

Robustness of Electrical Systems of Nuclear Power Plants in Light of the Fukushima Daiichi Accident (ROBELSYS)

Workshop Proceedings
Paris, France
1-4 April 2014

Unclassified

NEA/CSNI/R(2015)4

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

12-Mar-2015

English text only

**NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS**

NEA/CSNI/R(2015)4
Unclassified

Robustness of Electrical Systems of NPP's in Light of the Fukushima Daiichi Accident

ROBELSYS Workshop Proceedings

OECD Conference Centre, Paris, France

1-4 April 2014

Organised in co-operation with the Institut de Radioprotection et de Sûreté Nucléaire

This document only exists in PDF.

JT03372214

Complete document available on OLIS in its original format

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The Organisation for Economic Co-operation and Development (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 31 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 Russian Federation, 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;
- 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 programme 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.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Corrigenda to OECD publications may be found online at: www.oecd.org/publishing/corrigenda.

© OECD 2015

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of the OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to rights@oecd.org. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Centre (CCC) at info@copyright.com or the Centre français d'exploitation du droit de copie (CFC) contact@cfcopies.com.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made of senior scientists and engineers, with broad responsibilities for safety technology and research programmes, as well as representatives from regulatory authorities. It was set up in 1973 to develop and co-ordinate the activities of the NEA concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations.

The committee's purpose is to foster international co-operation in nuclear safety among the NEA member countries. The CSNI's main tasks are to exchange technical information and to promote collaboration between research, development, engineering and regulatory organisations; to review operating experience and the state of knowledge on selected topics of nuclear safety technology and safety assessment; to initiate and conduct programmes to overcome discrepancies, develop improvements and research consensus on technical issues; and to promote the co-ordination of work that serves to maintain competence in nuclear safety matters, including the establishment of joint undertakings.

The clear priority of the committee is on the safety of nuclear installations and the design and construction of new reactors and installations. For advanced reactor designs the committee provides a forum for improving safety related knowledge and a vehicle for joint research.

In implementing its programme, the CSNI establishes co-operative mechanisms with the NEA's Committee on Nuclear Regulatory Activities (CNRA) which is responsible for the programme of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with the other NEA's Standing Committees as well as with key international organisations (e.g. the IAEA) on matters of common interest.

EXECUTIVE SUMMARY

The March 2011 accident at Fukushima Daiichi triggered discussions about the significance of electrical power hazards and their treatment in safety analyses. In order to address these issues and provide relevant conclusions and recommendations to CSNI and CNRA, the Robustness in Electrical Systems (ROBELSYS) Technical Working Group was established in 2012 under the leadership of the *Institut de Radioprotection et de Sûreté Nucléaire* (IRSN) of France. The purpose of the ROBELSYS Technical Working Group was to organize an international workshop to identify and discuss the lessons learned from the Fukushima Daiichi accident. The workshop was focused on the provisions taken by various countries concerning national requirements and modifications to the plant designs in order to enhance the robustness of electrical systems, especially the protection against extreme external hazards.

After convening several organizing meetings the ROBELSYS workshop was held at the OECD Conference Centre, 2 rue André Pascal, in Paris, France, April 1-4, 2014. A total of 105 participants attended the workshop representing industry and government organisations from 25 countries, as well as international organisations. A total of 34 technical presentations were given in seven sessions. Full copies of all the workshop presentations are available for download on the OECD Nuclear Energy Agency website.

At the end of each session, a panel session was held allowing for more detailed discussions on any of presentations in that session. On the last day, a general discussion session concluded the workshop.

Based on the discussions a strong interest for continuing efforts after this ROBELSYS workshop was expressed by the participants of the workshop, leading the task group to recommend launching a more permanent international working group.

The support to the identification of the need for new specific international standards was also recommended regarding: system and component requirements for beyond design basis external events, diversity in the onsite electrical power systems, relaxation of electric power protection features used in emergency situations, qualification of existing and portable components to cope with AC station blackout.

The following issues were highlighted by the participants as topics of concern which needed further development:

- Simulation of electrical transients in general and in particular of asymmetric 3-phase electrical faults (one/two-open-phase issue)
- Development of standardised transient voltage wave forms for use in the qualification process of onsite electrical equipment. (These wave forms may replace or supplement the currently used lightning and switching impulse test wave forms.)
- Reliability and robustness of new battery designs regarding SBO scenarios.

It was also noticed that it would be beneficial to continue information sharing with several other NEA working groups and in particular with the Working Group on Risk Assessment (WGRISK) of CSNI with which several topics for enhancing synergies have already been identified.

