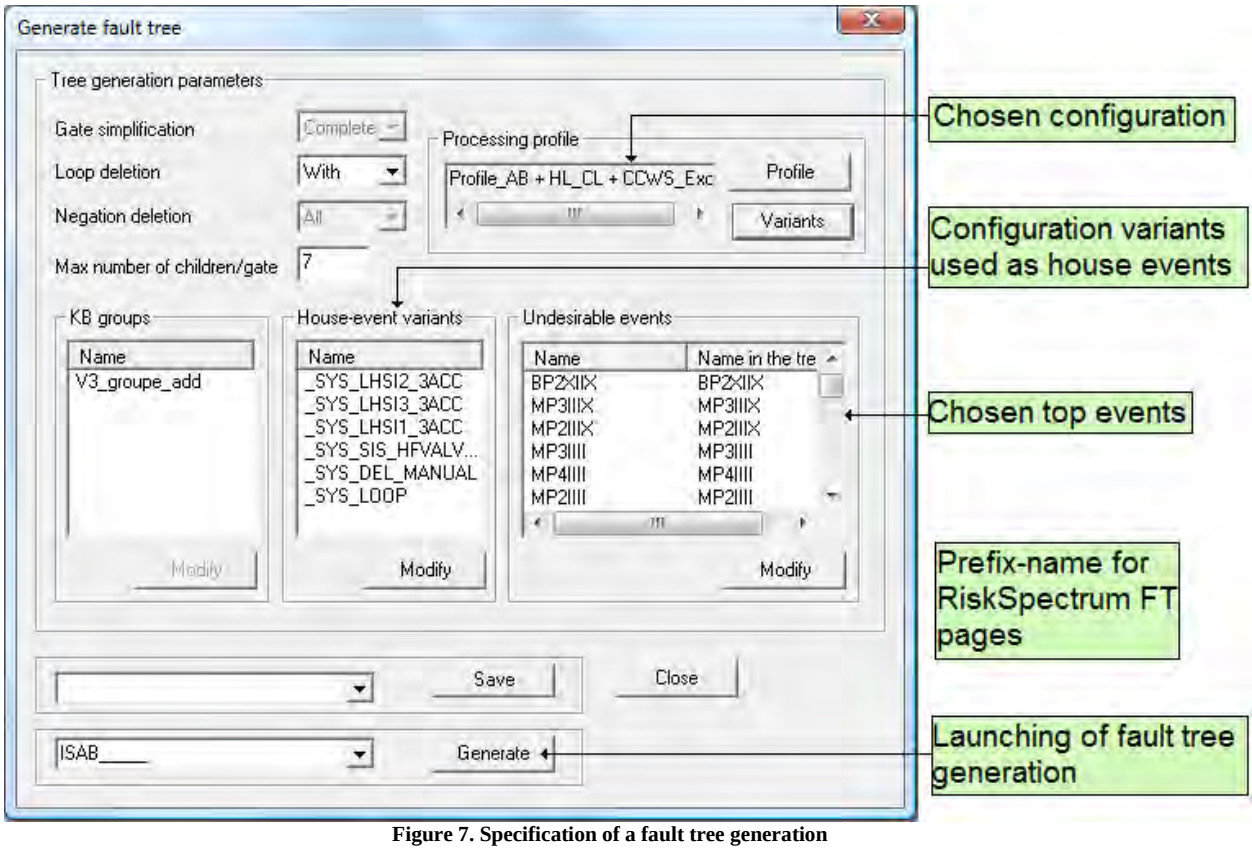


Figure 7. Specification of a fault tree generation

3. Export to a riskspectrum® project

Atelier EPS allows to choose the KB3 fault trees to export and the RiskSpectrum® target project. Below we present some extracts of the RiskSpectrum® project after the export of the KB3 fault tree "ISAB_____".

Figure8 shows the top event MP4IIII. The losses of fluid in testers have been replaced by the losses of fluid in the check valves linked to the testers.

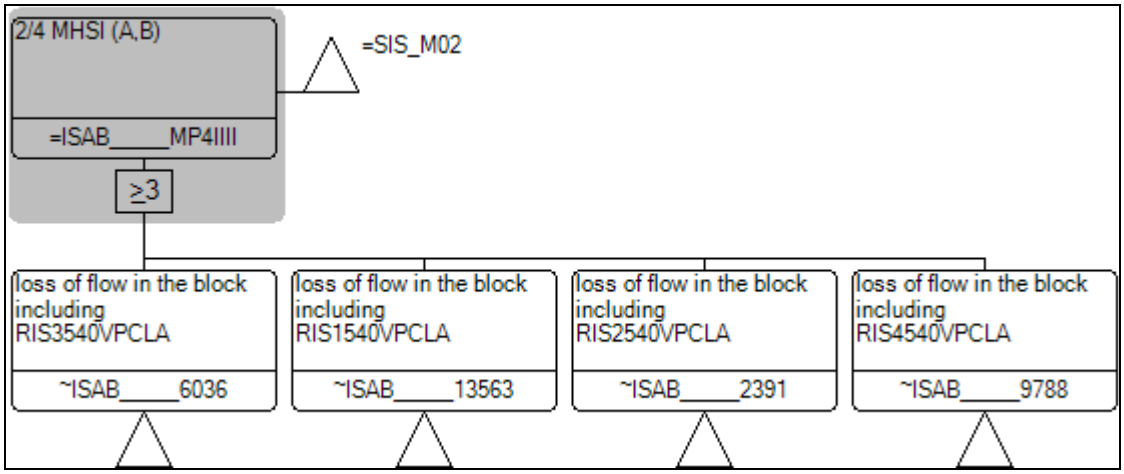


Figure 8. Top event MP4IIII

Figure9 shows the explanation for the loss of fluid in the check valve on Train1. The rules in the knowledge base use the upstream components of the check valve in the system diagram.

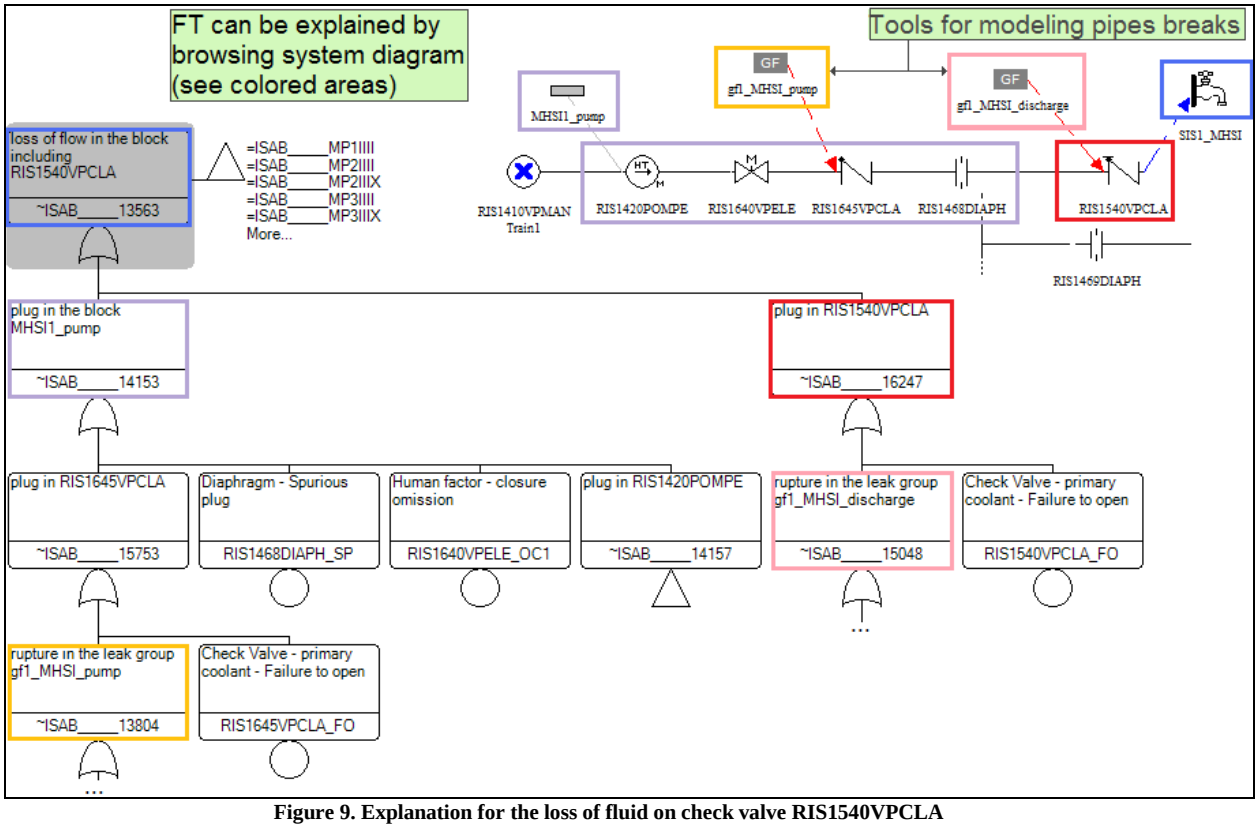


Figure 9. Explanation for the loss of fluid on check valve RIS1540VPCLA

Figure10 shows the explanation for the loss of the MHSI pump on Train1. The rules in the knowledge base use the description of the initial and mission states of the pump in the chosen configuration and the supplies linked to the pump. The added manual rules are also taken into account. Reminder: At this stage of the PSA, I&C was not related to the components.

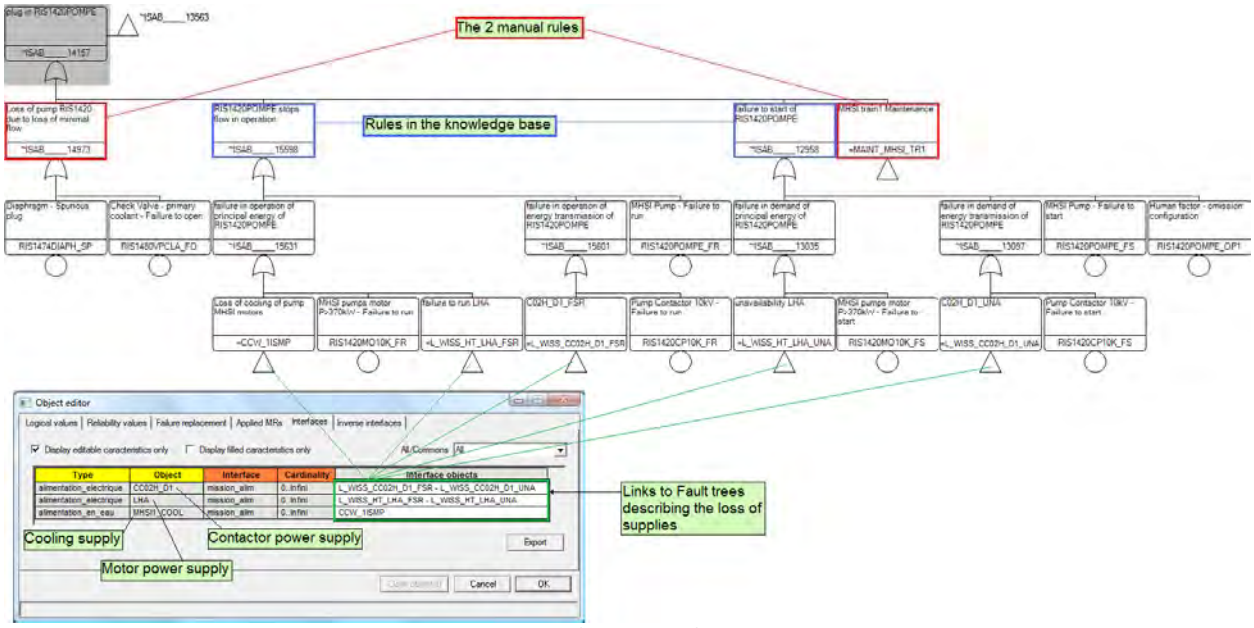


Figure 10. Explanation for the loss of RIS1420POMPE

4. Feedback on using KB3 and atelier EPS for EPR PSA

KB3 and Atelier EPS have been used from November 2009 to March 2010 to create the majority of the fault trees in the PSA Preliminary version developed during FA3 construction. This was the first PSA 4 trains modelled at EDF.

25 system studies were modelled (2 studies for electrical systems, 3 studies for I&C systems, 20 studies for thermal-hydraulic systems) and 127 top events were automatically generated in a rather short time by different analysts with the help of these tools.

4.1 Benefits

Using KB3 and Atelier EPS is particularly interesting for a PSA of a unit at design stage or a first PSA of an existing unit.

Flexibility

It’s very easy to modify the diagrams (adding a component or a train, deleting a component or a train, changing the supplies of components, changing the generic component associated to a component) and regenerate fault trees.

If necessary, the behaviour of generic components can be modified in the knowledge bases, then just reload the new knowledge base and regenerate the fault trees.

Diagrams

It is easier to work on the basis of a diagram than on a fault tree.

Homogeneity

Even if the system studies are performed by analysts with different level of expertise working in different teams, using KB3 and the same knowledge base ensures a good homogeneity between the fault trees. The support systems are systematically modelled.