1. INTRODUCTION

1.1 Background

The Defence in Depth of Electrical Systems (DIDELSYS) Project (2008-2011) was launched after a switchyard-induced voltage surge event at Forsmark Nuclear Power Plant (NPP) in July 2006 which caused the loss of two out of four safety-related AC buses along with all connected I&C and support systems. The DIDELSYS Project was focused on providing recommendations to address internal plant and grid upset events and the ability to safely recover from these events. Due to the tsunami-induced AC and DC station blackout accident at Fukushima Daiichi a loss of power associated with severe external events which were beyond the scope of the DIDELSYS Project were identified. The Committee for the Safety of Nuclear Installations (CSNI) called a Senior Task Group on Robustness of Electrical Systems of NPPs in Light of the Fukushima Daiichi Accident (ROBELSYS) to evaluate the safety implications of severe external events on safety related electrical systems. The ROBELSYS task group is responsible for the committee's programme work in the area of improving the robustness of safety related electrical systems in nuclear power plants.

The main purpose of the ROBELSYS Project is to improve the robustness of nuclear power plant electrical systems and defence in depth by comparing design practices, plant emergency and operating procedures in member countries. Furthermore, the safety review process of nuclear power plant electrical systems can be improved by learning from best practices in member countries and the cooperation among member countries to improve safety can be promoted.

To deliver the aim of the task group, it was decided to convene a workshop at the OECD Conference Centre in Paris between 1st and 4th April 2014 where specialists from across the world could gather together to share their own country or company responses to the event.

1.2 Objectives of the Workshop

The main objective of this international workshop is to provide a forum to exchange information on simulation and design of safety related electrical systems in nuclear power plants. Key focus areas are:

- Simulation of the impacts of external events on NPP electrical systems and lessons learned from the Fukushima accident.
- Evaluations of the coping capability of existing NPP electrical systems and components for external events.
- Identification and simulation of limiting features such as batteries, switchgears and controllers.
- Design features to facilitate electrical system recovery from various types of AC station blackout scenarios.

1.3 Organisation of the Workshop

The workshop was organised into seven sessions as follows:

- SESSION 1: National Programmes on Evolution of Onsite and Offsite Electric Power Systems
- SESSION 2: Role of Electric Power in Severe Accident Management
- SESSION 3: Requirements for Robustness of Onsite Electric Power Systems
- SESSION 4: Simulation of Transients within NPP Plant Distribution Systems
- SESSION 5: Requirements for Equipment Used for Emergency Response
- SESSION 6: Margin Assessments for Modern Power Electronics
- SESSION 7: Digital Components in Power Systems

The detailed workshop agenda is provided in Appendix 2. The participation was open to experts from regulatory authorities and their technical support organisations, research organizations, utilities, NPP designers and vendors, industry associations and observers.

1.4 Topics of the Workshop

Items addressed in the workshop included:

- Review of the lessons learned from the Fukushima accident concerning the robustness of electrical systems
- Review of the provisions already taken or planned after the Fukushima accident, regarding the sources, the distribution systems and the loads, and documenting the technical basis for these improvements
- Review of the possibilities to connect sources very close to the loads
- Review of the protection of distribution systems against external hazards

2. SUMMARY OF THE WORKSHOP ROBUSTNESS OF ELECTRICAL SYSTEMS

The workshop included an opening session, seven sessions with participant presentations followed by short discussions, and a facilitated discussion session. The contributions presented were devoted to discussions of national post-Fukushima regulatory programme developments, methods to determine allowable coping time for electric power recovery, electric power system simulation methods development and benchmarking efforts, analysis of component capability, and approaches to facilitate electric power system recovery from extended loss of AC power.

2.1 Opening Session

The workshop was opened by the ROBELSYS Workshop Chair, Pascal REGNIER (IRSN). A keynote presentation was then held by Jacques REPUSSARD, IRSN Director General reminding the participants of the importance of improved understanding of the role of electric power and defence against external events in assuring nuclear safety in the world's operating NPPs. John BICKEL, the DIDEYSYS Working Group Chair, briefly discussed the history of the CSNI sponsored DIDEYSYS Project which originated as a follow-up investigation to the 2006 switchyard fault at Forsmark plant in Sweden. The scope of the DIDEYSYS project did not include consideration of external events such as earthquakes, tsunamis, or floods – and this required expansion in light of the experience at Fukushima Daiichi.

2.2 Session 1 - National Programmes on Evolution of Onsite and Offsite Electric Power Systems

This session was devoted to the programmes that many countries have engaged at the national level to strengthen the robustness of either onsite or offsite electrical power systems in NPPs.

The following papers were presented:

- TEMPORARY AND LONG TERM DESIGN PROVISIONS TAKEN ON THE FRENCH NPP FLEET TO COPE WITH EXTENDED STATION BLACK OUT IN CASE OF RARE AND SEVERE EXTERNAL EVENTS, *Patricia DUPUY, Carine DELAFOND, Alexandre DUBOIS (IRSN, France)*
- ELECTRICAL SYSTEM DESIGN APPLICATIONS ON JAPANESE BWR PLANTS IN THE LIGHT OF THE FUKUSHIMA ACCIDENT AND HITACHI EXPERIENCE OF THE SOLID STATE POWER EQUIPMENT IN JAPANESE BWR, *Masashi SUGIYAMA (HITACHI, Japan)*
- ELECTRIC POWER SUPPLY OF GERMAN NPPS: DEFENCE IN DEPTH, PROTECTION AGAINST EXTERNAL HAZARDS AND RETROFITTING AS A CONSEQUENCE OF THE FUKUSHIMA ACCIDENT, *Sebastian A. MEISS (BfS, Germany), Robert ARIANS (GRS, Germany)*

- ELECTRICAL SYSTEMS AT LAGUNA VERDE NUCLEAR POWER PLANT (LVNPP) AFTER THE FUKUSHIMA EVENT, *José Francisco LÓPEZ JIMÉNEZ* (CNSNS, Mexico)
- STATUS OF THE REVIEW OF ELECTRIC ITEMS IN SPAIN RELATED TO THE POST-FUKUSHIMA STRESS TEST PROGRAMME, *Manuel R. MARTINEZ MORENO and Alfonso PEREZ RODRIGUEZ* (CSN, Spain)
- EVOLUTION OF ONSITE AND OFFSITE POWER SYSTEMS IN US NUCLEAR POWER PLANTS, *Gurcharan MATHARU* (NRC, USA)

Many presenters described the electrical arrangements on their sites before the events and how they have been enhanced. They described the use of hardened structures to provide resilience for equipment against specific hazards. Others discussed the revision of national safety guidelines for essential systems to increase redundancy and segregation.

Amongst the various presentations the following common themes have emerged:

- European presenters talked about their activities in the EU Council Stress Test process, while those from outside Europe also described how they had taken the format and applied it to understand the ‘Robustness’ of their plants to extreme events.
- There is an increased acceptance that plants should have mechanisms to cope with extreme hazards that are well beyond the design basis.
- The general approach is that this should be achieved through supplemental mobile equipment
- Many speakers talked about enhancing battery autonomy through either upgrading battery systems and/or through load shedding.
- Key regulations applied by the U.S. Nuclear Regulatory Commission, i.e., United States Code of Federal Regulation 10 CFR Part 50 and its associated Regulatory Guides, are used by many countries. . It is not clear how the respective countries have considered their suitability in their country or for their own regulatory regime.
- There was a general consensus that installed backup equipment to mitigate a specific design basis, such as flooding or seismic, should be resilient against the design basis event plus a suitable margin. Furthermore, that margin needs to be based on individual plant knowledge and judgment. This could be considered as Design Extension improvements.

Regarding the differences between national approaches, various speakers discussed the use of onsite hardened facilities to store supplemental emergency equipment. Other speakers described the use of offsite locations, using distance as a mitigation to the hazard and to minimize the occurrence of common cause failures.

It was also observed that the various speakers used the phrases: Loss of offsite power (LOOP), Station Blackout (SBO) and “extended SBO” with different meanings which would deserve some reflections and possibly harmonization in order to prevent confusions and misunderstandings.

It was noted that France, UK and USA are implementing rapid response teams with cached supplies (portable generators, quick connect cables, fuel and compressed nitrogen supplies) that can be deployed to bring offsite support in the case of an emergency.

At the end of the discussion, it was noted that while speakers talked about providing additional permanent or temporary generators there was little information on any enhancements being made to “switchboards” or the rest of the electrical infrastructure that could be the weak points in case of beyond design events.

It was also unclear how DC system load shedding would be achieved in practice especially where personnel switching was required.

Recommendations:

- Plants should have mechanisms to cope with extreme hazards that are well beyond the design basis.
- Enhancing battery autonomy through either upgrading battery systems and/or through load shedding should be considered.
- The meaning of the phrases “LOOP”, “SBO” and “extended SBO” should be harmonised.
- Enhancement of the robustness of electrical systems in NPPs should not solely focus on additional generators but also consider enhancement on switchboards and on the rest of the electrical infrastructure.