Traceability and control of modelling

The generated fault trees can be explained with the rules in the knowledge base and the content of the system study. Because knowledge bases and fault tree generator take benefit of a long experience, rather than validate the trees generated by KB3, the analyst validates the description of the system: diagram, configurations, supplies, top events and manual rules.

The final validation of the fault trees is based on minimal cut sets calculated by RiskSpectrum®.

Time saving

Information on the behaviour of most components is described in the knowledge base. The analyst can focus on the specificities of his study. In the design phase of a model, KB3 is efficient and facilitates the construction of fault trees, ensuring overall consistency.

4.2 Improvements to consider

Fault tree readability

Fault trees produced by KB3 for the EPR PSA were sometimes considered not easily "human-readable". Most of the blame on the readability of fault trees could have been avoided if the analysts had used existing functionalities (description fields, translation tools). We will facilitate the access to these functionalities.

Export to RiskSpectrum®

The transfer of KB3 fault trees to RiskSpectrum ® project is a tedious and repetitive task. Moreover, the transfer order may be important. We will facilitate the transfer of many KB3 fault trees to RiskSpectrum® in a **unique** operation with an algorithm deducting an appropriate transfer order.

Handling of the tools

The feedback should help us improve the handling of the tools. For example, we plan to extend report capabilities and to add new functionalities which should facilitate browsing in the studies.

5. Conclusion

KB3 and Atelier EPS have been used for all the PSAs at EDF. They had a strong contribution to the success of PSA Preliminary version developed during FA3 construction.

The feedback should help us improve these tools (including the knowledge bases) that are to be used for the fleet of EPRs that EDF plans to build.

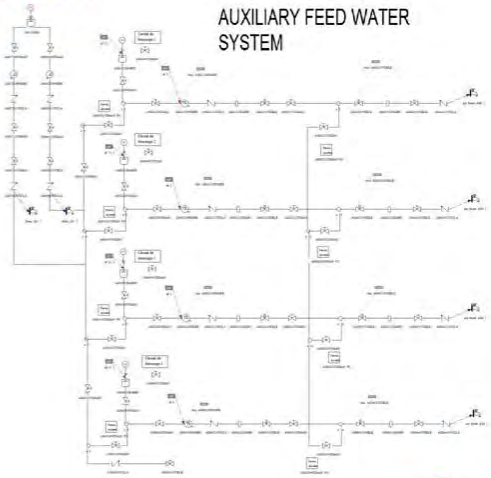
6. References

PILLIERE Mylène, MOUTTAPA Patrick, VILLATTE Nathalie, RENAULT Isabelle (1999). KB3: Computer Program for Automatic Generation of Fault Trees. Proceedings of RAMS'99, Washington, January-99

GALLOIS Marie, PILLIERE Mylène (1999). Benefits expected from automatic studies with KB3 in PSAs at EDF. Proceedings of PSA'99, Washington, August-99

BOUISSOU Marc, VILLATTE Nathalie, BOUHADANA Henri, BANNELIER Marc (1991). Knowledge modelling and reliability processing – Presentation of the FIGARO language and associated tools. Proceedings of SAFECOMP'91, Trondheim, Oktober-91

Automatic fault tree generation in the EPR PSA project



Nathalie VILLATTE
Philippe NONCLERCQ
Sandrine TAUPY

22 June 2011

EDF
CHANGER L'ÉNERGIE ENSEMBLE

Summary

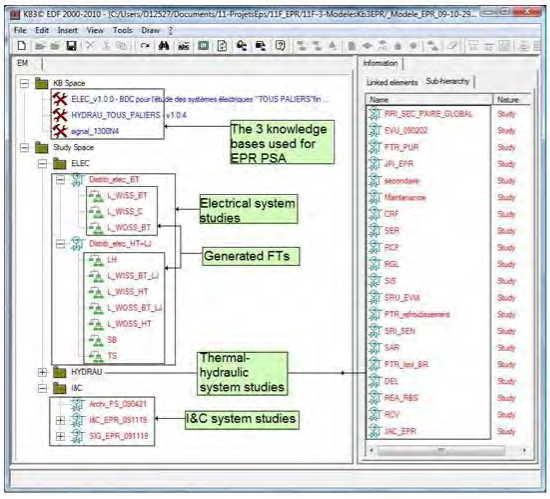
- Use of KB3 in the EPR Flamanville 3 PSA
- Description of the different steps to get KB3 fault trees
- Extracts of fault trees generated by KB3 and imported in a RiskSpectrum ® project
- Benefits seen in the use of KB3
- Ways to improve from the feedback

EDF

Use of KB3 in the EPR Flamanville 3 PSA

- The tool used to model PSAs in EDF is the Swedish code **RiskSpectrum®** (© ScandPower)
- A first version of the EPR Flamanville 3 PSA was built in 2008-2009
- Most of the fault trees describing failures of system missions were generated by **KB3** (© EDF) and transferred into the RiskSpectrum® project by **Atelier EPS** (© EDF)
  - 127 KB3 fault trees
    - More than 1000 top pages (several top events can be modelled in a same KB3 fault tree)
- Why use KB3?
  - Complexity of the systems (4 trains)
  - PSA analysts with different experience levels
  - PSA analysts working in different teams

Systems modelled with KB3 for EPR Flamanville 3 PSA (first version)



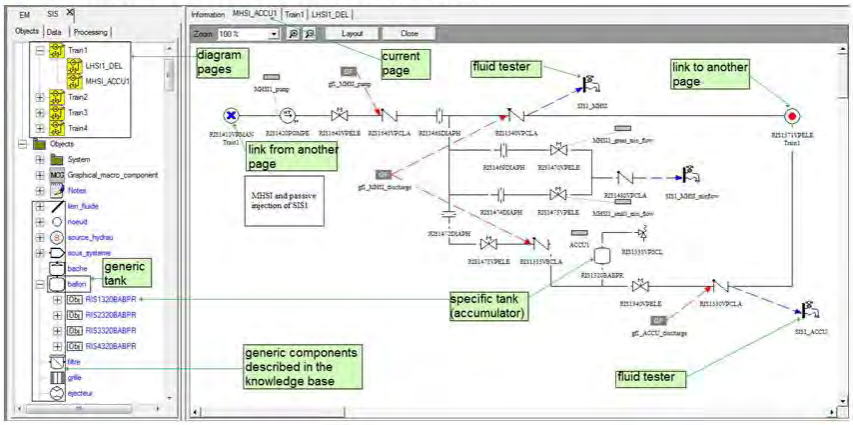
- KB3 is used together with knowledge bases
  - A knowledge base describes generic behaviour and failure modes of components
- 3 knowledge bases
  - Electrical
  - Thermal-hydraulic
  - I&C
- 25 studies
  - 2 electrical
  - 3 I&C
  - 20 thermal-hydraulic
- 127 KB3 Fault trees

The different steps to build a fault tree with KB3

- Create a study and choose the appropriate knowledge base
- First step: draw the system diagram
- Second step: define the I&C and supplies of controlled components
- Third step: define the top events to model
- Fourth step: add specific knowledge if necessary
- Fifth step: define the system configurations (initial state, mission states)
- Sixth step: launch the fault tree generation
- Last step: export to a RiskSpectrum® project

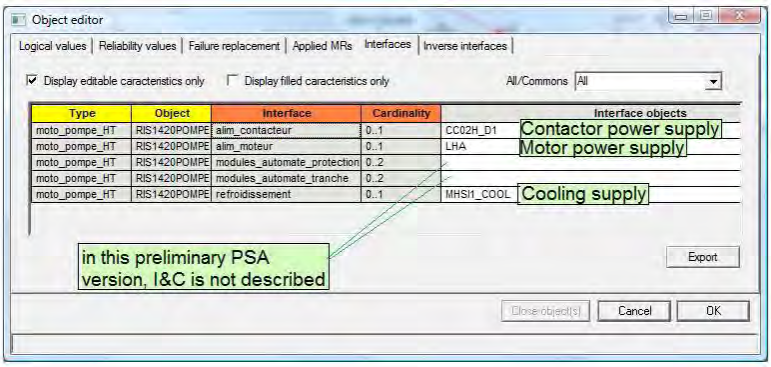
First step: drawing the system diagram

- Drag and drop of generic components on pages, connection of links to nodes
- The system diagram can be represented on several pages
  - A link can connect two nodes located on different pages



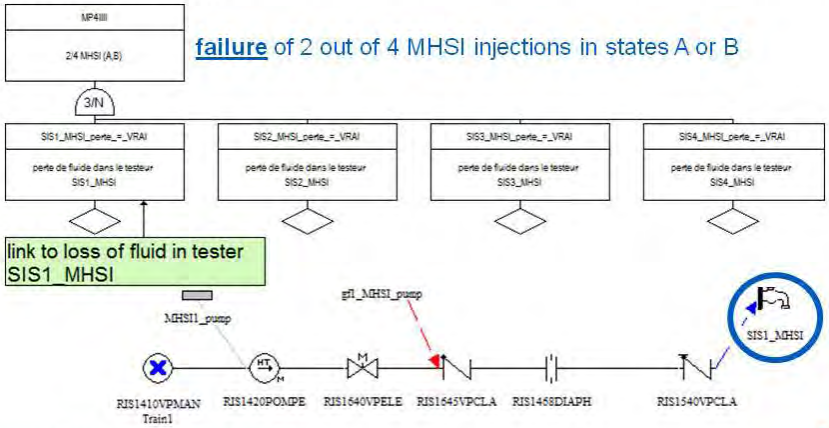
Second step: I&C and supplies

- In each controlled component (motor-driven pump, electric or pneumatic valve), it is possible to indicate the supplies and I&C



Third step: description of mission failures (top events of the generated fault trees)

- Usually the analyst connects top events to the loss of fluid testers (special tool predefined in the knowledge base) that means to the loss of fluid at the place checked by the tester

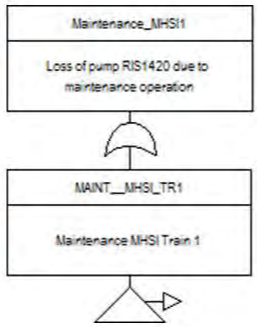


Fourth step : addition of specific knowledge (1)

- It may be desirable to add some specific behaviour. For this operation, it is possible to describe rules, in a graphic way, called "Manual rules"
- Example
  - Maintenance on MHSI Train1 leads to the loss of RIS1420POMPE

Link to the loss of RIS1420POMPE

Link to an external fault tree (transfer gate towards another fault tree)

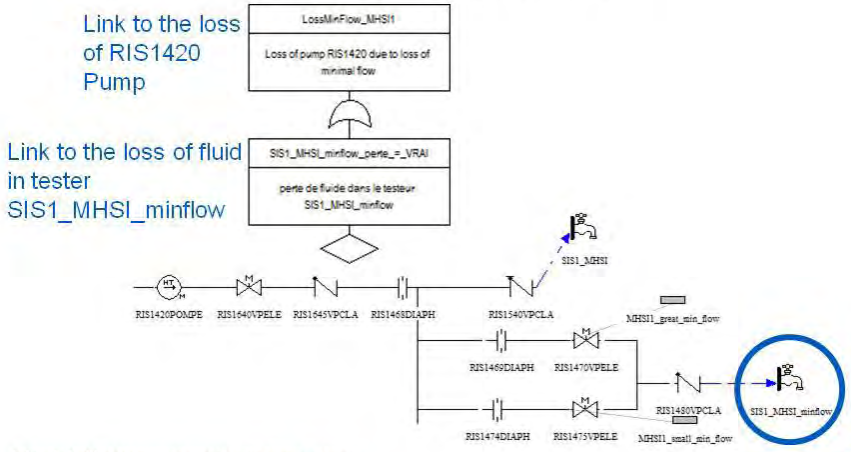


Fourth step: addition of specific knowledge (2)

- Example
  - Loss of minimal flow leads to the loss of RIS1420POMPE

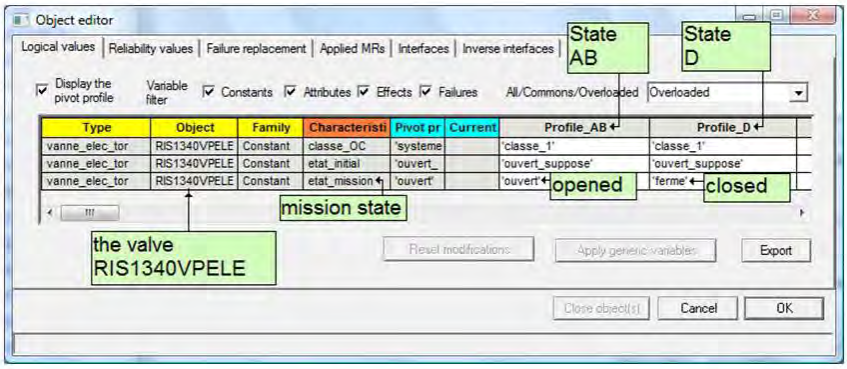
Link to the loss of RIS1420 Pump

Link to the loss of fluid in tester SIS1_MHSI_minflow



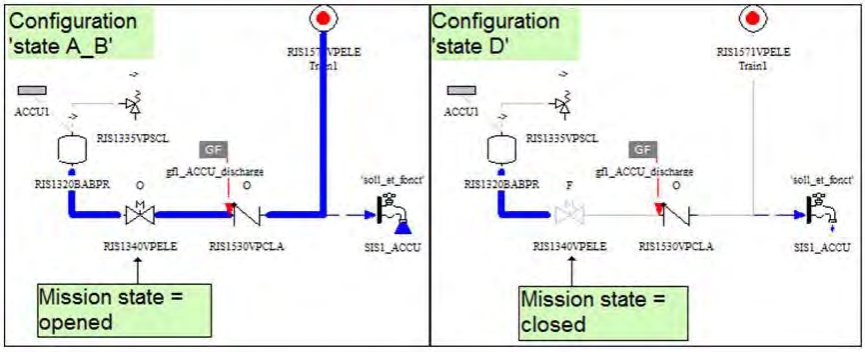
Fifth step: definition of configurations (1)

- The analyst can create several configurations and define them by modifying component characteristics



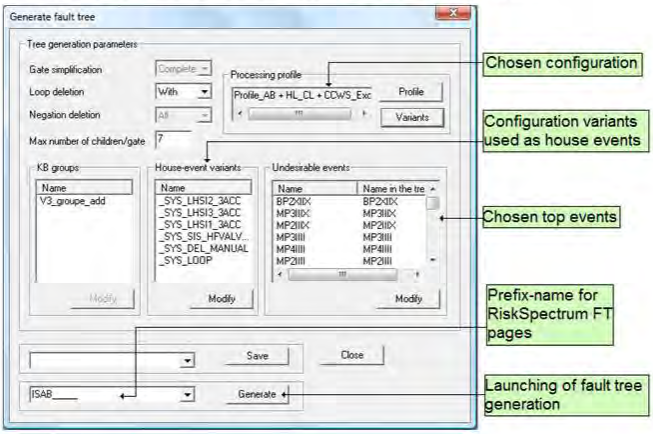
Fifth step: definition of configurations (2)

- Information relative to the system properties for a given configuration can be directly displayed on the system design
  - Example: automatic display of “mission” flow



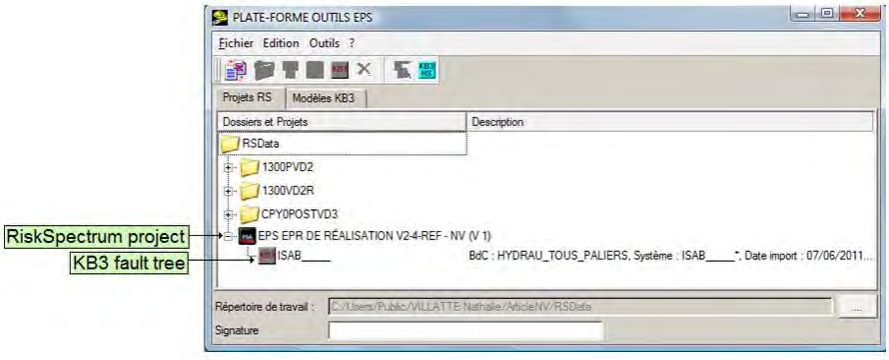
Sixth step: fault tree generation

- The analyst specifies the fault tree to be generated
  - KB3 allows to generate a fault tree with one or several top events



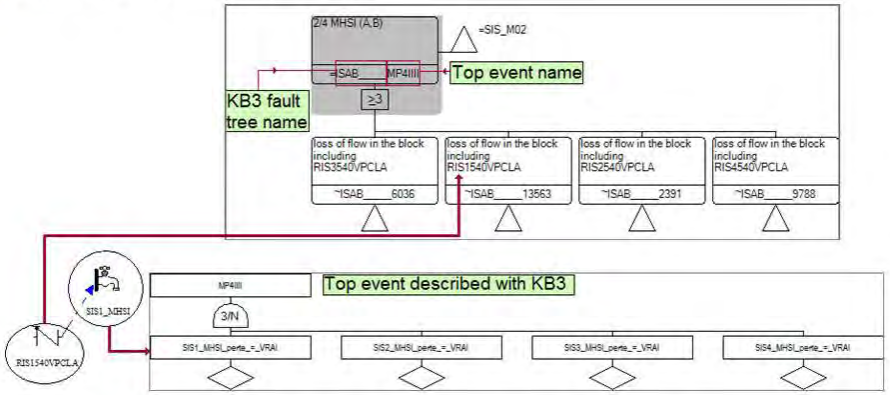
Last step: export to RiskSpectrum® project

- Atelier EPS allows to export KB3 fault trees to a RiskSpectrum® target project



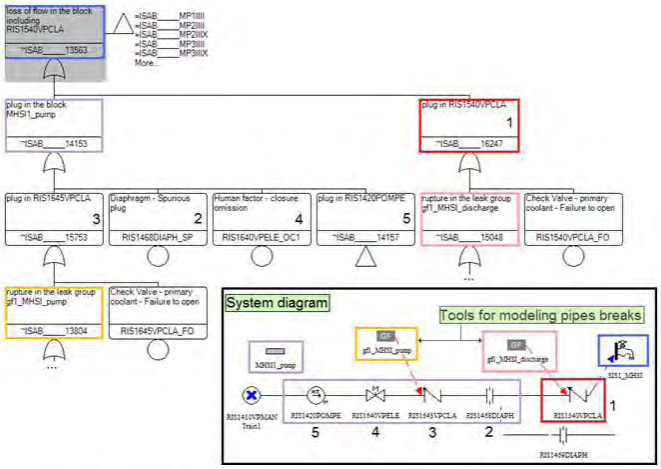
KB3 fault tree transferred to RiskSpectrum® (1)

- Link with the KB3 top events



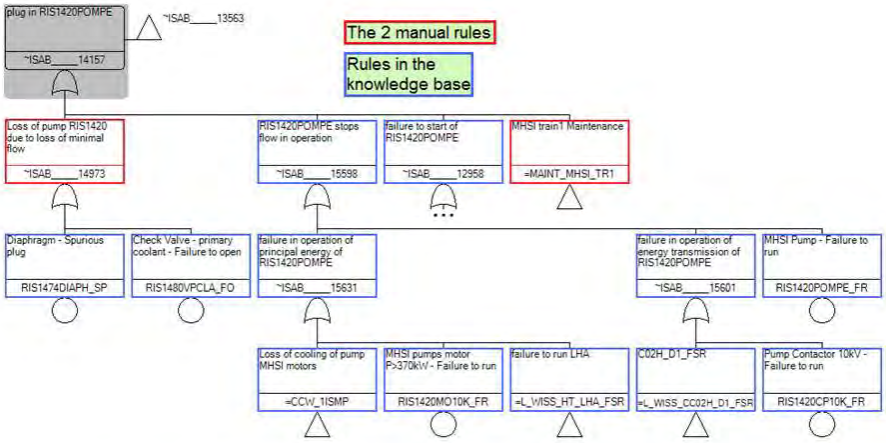
KB3 fault tree transferred to RiskSpectrum® (2)

- Link to the system diagram



KB3 fault tree transferred to RiskSpectrum® (3)

- Manual rules and generic rules



Benefits

- Flexibility
  - It's very easy to modify the diagrams and regenerate fault trees
  - If necessary, the behaviour of generic components can be modified in the knowledge bases
- Diagrams
  - It is easier to work on the basis of a diagram than on a fault tree
- Homogeneity
  - Using KB3 and the same knowledge base ensures a good homogeneity between the fault trees
- Traceability and control of modelling
  - The generated fault trees can be explained with the knowledge base and the content of the system study
- Time saving
  - The analyst can focus on the specificities of his study
  - Using KB3 and Atelier EPS is particularly interesting for a design PSA or a first PSA of an existing unit

Improvements to consider

- **Fault tree readability**
  - Fault trees produced by KB3 for the EPR PSA were sometimes considered not easily "human-readable". Existing functionalities (description fields, translation tools) have not always been used so we will facilitate the access to these functionalities.
- **Export to RiskSpectrum®**
  - We will facilitate the transfer of many fault trees to RiskSpectrum®
- **Handling of the tools**
  - The feedback should help us improve the handling of the tools. For example, the report capabilities will help to control the components characterization.

INVESTIGATIONS OF INTER-SYSTEM COMMON CAUSE FAILURES

Philippe Nonclercq, Marie Gallois, Dominique Vasseur

Electricité de France Recherche & Développement, 1 avenue du Général De Gaulle, 92140 CLAMART, France, philippe.nonclercq@edf.fr ; marie.gallois@edf.fr ; dominique.vasseur@edf.fr

ABSTRACT

Intra-system common-cause failures (CCF) are widely studied and addressed in existing PSA models, but the information and studies that incorporate the potential for inter-system CCF is limited. However, the French Safety Authority has requested that EDF investigate the possibility of common-cause failure across system boundaries for Flamanville 3 (an EPR design). Also, the modeling of inter-system CCF, or the proof that their impact is negligible, would satisfy Capability Category III for one of the requirements in the ASME/ANS PRA standard in the U.S.

EDF and EPRI have been working on a method to assess when it is necessary to take into account inter-system CCF in a PSA model between 2008 and 2010. This method is based both on the likelihood of inter-system CCF and on its demonstrated potential impact on CDF.

This method was first applied on pumps in different systems of the 900 MWe series plants. The second application concerned the motor-operated valves across different systems, using the same PSA model. This second application helped us refine the method, which was not optimal when the number of concerned components is very large. Since then, the method has been successfully applied on the pumps and 10 kV breakers of the EPR power plant in Flamanville.

This paper describes the method and the results obtained in some of these studies. All studies have shown either that components in different systems, when they were not already part of a common cause failure group in the model, are not susceptible to common causes of failure, or that the potential for inter-system common-cause failure is negligible regarding the overall risk.

Keywords : PSA, common-cause failure

1 Introduction

One of the principal characteristics of a probabilistic safety assessment (PSA) approach compared to the deterministic safety approach is to systematically account for common-cause failures (CCF) in the study of severe accident scenarios. There has been extensive analysis of intra-system (i.e., within a system) CCF in the existing fleet of PSA models, but the information and studies that incorporate the potential for inter-system (i.e., between systems) CCF is limited.

However, the Safety Authority in France has requested an inter-system CCF assessment for EPR plants. The French Basic Safety Rule does not have any requirement on this subject while the ASME PRA standard (ref.1) has a requirement only for Capability Category III in supporting requirement SY-B2: MODEL inter-system common causes failures (i.e., across systems performing the same function) when supported by generic or plant-specific data, or SHOW that they do not impact the results.

The intent of this paper is to present the methodology we used and 3 case-studies to which we applied it. All case studies are established PSA models. The first one deals with the pumps of the 900 MWe CPY plants (3-loop PWR), the second one with the motor-operated valves of the same plants and the third one with the high voltage circuit breakers in the new Flamanville 3 model (EPR design).

These works have been presented in detail in 2 older papers : ref. 2 and 3.

2 Background and proposed methodology

The methodology proposed is based on the NUREG/CR-5485 (ref. 4) approach, requirements of the French Basic Rule for PSA (ref. 4) and good practices for defining CCF groups in general.

NUREG/CR-5485 deals with the definition and modeling of CCF groups in the PSA and is recognized as an accepted reference in this field. NUREG/CR-5485 proposes a method to identify the vulnerabilities to common-cause failures. First, an initial screening (qualitative and quantitative) is performed to select potential common-cause failures of the components with strong potential to contribute to the risk of total unavailability of the system. Second, a detailed qualitative analysis is performed to evaluate the similarities between components and their causes of failure.

Finally, a detailed quantitative analysis can be performed to calculate the unavailability due to CCF.

In this paper, the primary focus is on the qualitative approaches suggested. This involves a thorough examination of the feedback from operating experience, design, and practices of the sites in order to identify the basic causes of the failures, the similarities between components of different systems and the lines of defense in place to prevent these potential CCF vulnerabilities.

The French Basic Safety Rule for PSA requires a selection of CCF groups "based on analysis of operating experience and on theoretical analysis of the consequences of cumulative failures."

The implicit understanding of this requirement is that it is useless to define CCF groups for components for which simultaneous multiple failures have few consequences, for example for components that do not contribute to the same safety function or that are not functionally redundant. The requirement in the French Basic Safety Rule for PSA highlights the importance of identical components within the same system providing the same function, because a loss of this equipment could represent the complete loss of the function.

From the ideas above, we have established a four-step process that covers the qualitative approach in NUREG/5485 (steps 1 and 2), quantitative calculations to analyze functional redundancy (step 3), and a final stage to develop and incorporate new CCF groups when warranted (step 4).

These four steps are illustrated in figure 1 and detailed below.