2.3 Session 2 - Role of Electric Power in Severe Accident Management

This session was devoted to the role which electric power plays in the prevention of severe accidents for different reactor types, and the time available to recover electric power to prevent different levels of severe accidents.

The following papers were presented:

- IMPLICATIONS OF EXTENSION OF STATION BLACKOUT COPING CAPABILITY ON NUCLEAR POWER PLANT SAFETY, *Andrija VOLKANOVSKI* (JSI, Slovenia)
- DC LEAD ACID BATTERIES IN NPP, PRESENT AND FUTURE SOLUTIONS, *Gery BONDUELLE* (ENERSYS, Sweden)
- CH-SOLUTIONS FOR PROVIDING ELECTRICAL POWER IN CASES OF LONG TERM BLACK OUT OF THE GRID, Franz ALTKIND, *Daniel SCHMID* (ENSI, Switzerland)
- STRENGTHENING THE FIRST LINE OF DEFENCE: KEEP TURBINE RUNNING AT SCRAM, *Marcel VAN BERLO* (KFD, The Netherlands)

Based on a US assessment during the last three years, six of the seven most important accident sequence precursors in US NPPs were caused by multiple electrical related failures. Improving existing electrical systems to prevent severe accidents may be even more important to improve the overall robustness of electrical systems than to install additional systems to mitigate severe accidents

The vulnerability of the grid was illustrated by pictures of the damage done to the 400kV grid by an ice storm last winter in Slovenia. An extra 400kV line that was recently installed prevented the LOOP for the Krsko plant.

The use of probabilistic safety analysis (PSA) was presented to evaluate a solution for improving safety by adding diesel generators and/or batteries under some consideration of diversity.

Electrical batteries are important for addressing the coping time in SBO condition. An overview of different types of batteries with their pros and cons was given. Today, lead acid type still seems to be the most reliable technology. More information on common cause failures of batteries can be found on the NEA website: ICDE PROJECT REPORT: COLLECTION AND ANALYSIS OF COMMON-CAUSE FAILURES OF BATTERIES, September 2003, NEA/CSNI/R(2003)19.

Although not presented during the workshop, the Swiss paper described their 7 layers of defence in depth of electrical power supply. The last layer consists of mobile generators available at a central storage. Procedures are in place allowing shift operators to operate the ultimate emergency equipment.

A proposal was made to use the turbine and main generator after scram (when connected to the grid) with an adapted pressure control system instead of dumping the steam to the condenser and/or the atmosphere. This could possibly lead to a smoothing of the transient and the use of auxiliary feed water and diesel generator power supply could be delayed. This proposal led to a lot of discussion where most of participants disagreed based on fundamental safety considerations.

Recommendations:

- Given the evolution of battery technology it could be worthwhile to explore the reliability and robustness of new battery designs. The ICDE project report is covering the period up to the year 2000 and could be updated.
- Further investigation on the use of PSA to improve insights in the role of different electrical power sources in reduction of core damage frequency (CDF) or mitigation of severe accidents.
- Further investigation to determine the available coping time in case of SBO to know the time in which critical functions are to be restored to prevent a severe accident.

2.4 Session 3 - Requirements for Robustness of Onsite Electric Power Systems

This session was devoted to the postulated environmental conditions due to extreme external events, for example, seismic aftershocks, continuous ice storm, continuous flooding, and so on, which should be considered in the specifications of the countermeasures or robustness.

The following papers were presented:

- ELECTRICAL SYSTEM'S DESIGN APPLICATIONS ON JAPANESE PWR PLANTS IN LIGHT OF THE FUKUSHIMA ACCIDENT, *Tsutomu NOMOTO* (MHI, Japan)
- EFFECTS OF COMMON CAUSE FAILURE ON ELECTRICAL SYSTEMS, *Kevin PEPPER* (ONR, UK)
- A SURVEY OF THE HAZARDS TO ELECTRICAL POWER SYSTEMS, *Gary JOHNSON* (USA)

- MODERNIZATION OF UNIT 2 – MAIN OBJECTIVES, EXPERIENCE FROM DESIGN, SEPARATION OF OPERATIONAL AND NUCLEAR SAFETY EQUIPMENT – LESSONS LEARNED, *Salah KANAAN* (E.ON/OKG, Sweden)
- RCC-E A DESIGN CODE FOR I&C AND ELECTRICAL SYSTEMS, *Jean-Michel HAURE* (EDF, France)
- OVERALL STRATEGY AND ARCHITECTURE FOR POST-FUKUSHIMA-MITIGATION AND MITIGATION ON OTHER EVENTS IN THE ELECTRICAL SYSTEM, *Waldemar GEISSLER* (AREVA, Germany)
- COMPARISON BETWEEN DIFFERENT POWER SOURCES FOR EMERGENCY POWER SUPPLY AT NUCLEAR POWER PLANTS, *Magnus LENASSON* (Solvina/AB/Sweden)
- ADVANCING RUGGEDNESS OF NUCLEAR STATIONS BY EXPANDING DEFENCE IN DEPTH IN CRITICAL AREAS, *Thomas KOSHY* (IAEA)

The purpose of this session was to share the technical information relevant for requirements on equipment, components or systems which are established or planned to be established as countermeasures for an SBO.

In addition, it was intended as an opportunity to share lessons learned from several electrical failures in past.

The most significant discussions in this session were the following:

- How to establish the requirements against beyond design basis external events (e.g. flooding, seismic, ice storm)
- Necessity of diversity for the electrical distribution system
- Safety and qualification requirements to the SBO countermeasure systems
- Continuous discussion and information sharing on the one/two-open-phase issue.

Recommendations

Through the discussion, it was found that there are still undefined areas related to electrical systems. It will be very beneficial for all members to continue sharing the information on following items:

- Requirements for addressing beyond design basis external events
- Scope of diversity in electrical systems
- Qualification requirements to systems used to cope with AC station blackout
- Asymmetric 3-phase faults (one/two-open-phase issue).

2.5 Session 4 - Simulation of Transients within NPP Plant Distribution Systems

This session was devoted to the methods and simulation tools used to predict the performance of components and systems in NPP electrical distribution systems and their ability to withstand internal and external hazards that challenge the ability to maintain safety margins.

The following papers were presented:

- VERIFICATION OF SIMULATION TOOLS, *Thierry RICHARD* (EDF, France)
- STANDARD PROCEDURE FOR GRID INTERACTION ANALYSIS, *Bertil SVENSSON, Sture LINDAHL, Daniel KARLSSON* (Gothia Power AB, Sweden), *Jonas JÖNSSON, Fredrik HEYMAN* (OKG AB, Sweden)
- ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK, *Per LAMELL* (Vattenfall, Sweden)
- INTRODUCTION OF ELECTRICAL SYSTEM SIMULATION ANALYSIS USED IN KOREAN NUCLEAR POWER PLANT, *Sang Hak KIM* (KEPCO, Korea)
- COMPUTER SIMULATION OF COMPLEX POWER SYSTEM FAULTS UNDER VARIOUS OPERATING CONDITIONS, *Tanuj KHANDELWAL, Cedric BAYLE* (ETAP, France)

The objective of this session was to focus on the methods and simulation tools used to:

- predict the performance of systems and components of the power distribution of NPPs,
- assess their ability to withstand internal and external hazards that could jeopardise the safety margins.

The presentations dealt with simulation tools and their use in slow transient studies of electrical distribution systems in NPPs (including electrical auxiliaries). None of the presentations dealt with fast transient phenomena studies (such as lightning).

A validation and verification process (V & V) of simulation tools used to support the demonstration of nuclear safety studies was also presented.

A focus was made on the importance of the main user of a simulation tool and his scope and missions in:

- the process of functional validation of the software,
- training for inexperienced users,
- maintaining the qualification,
- qualification of new versions.

The required input data and methods and hypothesis used for these studies were also presented. Although the presenting countries have their own specific adaptations, methodologies for slow transients and current calculations of short circuit are close in terms of philosophy.

Based on feedback events observed on the grid and on Swedish NPPs, 13 different profiles (initiating events) were introduced based on the following characteristics:

- Three-phase or single-phase fault, solid or resistant, near or far
- Surge and slow or rapid voltage collapse
- Under-frequency.

A focus on the various events taken place at Forsmark NPP and studies used to validate its basic design were also presented. The results of these studies allowed to plan design changes and improve the robustness of the electrical systems in Swedish NPPs.

Depending on the operating condition of the unit (plant start-up, normal operation, loss of coolant accident, hot standby, cold shutdown, loss of offsite power and station blackout.) and the availability of electrical sources (internal or external), different power balances were presented for Korean plants.

Different case studies included in the design were defined in a summary table through a combination of load cases (power balance) and the availability of the power source.

To confirm the validity of simulation results, comparisons were made with the results of tests carried out on site.

Finally, based on the case study of open phase conditions (Byron 2), a presentation was made:

- on the modifications applied to a simulation tool to take into account the asymmetrical aspects,
- on the validation and verification process, based on an inter-comparison between two simulation tools including one already considered as qualified.

The discussions and exchanges also highlighted the fact that no benchmarking of simulation tools has been made.