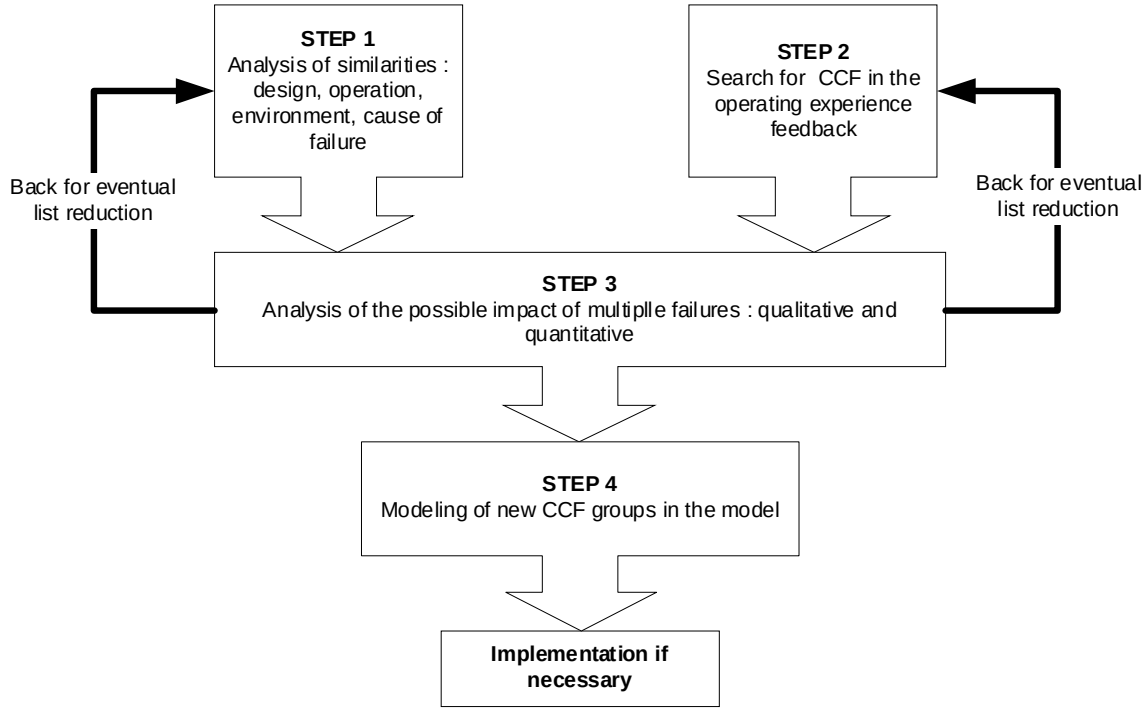


Figure 1. Logic diagram of the method

2.1 Step 1: Qualitatively Identify CCF Groups a Priori

NUREG/CR-5485 provides a suitable groundwork to search for the possible sources of CCF in a systematic and exhaustive fashion.

The purpose of the qualitative analysis of the components is to identify similarities between the components without taking into account the existing lines of defense to prevent the occurrence of CCF. Similarities can exist if two or more components share one or more of the following characteristics: same design, same hardware, same function, same installation, same maintenance practices, same procedures, same component interfaces, same location, or same environment.

The result of this step is a list of components that could be affected by common cause failures.

2.2 Step 2: Search the Operating Experience (OE) Feedback

The review of OE feedback is useful to determine if events would have affected several components from different systems, as is the search for degradations or incipient degradations that have affected multiple systems. The International Common-Cause Data Exchange (ICDE) database of OECD/NEA can also prove very useful at this stage.

2.3 Step 3: Analyse Possible Impact of Multiple Failures

This step is carried out by reviewing the dominant cutsets for the combinations of component failures from different systems that lead to core damage. A tool to ensure an exhaustive and automatic approach is the use of an importance measure defined hereafter for the combination of system or component failures, the RAWC parameter.

2.3.1 Risk Achievement Worth Cumulative (RAWC) importance factor

The risk achievement worth (RAW) of a component A (or for a system or a group of components), for purposes of this assessment, is the relative increase in risk for the case when component A is unavailable. The mathematical expression is the following:

$$RAW(A) = \frac{CDF_{A\_unavailable} - CDF_0}{CDF_0} \quad (1)$$

Where CDF_0 is the reference core-damage frequency.

The RAWC for a combination of components A and B is then defined as follows:

$$RAWC(A,B) = RAW(A,B) - [RAW(A) + RAW(B)] \quad (2)$$

RAWC represents the additional increase in risk due to the synergistic effect of multiple failures or combined unavailability of different systems (A and B).

For a given combination of components, three main cases can be distinguished:

- RAWC = 0: the RAW of the multiple failure case is equal to the sum of the RAW of the two components separately. That means that the components do not appear in the same cut sets or scenarios.

- RAWC < 0: the RAW of the multiple failure case is lower than the sum of the RAW of the two components separately. In this case the failure of one component leads to the failure of the other.

- RAWC > 0: the RAW of the multiple failure case is higher than the sum of the RAW of the two components separately. In this case, there is a multiplicative or synergistic effect. That means that the two components appear in dominant cut sets and the simultaneous failures have important potential consequences. These combinations are the most important to identify because if there is the potential for CCF, the risk increase could be important. At EDF, we calculate the RAWC factors with a post-processing code from a very large number of cut sets (typically more than 100 million).

A qualitative representation using a colour-coded scale for RAWC factors observed in our studies is proposed in figure 2.

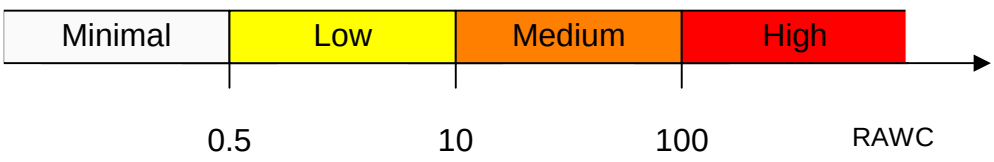


Figure 2. Qualitative representation of RAWC factor scale

RAWC calculations

The RAWC parameter must then be calculated between the right groups of components. It is natural to start by calculating the RAWC between two systems, and to do it for each pair of systems that contain at least one of the components potentially subject to CCF. Components that belong to a pair of systems for which the RAWC is minimal can be ruled out from the study.

The following calculation depends on the components studied. For the pump study, it was quite natural to study the RAWC between a train and another system, and then between a train and a train of another system. But when we studied the motor-operated valves or the circuit breakers the choice was not so obvious. We had then to go back to the definition of RAWC: large RAWC factors result between components that back up each other. To find these components, one must search in the dominant cut sets of the scenarios in which the systems studied back up each other. A list of initiating events and missions is thus selected. A search through the fault trees corresponding to these missions is then necessary to finally identify which components are of potential concern. At this last stage, all component failures, even those which are not critical to the mission, must be closely examined, since a common-cause failure of several of these components can prove to be critical.

Eventually, function-to-function, component-to-function and component-to-component RAWC calculations can be performed. Combinations with minimal RAWC factors are again ruled out from the study.

2.4 Step 4: Model New CCF Groups

This step is pursued only when combinations of various systems with similar components are encountered or actual common-cause events are identified from operating experience feedback, when the multiple failures would have an impact on the risk (RAWC >> 0).

This step has two challenging elements: determining the size of CCF groups and choosing appropriate CCF parameters for the new CCF groups.

2.4.1 CCF parameters

If operating experience feedback is sufficient, calculation of new parameters is possible. If not, conventional values available in the literature or in generic databases can be used.

2.4.2 Size of CCF groups

When a large number of components is identified in step 3, one can be tempted to insert a CCF group containing all the components. But when a calculation is launched with this new group, the resulting CDF can be lower than calculated without the new CCF group. This surprising effect is well-known to RAMS specialists. In 1975, Barlow and Proschan (ref. 6) wrote the following: “If we calculate the reliability of a series system assuming the components independent when in fact they are associated but not independent, we will underestimate system reliability. The reverse is true for parallel systems”.

The effect on a PSA can be explained simply: when a CCF group links two components that do not back up one another, part of the probability of failure of these two components goes into the combination of both failures, which does not lead to core damage and is therefore no more counted in the CDF calculation.

If the dependency between components is well known, i.e., if an adequate amount of operating experience is available for all orders of a CCF group (it seldom happens for large CCF groups in real life), it is recommended that the CCF group be added to the model. The resulting calculation should be appropriate. Conversely, if conventional values have to be used because no operating experience is

available, we recommend to add only those CCF groups for components that back up one another. Adding a CCF group between components whose failures cannot be found in the same minimal cut sets, when one is not sure of the realism of the CCF, could result in underestimating the CDF.

2.5 Return to Step 1 or Step 2

Additionally, it is noted that since the performance of steps 1 and 2 could be time-consuming and costly, the performance of steps 3 and 4 could be pursued in advance of performing steps 1 and 2. This reversal of the order of the steps listed above is therefore identified as a potential mechanism to focus resources on those items that would potentially have the most impact on the PSA model results.

For example, when a large number of components is involved, one can make a limited examination in step 1, go through step 3 and eventually go back to step 1 to make a more selective examination of the list of components potentially susceptible to CCF if needed. It is interesting to have this closer look at the end of step 3 because only a limited number of components needs to be analysed in depth this way.

3 Case studies

3.1 Pumps

The first study deals with the pumps of 900 MW series plants. The definition of "pump" in the 900 CPY PSA model includes the hydraulic part of the pump, i.e. it does not include the motor (or other motive driver) or the circuit breakers (for the electric pumps). On the other hand, it includes the auxiliary lube oil systems and cooling water systems when they exist. This makes possible to remain consistent with the component boundaries as defined in the reliability data reports resulting from the study of the Operating Experience Feedback at all EDF plants.

Because of operating conditions and design, the main coolant pumps (MCPs), the boron pumps, and the ultimate MCP seal injection pump can be readily screened from further inter-system CCF consideration. Consequently, only the safeguard pumps are retained for the study. With the exception of the AFW turbine driven pump, they are all electric pumps supplied with 6.6 kV power from the LHA or LHB safeguard switchgear. Although intra-system CCF groups are included for each of the pump groups, they are similar enough to not exclude the risk of inter-system common cause failure between these pumps without a thorough analysis.

3.1.1 Step 1: Search for similarities and failure causes

The purpose of the qualitative analysis of the components is to identify similarities between the components without taking into account the existing lines of defense to prevent the occurrence of CCF. Similarities can exist if two components or more coincide with one or more of the following characteristics: same design, same hardware, same function, same installation, same maintenance practices, same procedures, same component interfaces, same location, or same environment.

All the pumps considered are single-stage (CSS, ECCS, RHRS, CCW, and ESW) or multi-stage (AFW and CVCS) centrifugal pumps. Among these pumps, only the CSS pumps, ECCS pumps, and ESW pumps are vertical shaft pumps. These very general characteristics are not likely to justify a egrouping within the same CCF group.

All the pumps (except the turbine-driven AFW pump) are electric pumps supplied with a 6.6 kV motor, coupled with the switchgear by a 6.6 kV circuit breaker. The similarities in the power supply source are not dependent on the failures of the pumps but on those of the breakers, the motors, and the electric switchgear. The common dependencies of the electric switchgear are taken into account via the modeling of the support systems in the PSA models.

The analysis reveals that the LP ECCS and CSS pumps are sufficiently close to be regarded as part of the same CCF group: identical pumps from a design point of view, very similar operational practices, and similar maintenance and test routines. The few differences noted between these pumps (not enough to refute the conclusion) are related to their functional role. It is also noted that these pumps have common reliability (failure rate data) in the PSA model.

The analysis also shows an important coupling between the motor-driven AFW pumps and the turbine-driven AFW pump. The only notable differences are the size of the hydraulic part (the number of stages) and the sealing system. The current modeling (1 CCF group of order 3) is not called into question. In addition, the operating experience shows the occurrence of a common cause event affecting the turbine-driven pump and the motor-driven pumps.

Certain similarities were found between some other pumps but are not considered sufficient to qualitatively warrant a new CCF group.

In conclusion, the only new CCF group which would be considered as a potential group of order 4 consists qualitatively, of the LP ECCS and CSS pumps.

3.1.2 Step 2: Analysis of the operating experience feedback

EDF material experts from the Generation Division were questioned about the existence of failures which affected several pumps of different systems. This was followed by a review of available data for recent events. The search was on the precursor events and the CID database (which include all of the licensee significant events declared on EDF fleet since 1992).

Among the examined events, a brief analysis of the most significant events confirms that, apart from the LP ECCS and CSS pumps:

- The common cause events affecting pumps from different systems are very rare and even fewer than those affecting the pumps of the same system.

- The majority of the events detected do not correspond to real failures but to conformity deviations having little impact on the availability of the systems.

- The possible causes of events simultaneously affecting pumps of various systems are use of inappropriate spare parts, use of inappropriate greases, defects related to the environment (common suction for several pumps), and design defects or operational issues.

Among the defects affecting the most systems (eg. use of VITON seals on qualified equipment for RHRS, CVCS, ECCS, and CSS) only one system is generally affected for a plant. Thus, properly speaking, there is not a real inter-system CCF event associated with this issue.

Consequently, the study of OE Feedback confirms the conclusion of step 1: among the studied pumps, the risk of inter-system CCF is not likely except for the LP ECCS and CSS pumps.

3.1.3 Step 3: Analysis of the potential consequences of multiple failures

The objective of this section is to detect the combinations of pumps whose failure has the most potential consequences.

As the results show, a minimal impact in system-system and in system-train combinations could be screened from further analysis at the train-train level. However, these are shown for completeness in Tables 1 and 2.

	RAW	ECCS	CVCS	CSS	CCWS	RHRS (*)
ECCS	21621%		884	-75	232	22
CVCS	29889%	762		-136	-98	-0.3
CSS	8619%	-75	-69		-74	-0.06
CCWS	11970%	189	-75 (**)	-116		-0.6
RHRS	43031%	220959	11792	-0.003	-0.6	

(*) Without shutdown states

(**) CCWS and CVCS trains 1 and 2 have a positive RAWC

Table 1: System-system RAWC

		AFW			ECCS		CVCS			CSS		ESW				CCW				RHRS	
		1	2	3	1	2	1	2	3	1	2	1	2	3	4	1	2	3	4	1	2
	RAW	3.3	8.3	4.2	4.1	5.5	2.9	1.7	2.3	2.5	2.8	1.02	1.03	1.01	1.03	1.03	1.02	1.01	1.02	3.8	1.3
AFW	593.6				3300	3900	3600	1600	5	3200	4400	22	29	1.7	29	22	29	2.9	29	0.2	7E-2
ECCS	216.2	250	270	125			-1.8	4.4E-2	31	-1.4	-1.7	0.6	1.8	2.1E-2	1.8	0.6	1.3	3.8E-2	1.3	2000	72
CVCS	298.9	520	560	233	5.3	25				-1.4	-1.5	4.2E-2	0.2	-7.5E-4	0.2	4.2E-2	0.1	-1.3E-3	0.1	2320	10
CSS	86.2	250	260	125	-1.3	-1.6	-1.4	-0.5	-8E-3			-1.1E-2	-1E -2	-8.10-4	-1.0E-2	-1.1E-2	-1.0E-2	-1.3E-3	-1E-2	0	0
ESW	112.3	136	350	167	124	250	8	19	9E-2	-1.4	-1.4					-1.7E-2	-2.4E-2	-1.7E-3	-2.4E-2	450	- 0.25
CCW	119.7	400	400	170	132	264	8.6	20	8E-4	-1.4	-1.4	-1.7E-2	-2.4E-2	-1.0E-3	-2.4E-2					64	-1E-2
RHRS	430.3	-1.3E-3	-1.3E-3	-8E-4	0.2	0.8	-1.8E-3	-5.8E-4	-1.7E-2	-1.8E-4	-8.8E-4	-4.4E-4	-5.7E-4	-5.5E-5	-5.7E-4	-4E-4	-4.2E-4	-7.5E-6	-4.2E-4		

Table 2 : train-train RAWC Calculation

			AFW			ECCS		CVCS			CSS		ESW				CCW				RHRS	
		RAW	1	2	3	1	2	1	2	3	1	2	1	2	3	4	1	2	3	4	1	2
AFW	1	3.3		31	63	52	2.1	62.2	0.6	0.04	53.4	2.2	0.4	-0.03	-0.01	-0.03	0.4	-0.03	0.003	-0.03	-0.02	-0.04
	2	8.3	26.7		221	2.1	71.8	2.4	26.5	0.06	2.4	71.7	-0.03	0.4	-0.04	0.4	-0.03	0.4	-0.03	0.4	-0.05	-0.05
	3	4.2	63	227		9.6	12.6	11.9	6.5	0.06	9.7	13	0.035	0.05	-0.03	0.05	0.002	0.05	-0.02	0.05	0.003	-0.03
ECCS	1	4.1	53.4	2.1	9.5		265	-0.8	-0.1	0.3	-0.7	-0.03	0.9	-0.02	0.01	-0.02	0.9	-0.02	0.04	-0.02	26.5	0.5
	2	5.5	2	78	13.54	264		-0.07	-0.4	1.1	-0.03	-0.97	-0.03	1.8	-0.03	1.8	0.12	1.8	-0.01	1.84	71.7	2.4
CVCS	1	2.9	63.4	2.4	11.8	-0.9	-0.1		211	0.02	-0.8	-0.03	0.03	-0.03	-0.03	-0.03	0.03	-0.03	-0.03	-0.03	-0.03	-0.03
	2	1.7	0.6	29	6.7	-0.1	-0.5	212		50	-0.03	-0.4	-0.03	0.1	-0.03	0.1	-0.03	0.01	-0.03	0.1	1.6	-0.02
	3	2.3	0.03	0.1	0.02	-0.3	1.1	0.04	50		-0.04	-0.005	-0.005	-0.004	-0.005	-0.005	0.2	-0.005	-0.02	0.005	226	0.1
CSS	1	2.5	53.7	2.4	9.6	-0.7	-0.02	-0.6	-0.02	-0.01		105	0.02	0.52	-0.02	0.52	-0.02	0.5	-0.02	0.5	-0.02	-0.02
	2	2.8	2.25	77.8	13.7	-0 .01	-0.96	-0.0001	-0.31	0.03	105		0.52	-0.01	0.02	-0.015	0.5	-0.015	-0.03	-0.015	-0.015	-0.015
ESW	1	1.02	0.4	-0.004	0.05	0.9	-0.01	0.003	-0.01	-0.01	-0.01	0.52		-0.01	4.2	-0.01	-0.01	-0.01	-0.01	-0.01	-0.01	-0.01
	2	1.03	-0.01	0.4	0.06	-0.01	1.83	-0.0004	-0.1	-0.01	0.5	-0.02	-0.015		-0.01	6.4	-0.015	-0.015	-0.006	-0.015	3	-0.02
	3	1.01	0.02	0.006	0.006	-0.03	-0.001	0.001	-0.001	-0.001	-0.001	0.02	4.2	0.004		-0.005	-0.001	-0.005	-0.001	0.005	-0.001	-0.01
	4	1.03	-0.01	0.4	0.06	-0.01	1.83	-0.0005	0.1	-0.01	0.5	-0 .02	-0.015	6.4	-0.01		-0.015	-0.015	-0.006	-0.015	3	-0 .02
CCW	1	1.03	0.4	-0.006	0.005	0.93	0.12	0.06	-0.01	0.15	-0.02	0 .5	-0.015	-0.015	-0.01	-0.015		-0.01	14.4	-0.01	-0.02	0.5
	2	1.02	-0.006	0.4	0.07	-0.01	1.85	-0.0004	0.1	0.01	0.5	-0.02	-0.01	-0.01	-0.006	-0.01	-0.01		-0.004	12.2	0.4	-0.01
	3	1.01	0.03	0.007	0.007	0.06	0.01	0.002	-0.003	0.025	-0.004	0.05	-0.003	0.006	-0.003	0.006	14.4	-0.006		-0.006	-0.003	0.2
	4	1.02	-0.006	0.4	0.07	-0.01	1.8	-0.0004	0.1	-0.01	0.5	-0.02	-0.01	-0.001	-0.006	-0.01	-0.01	12.2	-0.04		0.4	-0.01
RHRS	1	3.8	0 .03	-0.0001	-0.05	26	71.5	-0.0004	1.5	245	-0.1	-0.1	-0.1	2.7	-0.1	2.7	-0.1	0.35	-0.1	0.4		448
	2	1.3	-0,005	-0,001	-0,005	0,52	2,4	-0,00005	0,003	0,1	-0,005	-0,005	-0,002	-0,005	-0,001	-0,005	0,5	-0,005	0,16	-0,005	397	

Table 3 : train-train RAWC Calculation

Interpretation of the results

From Table 1, at the system-system level, the most important inter-system impacts are presented below:

- The most important inter-system impacts are obtained between AFW with one of the systems necessary for the success of feed and bleed (ECCS, CVCS, CSS, ESW, or CCW). However, the combinations of AFW with one of the ESW or CCW pumps are less important because these systems have more redundancy than ECCS, CSS, or CVCS (4 pumps instead of 2).

- Another high impact inter-system combination is ESW, CCW, or RHRS system with a LP ECCS. These are "loss of the heat sink" scenarios combined with the failure of ECCS.

- The same "loss of the heat sink" scenario type makes RHRS with CVCS combination another high impact system-system combination, as is the loss of ECCS and CVCS.

From Table 2, at the system-train level, the results are the same as the first three important impacts at system-system level with some asymmetries also detected at the train-train level in Table III (e.g. RHRS combined with ECCS or CVCS).

The list of important systems of step 3 has very few in common with that obtained in step 1:

- No significant similarity was found either between AFW pumps and the pumps necessary for feed and bleed or between RHRS and LP ECCS, CVCS, ESW and CCW.

- If there are similarities between the ESW and CCW pumps, failures between these systems are not multiplicative.

- The LP ECCS and CSS pumps are very similar but the effect of simultaneous failures between these systems is also not multiplicative.

The only common point between the analysis of similarities and the analysis of the potential consequences of multiple failures relates to LP ECCS and CVCS (with a potential risk of CCF related to the common suction from the RWS tank or from the recirculation sumps). Nevertheless, this dependence is modeled in a functional way in the PSA and the operating experience feedback analysis has not shown common cause events between the ECCS pumps and CVCS pumps.

3.1.4 Step 4: Model new CCF groups

CCF parameters used currently in French PSA models for pumps only depend on the order of CCF group (2, 3, or 4) and are identical for all the pumps and all the failure modes. These parameters do not result from an analysis of the OE feedback but are conventional values, partially based on OE feedback analysis and international data. These data parameters have not been updated since the first PSA carried out by EDF.

In this modified analysis, two CCF groups of order 2 (with the same β parameter with a value of 0.05 applied) are transformed into one group of order 4, for the closest pumps in design, ie ECCS and CSS pumps. To do this transformation, it is necessary to define a set of MGL parameters (β, γ and δ) for the new group.

Analysis of the OE feedback of the LP ECCS and CSS pumps to develop specific MGL parameters was not possible in the brief context of this study. The standard MGL parameters used in the EDF PSA for the pump groups of order 4 were used instead (b=0.1, g=0.4, d=0.25).

With these parameters, the new CDF was actually found lower than the reference CDF, which is logical since they do not back-up one another (see §2.4.2), and their RAWC was actually found not multiplicative.

3.2 Motor-Operated Valves

The second study deals with the motor-operated valves (MOVs) of 900 MW series plants. These devices can be classified from the design point of view, according to the valve (pressurized containment with shutoff device, the control, the shutoff device and its accessories) or to the servomotor (the whole of the motor, its control apparatus and its mechanical transmission parts). From the functional point of view, the MOVs are isolation valves. In this study, we excluded the 380 V supply circuit breaker of the valve and the instrumentation and control, because in CCF terms, these components are dealt with separately in the PSA model.

There are 91 MOVs taken into account in the 900 PSA model. The distribution by system is presented in table 4, depending on the fluid in circulation.

	VB (Borated water)	VL (Condensed water)	VP (Primary coolant)	VV (Steam)	VN (Demineralized water)
CES		6			
CSS	12			3	
RCS			2		
CVCS			12		
ECCS	2		23		
RHRS			4		
CCWS					6
SBPC				3	

Table 4: MOVs in the 900 Mwe PSA model by system and fluid type

Three types of failure modes can be affected by common-cause failures: internal leakage, failure to open and failure to close. Some of these valves' failure modes already belong to CCF groups: 31 groups of size 2, 3 of size 3, and 7 of size 4. Among these last CCFs, two already concern two groups of valves that do not belong to the same system: RHRS01, RHRS021 and RCS212, RCS215 on the suction line from main reactor coolant.

3.2.1 Step 1: Search for similarities and failure causes

An extensive description of the possible common points between valves and servomotors was performed at this stage. Since it is not possible to expose it here in its entirety, we only give below a few examples of the work performed.

Design and manufacture:

Most of the MOVs are made by the same manufacturer and have the same technology; these are parallel seat valves.

All electric servomotors fitted on safety-related valves are made by a single manufacturer. The main types of servomotors are designated DR and L. The DR and L servomotors are very similar in terms of design. They differ mainly in the torque they deliver. The rest of the servomotors are of type SR, fairly different from these other two (it is not safety-qualified and the reduction system is different).

In design terms, depending on the combinations of valve and servomotor (SM), there are identical valves in all the systems.

Operation:

In the reactor protection rules (RPR), in order to prohibit the operator from opening or closing an important valve (for example injection), the signal is sent permanently to the electrical panel for a certain time. If the torque limiter has been damaged by a manual operation, the motor can be seriously damaged. The recent EDF operating experience feedback shows events of this type for the CSS and ECCS MOVs. This type of procedure and operation only constitutes a similarity for the valves of systems subject to permanent orders.

Maintenance:

One of the discrepancies in compliance sometimes observed in the operating experience feedback of the French fleet is due to the mixture of greases for the servomotors. Greasing is often carried out for all valves and systems at the same time and by the same team or person. In this case, only the operation of the MOVs which can withstand accident conditions for a "long" duration is questioned.

Environment:

Fluid quality is a major factor affecting corrosion and leaktightness. There are therefore common points between valves that carry the same type of fluid.

3.2.2 Step 2: Analysis of the operating experience feedback

For this step, we searched the EDF operating experience feedback and the ICDE database.

There are inter-system CCF events in the operating experience feedback mainly due to maintenance errors. Discrepancies in compliance, only important for certain components in certain accident situations, were due to incorrect greasing of the servomotors.

It is worth mentioning that the events found in the EDF operating experience concern RHRS and RCS valves which already belong to the same inter-system CCF group in the model (see introduction of chapter 3.1).

In most cases, a single MOV is affected, the rest of the components potentially impacted having been inspected at once. When the cause of failure was identified, a line of defense was implemented for all components of the fleet potentially affected. This type of procedure reduces the possibility of the occurrence of events associated with the identified cause.

3.2.3 Step 3: Analysis of the potential consequences of multiple failures

We deduced from the system-system table 1 that only the valves of the ECCS, CVCS, CCWS and RHRS systems need to be retained for the analysis.

We then refined the reasoning made on the system level, in order to more accurately identify the missions of the systems backing up one another and of the associated valves. Valves are not generally critical components for the system and therefore refining the qualitative analysis for the mission proved to be necessary.