However, a format for the input data now exists and is gradually integrated into different simulation tools, which should ultimately facilitate inter-comparisons between tools.

Some simulation tools have important data libraries. However, the use of such libraries requires careful verification that the characteristics of the plant equipment match those of the library components.

To conclude, most participants agree on the following facts:

- Single simulation tool cannot be used to perform all studies (including fast and slow transient studies). Indeed, the models used are different as well as the necessary input data.
- Simulation tools used for the studies supporting the safety case must be qualified and users properly trained and supervised.
- Models representing the components of a single-line diagram must be representative for the studied phenomena and should be adapted to the types of studies.

For example, for the bus transfer studies all buses (HV and LV) and transformers should be represented.

The future studies to perform mainly concern asymmetric faults and:

- their detection,
- the behavior of the NPP auxiliaries,
- the means and logics which have to be implemented in order to identify them and cope with their consequences.

Recommendations:

Based upon the panel discussion at the end of the session a number of participants inquired about the further efforts after the ROBELSYS workshop and particularly the importance of launching an international working group on simulation tools and methods related to this type of studies.

2.6 Session 5 - Requirements for Equipment Used for Emergency Response

This session was devoted to the requirements for equipment used for emergency response in case of loss of electrical power in NPPs. It addresses requirements on new equipment, whether fixed or mobile, as well as requirements to facilitate rapid connection to existing equipment.

The following papers were presented:

- DESIGN PROVISIONS FOR STATION BLACKOUT AT NUCLEAR POWER PLANTS, THE IAEA TECDOC, Alexander DUCHAC (IAEA)
- TIMING CRITERIA FOR SUPPLEMENTAL EMERGENCY RESPONSE EQUIPMENT, John H. BICKEL (ESRT, USA)
- RESILIENCE IMPROVEMENTS TO UK NUCLEAR POWER PLANTS, Kevin PEPPER (ONR, UK)
- EMERGENCY MITIGATING EQUIPMENTS – POST FUKUSHIMA ACTIONS AT CANADIAN NUCLEAR POWER PLANTS PORTABLE AC POWER SOURCES, Jasmina VUCETIC, Ram KAMESWARAN and Krishnan RAMASWAMY (CNSC, Canada)
- FUNDAMENTAL DESIGN BASES FOR INDEPENDENT CORE COOLING SYSTEM, Jan HANBERG (SSM, Sweden)
- ULTIMATE ELECTRICAL MEANS FOR SEVERE ACCIDENT AND MULTI UNIT EVENT MANAGEMENT, Xavier Hubert Rene GUISEZ (Electrabel, Belgium)

The first paper dealt with the already observed need to harmonise some basic definitions regarding electrical systems, starting with the definition of SBO (station blackout). It presented the motivation and current status of an IAEA technical document (Tecdoc) dedicated to SBO topic which should be published in June 2015.

The following papers gave some feedback on studies and solutions implemented for emergency response equipment for specific NPPs. The presentations and the associated discussions lead to the general following remarks:

- The decision if supplement response equipment should be stored on site or in remote response centres requires specific studies to establish the coping time. An example of such a study involving computations on 80 scenarios and sensitivity studies was presented confirming that the envisioned on site supplemental equipment (with adequate fuel and compressed Nitrogen gas storages) would be

sufficient to prevent fuel damage even beyond the 24 h delay to have remote equipment brought to the site.

- Improving the resilience of NPPs to SBO can be achieved through a significant enhancement of the battery capacity (i.e. 40 min to 8 hours). This can be done by augmenting the battery capacity and sometimes using load shedding. Additional mobile diesel generators are also currently installed on many sites worldwide.
- Implementation of an independent core cooling system is also sometimes considered.
- Improving the resilience of NPPs to SBO is, however, not only having more diesel generators but rather the ability to supply power through the distribution and down to the safety actuators. This leads to the need to explore solutions such as suitable event qualified connection points and making prime-mover-driver generators and pumps self-sufficient (i.e., not requiring shared support systems). Additional specific requirements for emergency response systems may also include qualification to extreme seismic events, proper initial and periodic testing as well as dedicated procedures.
- Limiting the size (and hence the power) of emergency response equipment should be considered as it leads to equipment which is more likely to be self-sufficient and capable of being moved, installed, and started up by hand.
- Emergency equipment is meant to operate when no other equipment may be operable. Hence, it may be better to relax the types and/or thresholds of the electrical protections in order to favour operation of the loads versus electrical protection (in particular not implementing overvoltage protections). The extent to which the electrical protection could be relaxed was debated.