We searched among predominant cut sets of the scenarios where the systems studied back up one another in order to establish a list of initiating events. We discovered mainly four groups of initiating events: LOCA, losses of heat sink, partial losses of power sources and steam line breaks (SLBs).

We then targeted the missions (or top events) in operational redundancy for each initiating event by manually searching in each event tree, and we identified the motor-operated valves and failure modes associated with each mission. We performed a search from the fault trees to detect the components whose loss would result in the loss of the mission.

Finally, the new potential groups were identified. Table 5 gives, for example, the potential CCF groups for the failure-to-open mode.

Failure to Open	CVCS 48; CVCS 50 ECCS 13 and 12 **Feeding**	ECCS 78 and ECCS 77 **Boosting**	ECCS 75 and 85 **Injection**	ECCS 51 and 52 **Recirculation**
CVCS 48 and 50 ECCS 13 and 12 **Feeding**			x	x
CCWS 41 **Switchover**	x		x	x
ECCS 20 and 21 **RHRS low work pressure makeup**	x			
ECCS 19 and 20 RHRS 01 and 021 RHRS 013 and 014 RCS 212 and 215 **RHRS operation**		x	x	x

Table 5: Potential CCF groups for the failure to open mode

N.B.: The combination of three systems can also be deduced from this table. For example, CCWS, CVCS and ECCS with failure of the "CCWS line A to B switchover" and "Isolation of CVCS lines" and "LPSI injection and recirculation" could be considered. Such combinations, however, typically have a negligible contribution in the quantification of CDF.

In parallel with this qualitative work, we performed RAWC calculations between functions. The result has consolidated the qualitative analysis, with the bonus of a quantification of the importance of potential CCF between functions. We finally found out the following hierarchy:

1 - The largest RAWC is the accumulation of failures between the CVCS feeding valves backing up the RHRS low work pressure makeup valves required during breaks in a shutdown state or loss of RHRS scenarios. At the same time, the charging may be backed up via low-pressure recirculation or injection but the accumulation of the associated valves has a smaller value for RAWC (orange).

2 - The accumulation of failures of the valves associated with the high-pressure recirculation function and the CCWS switchover also has an important RAWC. Low-pressure recirculation is necessary for controlling a primary break caused by the loss of cooling for reactor coolant pump set bearings and seals during power operation, partial losses of power sources, losses of heat sink due to loss of the feedwater plant or partial losses of CCWS/RWS or in primary transients.

3 – CVCS Feeding or the HP injection also back up the ECCS switchover but with less multiplicative RAWC (orange).

4 - The accumulation of the failure of the low-pressure ECCS recirculation and the non-isolation or non-operation of the RHRS have a multiplicative RAWC (orange) in LOCA, loss of RHRS or partial loss of power source scenarios where low-pressure ECCS recirculation is required to restore sufficient water makeup.

3.2.4 Return to Step 1

For the valves belonging to the potential CCF groups identified in step 3, we carried out a more thorough examination to determine the degree of similarity. We concluded that, although we could not discard any of the potential CCF groups, some contained valves operated by servomotors of very different design that operated differently (some subject to permanent orders, some not). The probability of a CCF between these last valves was considered to be low.

3.2.5 Step 4: Model new CCF groups

In order to avoid a potentially non-conservative result, we introduced the smallest CCF groups possible, and only for valves backing up one another (see § 2.4.2). CCF parameters used are the generic parameters used for identical valves. Only four new CCF groups were found to increase the reference risk

- Failure-to-open mode: a new CCF group of order 4 between the CVCS feeding backing up the RHRS low work pressure makeup valves adds 1.04% to the reference risk (failure-to-open mode). Valves and servomotor are identical.

- Failure-to-open mode: three CCF groups of order 3 were added between the CCWS switchover and the ECCS recirculation valves. Summing the contribution of these groups leads to a 1.7% increase in the risk (failure-to-open mode). Servomotors of the valves are different and they are also operated differently. This estimation of the increase of risk is therefore highly conservative.

- Failure to close: a CCF group of order 3 between CCWS switchover and ECCS recirculation valves adds 0.17% to the reference risk.

3.3 Circuit Breakers

This third study deals with the 10 kV circuit breakers of the EPR (Flamanville 3) nuclear power plant. Figure 3 shows the electrical supply architecture of the four-train EPR plant.

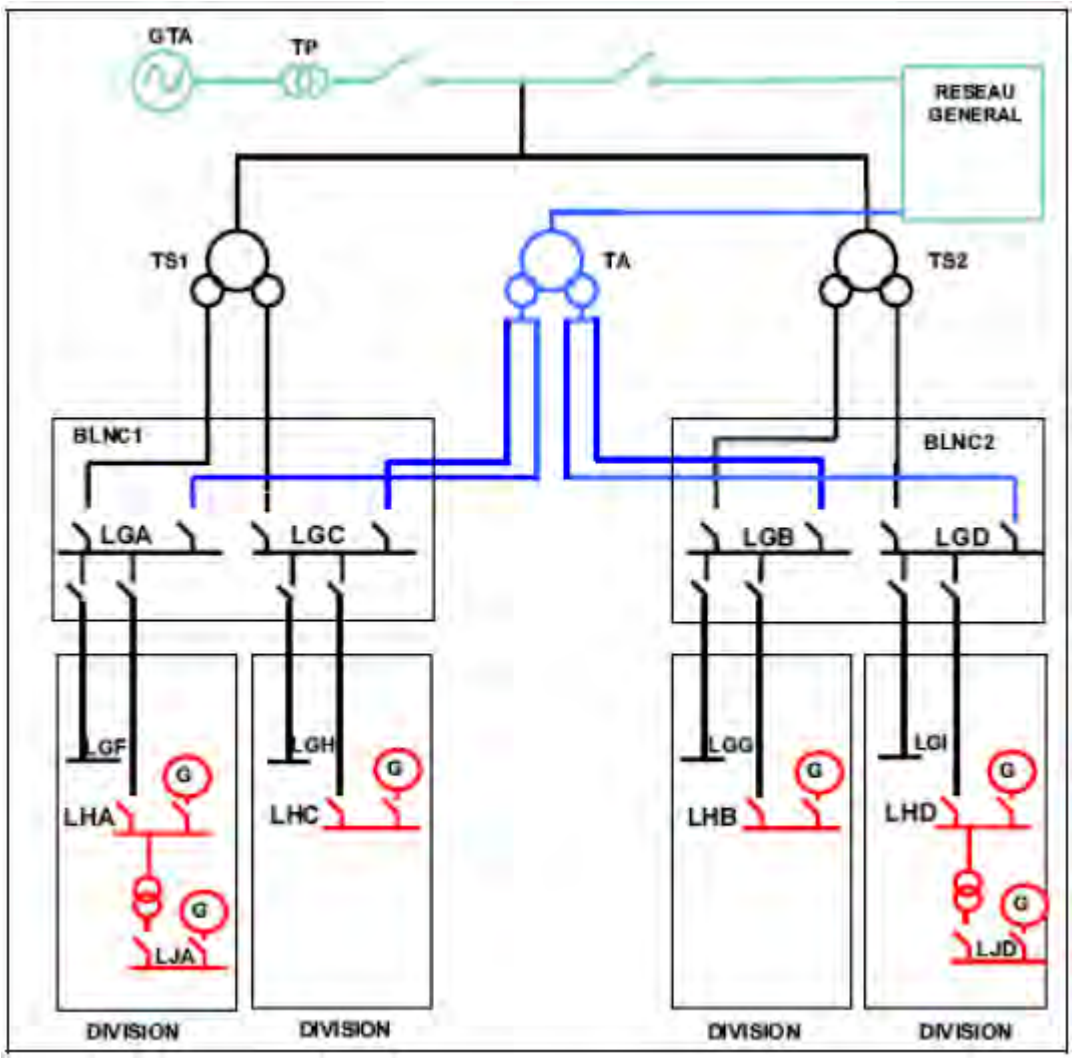


Figure 6 EPR Electrical Supply

There are 38 10 kV breakers used in the EPR plant and modeled in the EPR PSA, and that are of concern in this study. They are installed on the normal supply (systems LGA/B/C/D/F/G/H/I/K/N/P/Q/R/S), backup supply (systems LHA/B/C/D) and on the four main reactor coolant pumps supply (system RCP).

There are already three CCF groups of size 4 in the PSA model:

- failure to open of 4 breakers on the outgoing line to the main coolant pumps (LGF/G/H/I systems)

- failure to open of the 4 breakers on the main coolant pumps (RCP system)

- failure to close of the breakers on the incoming line from the diesel generators (LHA/B/C/D systems).

3.3.1 Step 1: Search for similarities and failure causes

All breakers are very similar with respect to design, operation, maintenance and operating environment. There actually is a single significant difference between the diesel generators breakers and the others since they only function as a backup.

3.3.2 Step 2: Analysis of the operating experience feedback

EPR breakers cut-off in void whereas high voltage breakers of the other French nuclear power plants cut-off in SF6. One coal-fired plant uses void cut-off breakers in France. A search revealed that no failure involving the cut-off system of its 57 breakers was ever experienced since they were installed in 1995.

In spite of their different cut-off technology, we searched the operating experience of the French nuclear power plants. We found one CCF event that potentially affected all breakers of the CP0 plant series (the first four 900 MWe plants), linked to a degradation of the insulation of reset motor supply. This type of CCF cannot be excluded for the EPR breakers.

In the ICDE database, two CCF events were found.

3.3.3 Step 3: Analysis of the potential consequences of multiple failures

This step started by a functional analysis of the different breakers. We distinguished small groups of breakers which operated in normal/backup operation. We searched then which failures caused the loss of LG switchboards, and the loss of LH switchboards.

We therefore identified the following:

1 Four groups of 8 breakers for short circuit, failure to run, failure to open, and spurious opening failure modes on LG switchboards. They concern the incoming lines from the transformers (unit and auxiliary transformers).

2 One group of 4 breakers for the failure to close mode on LG switchboards. They only concern the incoming lines from the auxiliary transformer.

3 Three groups of 8 breakers for short circuit, failure to run, and spurious opening modes on LH switchboard. They concern the incoming lines from LGA/B/C/D switchboards and from the diesel generators.

4 One group of 4 breakers for the failure to close mode on LH switchboards. They concern the incoming lines LG switchboards and from the diesel generators.

5 1 group of 4 breakers for the failure to open mode on LH switchboards. They concern the incoming lines to the LG switchboards and from the diesel generators.

To ensure an adequate level of completeness, we also performed some RAWC calculations. The pairs of components considered were, on the one hand, the loss of a safeguard switchboard LHA/B/C/D through a failure of a well-chosen breaker, for spurious opening, short circuit and failure to run mode; and on the other hand any failure mode of any other breaker of the study.

We identified thus three potential CCF groups with RAWC values greater than 100. The first one (number 6) contains 13 LG and LH breakers, for the short-circuit failure mode. The second one (number 7) contains 4 LH breakers, for the failure-to-run failure mode. The last one (number 8) contains 3 LH breakers, for the spurious opening failure mode.

3.3.4 Step 4: Model new CCF groups

CCF groups are created and were evaluated by applying conventional values used at EDF since the 1990s based on expert judgments.

All CCF groups identified in step 3 were put into the model. CCF groups 3, 4 and 5 add together about 1% to the reference risk. CCF groups 6 to 8 add together 0.6% to the reference risk. The first three CCF groups do not change the reference risk.

As a further sensitivity, we also modeled CCF groups containing all the breakers for each failure mode included in the model, using conservative parameters. The result was between a slight decrease in the reference risk and a slight increase: [-0.03%;+0.16%].

4 Conclusions

These three studies helped us refine the method for assessing whether or not it is necessary to include inter-system CCFs in a PSA model. As far as 900 MWe pumps, valves and EPR 10 kV breakers are concerned, we established that including these intersystem CCFs would have a negligible impact on CDF.

5 Acknowledgments

We would like to thank Prof. Berenguer of Université Technologiques de Troyes who provided us with ref. 6, which helped us explain the result of a CDF calculation with a large CCF group that can be lower than the same CDF calculation without this CCF group.

We also must thank Paula Calle-Vives (formerly EDF), who did most of the work on the valves, and Simon Bregand (Sector) who helped us on the breakers. This work was also read and commented by EPRI, particularly MM. Kenneth Canavan and Stuart Lewis.

6 References

1. American Society of Mechanical Engineers, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-Sb-2005, New York, New York, December 30, 2005.

2. P. Calle Vives, J. Primet, K. Canavan, D.E. Vanover, “Investigation of inter-system common cause failure”, Proceedings of PSA ’08, Knoxville, Tennessee, September 7-11, 2008.

3. M. Gallois, D. Vasseur, Ph. Nonclercq, J. Primet, « Investigation of inter-system common cause failures : an update », Proceedings of PSA ’11, Wilmington, North Carolina, March 13-17, 2011.

4. Idaho National Engineering and Environmental Laboratory, Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessment, NUREG/CR-5485, INEEL/EXT-97-01327, November 1998.

5. Direction Générale de la Sûreté Nucléaire, Basic Safety Rule, Development and Utilisation of Probabilistic Safety Assessments, December 2002.

6. R.E. Barlow, F. Proschan, Statistical Theory or Reliability and Life Testing, Ed. Holt, Rinehart & Winston, pp. 32-33, 1975

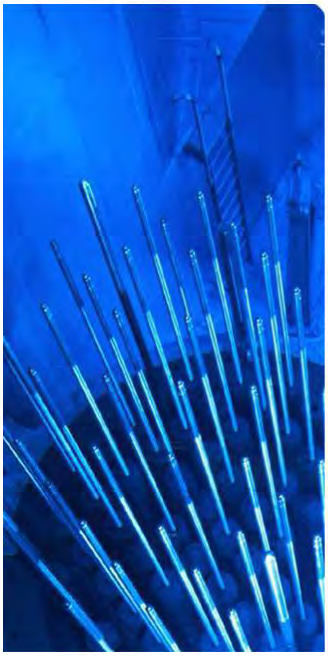
Investigation of Inter-system Common Cause Failures : an Update

Dominique Vasseur, Marie Gallois
Philippe Nonclercq
EDF R&D

In collaboration with
EPRI

WGRISK Workshop on PSA for new and advanced reactors
June 20-22 2011
Paris

EDF
CHANGER L'ÉNERGIE ENSEMBLE



Contents

EDF

Introduction

A common issue

- ASME/ANS RA-SA-2009
  - *« Model inter-system common cause failure (i.e. across systems performing the same function) when supported by generic or plant specific data, or SHOW that they do not impact the result. »*
- Request from French Safety Authorities (ASN)
  - 900 Mwe series pilot studies : 2007 – 2008
    - Pumps and MOVs
  - EPR studies : 2009 – 2010
    - Pumps, MOVs, 10kV Breakers

• EPRI co-funder

Methodology

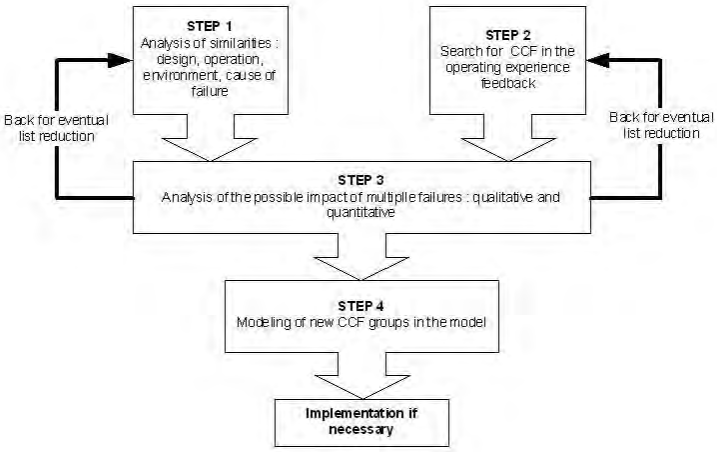
Basis

- Methodology based on :
  - NUREG/CR-5485 « Guidelines on Modeling CCF in PSA »
    - Principles of a qualitative identification of CCF groups
  - French PSA fundamental safety rule
    - Select CCF groups by operating experience analysis and consequences of multiple failures evaluation

Main Steps

- Step 1 : Qualitative identification of potential CCF groups
  - Based on NUREG : tracking of design, operation & maintenance similarities
- Step 2 : Operating experience analysis
  - Search for failures or incipient failures for similar components in different systems, with same failure cause
  - Search in EDF and international (ICDE) OPEX
- Step 3 : Consequences analysis of CCF groups identified in steps 1 & 2
  - Asked by the French basic safety rule
  - Qualitative analysis of predominant cutsets
  - Importance Factors calculations
- Step 4 : New CCF groups modeling

Logigram – An iterative method



RAWC : a tool for step 3

- Risk Achievement Worth Cumulative Factor (RAWC)
  - Estimates the risk increase of multiple failures, compared with single failures
  - Used to identify critical cumulative failures

$$RAWC(A,B) = RAW(A.B) - [RAW(A) + RAW(B)]$$

$$RAW(A.B) = \frac{R(A.B) - R_{réf}}{R_{réf}} \quad RAW(A) = \frac{R(A) - R_{réf}}{R_{réf}} \quad RAW(B) = \frac{R(B) - R_{réf}}{R_{réf}}$$

With :
R(A.B) : CDF with A and B unavailable
R(A) : CDF with A unavailable
R(B) : CDF with B unavailable
$R_{réf}$: Reference CDF

RAWC(A.B) ≤ 0 => Risks add :
No functional redundancy between systems/components in accidental scenarios
RAWC(A.B) > 0 => Risks multiply :
One system/component backs the other up in accidental scenarios

EDF

RAWC Interpretation

RAWC<0	Failure of one pump/system leads to the failure of the other pump/system
0<RAWC<0,5	Pumps/system don't appears in the same cutsets → no impact if considering CCF
0,5<RAWC<10	Simultaneous failures of pumps from different systems can have important consequences
10<RAWC<100	
100<RAWC	

EDF

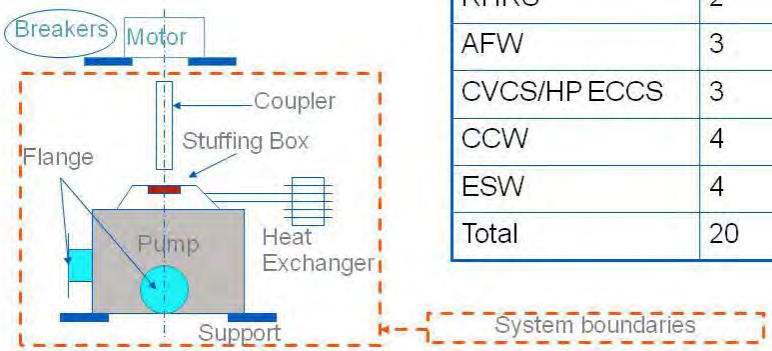
900 MWe series Pumps Results

EDF

900 MWe series pumps : scope

Model PSA 900 CPY
- internal events
- power and shutdown

Centrifugal pumps
- hydraulic part



System	No. of pumps
LP ECCS	2
CSS	2
RHRS	2
AFW	3
CVCS/HP ECCS	3
CCW	4
ESW	4
Total	20

EDF

900 MWe series pumps : result of steps 1 & 2

- Step 1 : search for similarities
  - LP ECCS and CSS pumps should be considered as a CCF group.
  - AFW Motor-Driven Pumps and Turbine-Driven Pump should be considered as a CCF group
  - Similarity between CCW and ESW pumps or LP ECCS, CSS and CVCS isn't important enough to consider a priori a CCF group
- Step 2 : operating experience
  - Review of OE confirms step 1 a priori analysis
  - Intersystem CCF are even unlikely than intra-system CCF
  - Lessons learnt can help to strengthen defence lines against CCF

EDF

900 MWe series pumps : result of step 3 (1)

Qualitative analysis

Families of accidental sequences		Identification of pumps in back-up of the others												
		AFW-CSS	AFW-ECCS	AFW-CVCS	AFW-CCW	AFW-ESW	ECCS-CVCS	CCW-CVCS	ESW-CVCS	CCW-ECCS	ESW-ECCS	CCW-RHRS	ESW-RHRS	ECCS-RHRS	CVCS-RHRS
APRP GB	Loss of cooling accident (large break)						*								
APRP PB	Loss of cooling accident (small break)			*			*								
PSL BT	Loss of heat sink	*	*	*	*	*						*	*	*	*
PSF	Loss of low voltage bus bars	*	*	*	*	*	*								
PSL HT	Total loss of power supplies	*	*	*	*	*				*	*				
TGTA	Secondary transients	*	*	*	*	*									
TRCP	Primary transients				*	*		*	*	*	*				
RTS-RTGV	Break on secondary pipes + induced SGTR														
RTGV	SGTR	*	*	*	*	*									
ATWS	Transients with failure of scram														
RTE-RTV	Ruptures of secondary pipes of FW or main steam	*	*	*											

- Dominant scenarios :
  - Loss of AFW followed by failure of feed &bleed (LP ECCS, CSS, CVCS)
  - Lost of cooling chain during outage (RHRS, ESW, CCW) followed by failure of make-up (CVCS, LP ECCS)

EDF

900 MWe series pumps : result of step 3 (2)

- Train-train

		AFW			ECCS		CVCS			CSS		ESW				CCW				RHRS	
		1	2	3	1	2	1	2	3	1	2	1	2	3	4	1	2	3	4	1	2
AFW	1		31,15	63	52	2,1	63,2	0,6	0,04	53,4	2,2	0,4	-0,03	-0,01	-0,03	0,4	-0,03	0,003	-0,03	-0,02	-0,04
	2	26,7		221	2,1	71,8	2,4	26,5	0,06	2,4	71,7	-0,03	0,4	-0,04	0,4	-0,03	0,4	-0,03	0,4	-0,03	-0,05
	3	63	221		9,6	12,6	11,9	6,5	0,06	9,7	13	0,035	0,03	-0,03	0,03	0,002	0,03	-0,02	0,03	0,003	-0,03
ECCS	1	53,4	2,1	9,5		265	0,8	0,1	0,3	0,7	-0,03	0,9	-0,02	0,01	-0,02	0,9	-0,02	0,04	-0,02	26,5	0,5
	2	2	78	13,54	264		-0,07	0,4	1,1	0,03	-0,02	-0,02	1,8	-0,03	1,8	0,12	1,8	-0,01	1,84	71,7	2,4
CVCS	1	63,4	2,4	11,8	-0,0	-0,1		111	0,02	-0,8	0,05	0,03	-0,03	-0,03	-0,03	0,03	-0,03	-0,03	-0,03	-0,03	-0,03
	2	0,6	29	6,7	-0,1	-0,5	212		50	-0,03	-0,4	-0,03	0,1	-0,03	0,1	-0,03	0,01	-0,03	0,1	1,6	-0,02
	3	0,03	0,1	0,02	-0,3	1,1	0,04	50		-0,04	0,003	-0,003	0,004	0,005	-0,005	0,2	0,003	-0,02	0,008	226	0,1
CSS	1	53,7	2,4	9,6	-0,7	-0,02	-0,6	-0,02	-0,01		186	0,02	0,52	-0,02	0,52	-0,02	0,5	-0,02	0,5	-0,02	-0,02
	2	2,25	77,8	13,7	-0,01	0,06	-0,0001	-0,21	0,05	186		0,52	0,01	0,02	-0,015	0,5	-0,015	-0,03	-0,015	-0,015	-0,015
ESW	1	0,4	-0,004	0,05	0,9	-0,01	0,003	-0,01	-0,01	-0,01	0,52		-0,01	4,2	-0,01	-0,01	-0,01	-0,01	-0,01	-0,01	-0,01
	2	0,01	0,4	0,06	-0,01	1,83	-0,0004	0,1	-0,01	0,5	-0,02	-0,015		-0,01	6,4	-0,015	-0,015	-0,006	-0,015	3	-0,02
	3	0,02	0,006	0,006	-0,03	0,001	0,001	-0,001	-0,001	-0,001	0,02	4,2	0,004		-0,005	-0,001	-0,005	-0,001	0,005	-0,001	-0,01
	4	0,01	0,4	0,06	-0,01	1,83	-0,0005	0,1	-0,01	0,5	-0,02	-0,015	6,4	-0,01		-0,015	-0,015	-0,006	-0,015	3	-0,02
CCW	1	0,4	-0,006	0,005	0,93	0,12	0,06	-0,01	0,15	-0,02	0,5	-0,015	-0,015	-0,01	-0,015		-0,01	14,4	-0,01	-0,02	0,5
	2	0,006	0,4	0,07	-0,01	1,85	-0,0004	0,1	0,01	0,5	-0,02	-0,01	-0,01	-0,006	-0,01	-0,01		-0,004	12,2	0,4	-0,01
	3	0,03	0,007	0,007	0,06	0,01	0,002	-0,003	0,025	-0,004	0,05	-0,005	0,006	0,002	0,006	14,4	-0,006		-0,006	-0,005	0,2
	4	-0,006	0,4	0,07	-0,01	1,8	-0,0004	0,1	-0,01	0,5	-0,02	-0,01	-0,001	0,006	-0,01	-0,01	12,2	-0,04		0,4	-0,01
RHRS	1	0,03	-0,0001	-0,03	26	71,5	-0,0004	1,5	245	0,1	-0,1	-0,1	2,7	-0,1	2,7	-0,1	0,25	-0,1	0,4		446
	2	-0,005	-0,001	-0,005	0,52	2,4	-0,00005	0,003	0,1	-0,005	-0,005	-0,002	-0,005	-0,001	-0,005	0,5	-0,005	0,16	-0,005	387	

- **Potential impact of INTRASYSTEM CCF is higher than for INTERSYSTEM CCF**
  - ✓ exceptions are RHRS/CVCS and AFW with F&B systems

900 MWe series pumps : conclusion

- Conclusions of step 1, 2 and 3 are :
  - Confirmation of grouping turbine-driven and motor-driven AFW pumps
  - LP ECCS and CSS could be modeled in the same CCF group but no impact on CDF is expected
  - Cumulative failures of AFW/F&B or RHRS/CVCS have potential impact but no similarities and OE occurrences were found for these systems