Recommendations:

- Further investigations are needed to develop more internationally consistent requirements for emergency response equipment.
- Further investigations are needed to explore which types of electrical protection feature requirements could be relaxed for emergency equipment.

2.7 Session 6 – Margin Assessments for Modern Power Electronics

This session was devoted to the safety implications and design margins associated with modern solid state power electronics used in applications such as battery charger/inverter units and main generator excitation systems. It is motivated by the increasing number of applications of modern electrical systems important to safety making use of power electronics, e.g. thyristors and IGBTs. More precisely, recent operating experience in NPP's, e.g. IAEA IRS #7788 and #8294, has revealed that the design margins that should have been applied to deal with uncertainties in the real stress values and the equipment capability were inadequate.

The following papers were presented:

- RECENT OPERATING EXPERIENCE INVOLVING POWER ELECTRONICS FAILURE IN KOREAN NUCLEAR POWER PLANTS, *Jaedo LEE* (KINS, Korea)

- HOW TO SECURE UPS OPERATION AND SUPPLY OF SAFETY CRITICAL LOAD DURING ABNORMAL CONDITIONS IN UPSTREAM SUPPLY, *Joerg LAASER* (GUTOR, Switzerland)
- MODIFICATION TO BATTERY CHARGERS INVERTERS UNITS, *Florent RAISON* (AEG, France)

The technology of power electronic systems and components is still evolving. Functionality gets more complex and ratings of devices are increased. Design and knowledge of the design basis should be transparent for both manufacturers and customers so that systems can be designed and maintained with sufficient margins for electric transients and ageing.

Power electronics are susceptible to transients, both to power-frequency over voltages and switching and lightning impulse voltages. A knowledge gap between what the equipment is subjected to in the real world and what it is designed to endure still exists. This gap continues to represent a risk factor in reactor safety as many safety features are dependent on power electronics.

In order to combat this risk further work has to be done in several fields. The session identified the following items:

- strengthened design basis,
- improved standards for testing,
- diagnostics for transients,
- knowledge on ageing effects on silicon-controlled rectifiers (SCR) and
- improved knowledge through fault reports and statistics.

The session also identified that there is some customer reluctance to implement software based power electronics in safety grade systems. However, this seems not to be driven by failure statistics but rather on the issues of qualification, design knowledge, maintenance knowledge and obsolescence.

Hence, a life time perspective has to be included in the design (e.g. software lifecycle).

The presentations and associated discussions lead to the following findings:

- There are aging effects on SCRs (including device types of Thyristors, gate turn-off thyristors, and insulated-gate bipolar transistor) used in power electronics such as rectifiers, inverters and variable speed drives. Some manufacturers' claim long life time for such devices. However, further knowledge has to be gathered to support these claims.
- The measuring of the status and possible degradation on devices is not easily done. Simple measurement of impedance and insulation status is not sufficient. The devices have to be measured under load conditions (with current) based on the supplier's recommendation, in order to provide information for a correct assessment.
- Power electronics are susceptible to transients, both to power-frequency over voltages and switching and lightning impulse voltages. The problems of power-frequency over voltages have been discussed extensively in the DIDELSYS workshop. Impulse voltage is normally attenuated by surge arresters close to the source but harmful residues of the impulse may travel down as a travelling wave into the medium and low voltage systems hitting power electronics. Further modelling of voltage transient phenomena has to be developed. Over voltage protection (e.g. arresters) are recommended also at medium and low voltage systems and at sensitive components (e.g. power electronics). There is a need

for developing improved standards for testing power electronics against power-frequency over voltages and switching and lightning impulse voltages.

- Power distribution systems often lack instrumentation capable of verifying fast electrical transients. The real over voltages to which these power electronics are subjected to can therefore not be recorded. Hence, neither errors in design assumptions nor possible degradation can be discovered. Suitable diagnostics have to be developed.
- The need for gathering more knowledge on power electronics from the failure reports collated by international bodies such as the Institute of Nuclear Power Operations (INPO) or IAEA International Reporting System (IRS) was identified.
- The technology of power electronic systems and components is still evolving. Functionality gets more complex and ratings are increasing. There is a great interest and need for improving power electronic systems and the knowledge of these systems, so that the systems can be designed and maintained with sufficient margins for electric transients and ageing. A life time perspective has to be included in the design. The design and knowledge of the design basis should be transparent for both manufacturers and customers.
- Several customers have requested *software free* power electronics (e.g. containing no embedded microcontrollers and software). The drivers for this request focus on the issues (from the customer's perspective) on design knowledge, qualification, maintenance knowledge and obsolescence. However, there seems to be no failure statistics that indicate that software based power electronics have more problems than non-software based equipment.