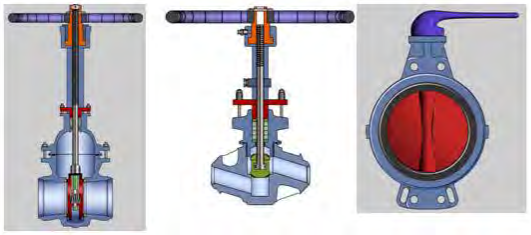
- Thus, step 4 is not strictly necessary for pumps but was developed without measurable impact
  - grouping ECCS and CSS pumps in the same CCF group :
    - Creates difficulties to interpret the cutsets
    - Reduces the CDF

900 MWe series MOVs Results

900 MWe series valves : scope (1)

Model PSA 900 CPY
- internal events
- power and shutdown states

Motor Operated Valves



Valve with parallel seats	Globe valve	Butterfly valve

Breaker and I&C are excluded from the system boundaries

+ servomotor (3 different types depending on their power)

900 MWe series valves : scope (2)

	VB Borated	VL Condensate	VP Primary	VV Steam	VN Demineralised
Condensate		6			
CSS	12			3	
RCS			2		
CVCS			12		
ECCS	2		23		
RHRS			4		
CCW					6
Turbine bypass				3	

91 valves modeled in 900 Mwe PSA
No MOVs on EFWS

3 failure modes per valve : FTO, FTC,IL

EDF

900 MWe series valves : result of steps 1 & 2

- Step 1 : search for similarities
  - Some similarities of design, operation and environment were found
  - The possible number of new CCF groups is very high
  - ➔ Relevant groups must be identifed through a prioritisation according to the consequences of a common failure (go through step 2 and 3 before going back to step 1)
- Step 2 : operating experience
  - EDF OE 1988 – 1994
    - No Common-Cause occurrences for valves on different systems
  - ICDE and EDF OE 1995-1999, CID OE databases :
    - 7 Common-Cause occurrences (Spain, France)
      - Concerns CCW, RHRS, ECCS, CVCS, CSS
      - Maintenance errors, grease mistakes
      - 1 single failure occurred at most, other valves were checked (defence line) and only degradations or incipient degradations were found
  - EDF maintenance feedback databasis
    - RHRS and RCS intersystem CCF were found, but this CCF group already exists in the model

EDF

900 MWe series valves : result of step 3 (1)

failure to open	RIS32 to 35 RIS13 AND 12 **HP Injection**	RCV 50-48 RIS13-12 **Feeding line**	RIS51-52 **Recirculation**
RRI 40; 41; 59 **Switchover**	3		2
RIS20-21 **RHRS Makeup**		1	
RRI 19-20 **RHRS operation**			4

1. failure to open of feeding line after the failure to open of RHRS makeup necessary in case of small break in shutdown states or loss of RHRS scenarios

failure to close	RCV 48-50 RCV 222-223 **Not isolated**	RCV 33-34 **Feeding**	RIS75-85 RIS134-163 **Recirculation**
RCV 33-34 **Feeding**			
RRI 58-41 **Switchover**		3	2
RRA 01-021 RCP 212-215 **RHRS isolation**			4

2. Failure of ECCS recirculation and CCWS switchover in case of loss of primary pumps seals and bearings cooling in power states, partial loss of power, loss of heat sink or primary transients

EDF

900 MWe series valves : back to step 1 : search for similarities

- Failures mostly affect the servomotors, particularly for those subject to permanent orders

→ Potential high coupling for valves with identical servomotors
  - RCV, RIS 20-21, 75-85, 134-163, RRI (CVCS, ECCS, CCWS)

→ Potential high coupling for valves subject to permanent orders
  - RCV 33-34, 222-223, RIS 51-52, 75-85, 134-163 (CVCS, ECCS)

→ Low coupling for the others
  - RRA, RCP with RIS 75-85, 134-163 (RHRS, RCS, ECCS)

EDF

900 MWe series valves : step 4 : Modelling new CCF groups

- Model
  - 17 new CCF groups identified in former steps
  - standard CCF parameters
- Results negligible for most of the new groups
  - RRI 40-41-58-59VN with RIS 51-52VP : cdf increased by 1.7%
    - Standard parameters could be significantly lowered : different servomotors, different locations, different fluids, different tests
  - RCV 50-48VP with RIS 20-21VN : cdf increased by 1.04%
    - Same valves, servomotors, environment
    - Different operation regime
    - Limited impact on the cdf

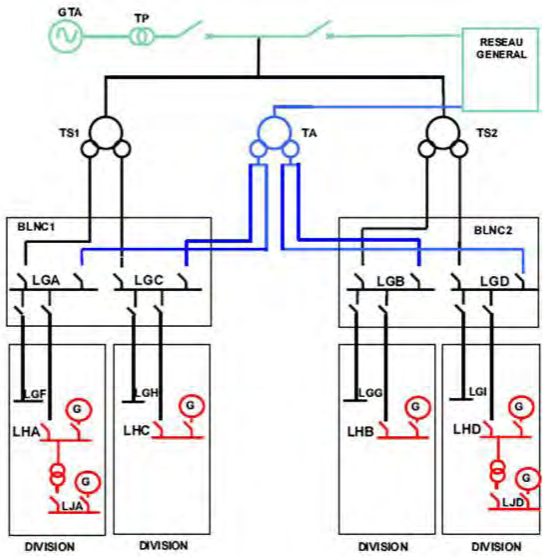
EDF

FA3 Electrical cabinets installation

EPR 10KV Breakers Study Results

EDF

EPR Electrical Distribution



EPR 10 kV Breakers List

LGi Breakers	LGi Breakers (cont')	LHi Breakers	LIi, Lki, Lli Breakers
LGA1110JA10K	LGH1101JA10K	LHA1101JA10K	LIB1101JA10K
LGA1120JA10K	LGI000XJA10K	LHA1102JA10K	LIC1101JA10K
LGB1110JA10K	LGI1101JA10K	LHB1101JA10K	LKB1101JA10K
LGB1120JA10K	LGK1101JA10K	LHB1102JA10K	LKC1101JA10K
LGC1110JA10K	LGK1102JA10K	LHC1101JA10K	LLA1101JA10K
LGC1120JA10K	LGK1103JA10K	LHC1102JA10K	LLC1101JA10K
LGD1110JA10K	LGN1101JA10K	LHD1101JA10K	
LGD1120JA10K	LGN1102JA10K	LHD1102JA10K	
LGF000XJA10K	LGN1103JA10K	**Diesels Breakers**	
LGF1101JA10K	LGP1101JA10K	LHA1103JA10K	
LGG000XJA10K	LGQ1101JA10K	LHB1103JA10K	
LGG1101JA10K	LGR1101JA10K	LHC1103JA10K	
LGH000XJA10K	LGS1101JA10K	LHD1103JA10K	

EPR breakers : step 1 : Qualitative Identification of Potential CCF Groups

- Design
  - Same supplier, insignificant design differences => all breakers share the same technology and design
- Operation
  - Same operation mode, but for the emergency diesel generators breakers
- Maintenance
  - Same monitoring and maintenance for all breakers
- Localization
  - All electrical cabinets are in air-conditioned rooms.
  - Cabinets hosting different channels breakers are in separate rooms. Separation should resist flood or an airplane crash

10 kV breakers intersystem CCF groups existence cannot be ruled out by qualitative analysis

EDF

EPR breakers step 2 : Operating Experience Analysis

- EPR : void-break circuit-breakers
- EDF Operating Experience (OPEX)
  - Existing plants : 6.6 kV oil-blast or SF6-blast circuit breakers
  - 2 common-cause events :
    - Solidified lube oil presence in non-accessible parts of the system. Corrective maintenance actions were undertaken
- ICDE (international)
  - ICDE database : 5 countries operate void-break circuit breakers between 2 and 11 kV : UK, Spain, Sweden, South Korea and Germany.
  - Some incipient degradation or degradation were observed.
  - 2 CCF events.

10 kV breakers intersystem CCF groups existence cannot be ruled out by OPEX analysis

EDF

EPR breakers : step 3 : Consequence Analysis (1)

0<RAWC<0.5	No impact
0,5<RAWC<30	Weak impact
30<RAWC<100	Medium impact
RAWC> 100	Strong impact

- Example of RAWC calculation results

		ASG		RIS (ISHP)				RRI				SEC				RCV	
		2	3	1	2	3	4	1	2	3	4	1	2	3	4	1	4
ASG	2		4,249	0,667	51,514	0,870	0,667	0,018	47,790	0,116	0,119	0,029	48,720	0,171	0,174	0,029	0,001
	3	4,254		1,231	0,704	51,438	0,708	0,590	0,123	48,030	0,038	0,639	0,177	49,060	0,048	0,001	0,029
RIS (ISHP)	1	0,231	0,954		21,013	20,873	4,369	0,006	10,168	8,392	2,593	0,000	10,190	8,418	5,051	1,403	0,000
	2	49,840	0,254	20,998		22,149	1,824	16,337	0,003	9,028	0,956	8,399	0,000	9,070	3,133	0,080	0,000
	3	0,226	49,750	20,856	22,146		1,770	16,327	9,029	0,002	0,533	8,419	9,070	0,000	0,451	0,000	0,001
	4	0,222	0,250	3,850	1,318	1,266		25,496	4,263	0,441	0,005	23,991	4,274	0,469	0,000	0,000	1,278
RRI	1	0,197	1,366	0,794	21,342	21,312	50,091		[illegible]	9,249	48,940	0,000	[illegible]	10,240	45,830	0,060	0,061
	2	47,490	0,267	26,027	0,569	22,314	10,617	[illegible]		48,450	[illegible]	[illegible]	0,001	51,500	[illegible]	0,079	0,000
	3	0,261	47,650	20,792	22,021	0,278	1,453	16,290	48,410		19,340	10,240	51,480	0,000	20,500	0,014	0,000
	4	0,271	0,204	4,914	1,766	0,975	0,145	48,940	[illegible]	18,960		40,140	[illegible]	20,510	0,001	0,471	0,000
SEC	1	0,188	1,303	0,792	21,278	21,248	49,870	0,018	[illegible]	9,104	48,870		[illegible]	9,898	45,510	0,030	0,055
	2	46,640	0,257	25,929	0,566	22,239	10,461	[illegible]	0,020	47,500	[illegible]	[illegible]		50,980	[illegible]	0,059	0,064
	3	0,252	46,790	20,719	21,949	0,277	1,400	16,140	47,460	0,012	18,750	9,891	50,960		20,110	0,008	0,000
	4	0,263	0,199	10,878	2,690	1,143	0,362	56,350	[illegible]	18,770	0,001	45,510	[illegible]	20,120		0,247	0,000
RCV	1	0,053	0,024	1,373	0,126	0,018	0,018	0,030	0,049	0,014	0,333	0,030	0,049	0,018	0,026		0,004
	4	0,025	0,053	0,014	0,014	0,015	1,264	0,062	0,071	0,000	0,000	0,063	0,072	0,000	0,000	0,000	

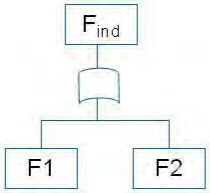
Critical cumulative failures : CCWS/ECCS, CCWS/AFWS and ECCS/AFWS : analysis must carry on.

EPR breakers step 3 : Consequence Analysis (2)

- A functional analysis : why ?
  - RAWC calculations are easily made at the train level and give evidence of train dependences.
    - → Grouping components of trains with important RAWC
  - **BUT** the biggest CCF group has not necessarily the biggest contribution : if grouping components functionally in series system, the result will be a risk decrease (see Barlow and Proschan, 1975)
    - → Avoid grouping components from trains "in series"

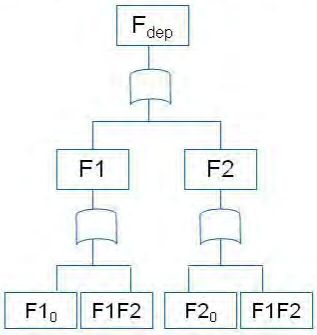
Step 3 : Consequence Analysis (3)

- Series system without dependency



$p(F_{ind}) = p(F1)+p(F2)$

- Series system with dependency



$P(F_{dep}) = p(F1_0)+p(F2_0)+p(F1F2)$

$p(F1) = p(F1_0)+p(F1F2)$

$p(F2) = p(F2_0)+p(F1F2)$

$\Rightarrow P(F_{dep}) = p(F1)+p(F2_0) < p(F_{ind})$

Step 3 : Consequence Analysis (4)

- For EPR 10kV Breakers, 12 inter system CCF Groups identified
- The most significant risk increase (~1 %) obtained for 5 CCF Groups modeled together:
  - Three groups of 8 breakers for short circuit, failure to run, and spurious opening modes on LH switchboard. They concern the incoming lines from LGA/B/C/D switchboards and from the diesel generators.
  - One group of 4 breakers for the failure to close mode on LH switchboards. They concern the incoming lines LG switchboards and from the diesel generators.
  - One group of 4 breakers for the failure to open mode on LH switchboards. They concern the incoming lines to the LG switchboards and from the diesel generators.

FA3 Electrical cabinets installation

Conclusion

EDF

Small impact for the cases studied up to now

- 900MW Plants Pumps
  - No risk Impact
- 900MW Plants MOVs
  - Potential intersystem CCFs for some MOVs within ECCS, CVCS, CCWS and RHRS
    - Based on design & operation similarities
    - Existing events in operating feedback
    - Small risk impact (<2%) – the bigger impact relates to the group involving ECCS and CCWS MOVs
- EPR 10kV Breakers
  - Less than 1%

EDF

Thank you for your attention !