Recommendations:

- A periodic replacement programme for SCRs should be considered, based on the manufacturers' recommendations.
- A proposal for new standardised transient voltage wave forms was suggested. These wave forms could replace or supplement the present lightning and switching impulse test wave forms used.
- The need for gathering more knowledge from failure reports on power electronics.

2.8 Session 7- Digital Components in Power Systems

This session was devoted to the current and foreseen use of digital components in electrical systems of NPPs, including operating experience, considerations for equipment selection, methods of qualification, and qualification issues.

The following papers were presented:

- DIGITAL COMPONENTS IN SWEDISH NPP POWER SYSTEMS, *Tage ERIKSSON et al.* (SSM, Sweden)
- OPERATING EXPERIENCE OF DIGITAL, SOFTWARE-BASED COMPONENTS USED IN I&C AND ELECTRICAL SYSTEMS IN GERMAN NPPS, *Stefanie BLUM, André LOCHTHOFEN, Claudia QUESTER, Robert ARIANS* (GRS, Germany)
- SMART DEVICES IN THE UK NUCLEAR SECTOR: A REGULATOR'S PERSPECTIVE, *Steve FROST* (ONR, UK)

- MASS ALARMS IN MAIN CONTROL ROOM CAUSED BY CONDENSATE ON THE INSTRUMENTATION AND CONTROL CARDS IN TURBINE BUILDING, *Cheol Soo GOO* (KINS, Korea)

This session had a consensus that digital components are increasingly replacing analogue devices for control and protection in electrical systems as it becomes more and more difficult to obtain components based upon analogue technology.

Digital components can provide increasing functionalities but show a higher level of complexity. Due to the more complex structure, digital components show the potential for new failure mechanisms and an increasing number of failure possibilities, including the potential for common cause failures. Failures in the electrical systems have been challenging to analyse, often due to a lack of detailed information about the systems, which has led to non-detectable, or non-identifiable, failure modes.

Operating experience has shown that the failures of digital components were mainly caused by parts which are not related to the software. Nevertheless, new failure mechanisms in digital components were identified (e.g. programming errors can have a major effect on the system). Due to the increased complexity of digital components they will require a more thorough assessment than simple analogue technology.

Therefore, digital components need to be rigorously qualified for their application depending on their safety significance. The qualification should also include the evaluation of the manufacturer's production of excellence and independent confidence building measures.

Recommendations:

- Digital components should be assessed in depth to gain further insight in failure mechanisms and failure possibilities.
- Digital components need to be rigorously qualified for their application depending on their safety significance.
- The qualification of digital components can be time consuming which should be taken into account when considering digital components for use in NPPs.
- When installing digital components, an appropriate design basis should be established. This should take into account possible new failure mechanisms as well as an understanding of component behaviour and sensitivities.
- In some circumstances the increased functionality and sensitivity or reduced response time of digital components can give the best overall solution for protection arrangements. For example phase unbalance may be difficult to measure accurately with analog devices.

3. CONCLUSIONS AND RECOMMENDATIONS

The following conclusions and recommendations are made based on workshop presentations, discussions during particular sessions, and facilitated discussions:

- Based upon the panel discussions at the end of the workshop, a majority of the participants suggested the need for continuing efforts after the ROBELSYS workshop and particularly the importance of launching a more permanent international working group on modeling tools and methods related to nuclear power plant electrical power system studies. The working group would be modelled on WGRISK. (It is recognized that creating such a permanent working group would require a multi-year commitment of CSNI and the participants.)
- It will be very beneficial to continue international information sharing of the following items, eventually leading to development of suitable international electrical standards:
 - System and component requirements for addressing beyond design basis external events
 - Recommended practice for incorporating diversity in the onsite electrical power system
 - Recommended practice for relaxing electric power protection features used in emergency situations (assuring margin against spurious electrical shutdowns)
 - Recommended practice for qualification requirements for existing systems and portable components used to cope with AC station blackout.
- There is a need for further development and improvements in the analysis and simulation of the following:
 - Simulation of asymmetric 3-phase electrical faults (one/two-open-phase issue)
 - Development of standardised transient voltage wave forms for use in qualifying onsite electric system components. (These wave forms could replace or supplement the present lightning and switching impulse test wave forms used.)
 - Reliability and robustness of new battery designs relied upon in SBO scenarios
- In coordination with WGRISK the following developments in PSA modeling should be given priority for improvement:
 - Investigation on the use of PSA tools to improve insights in the role of different electrical power sources in reduction of CDF or mitigation of severe accidents
 - Improved and consistent methods to determine the available coping time in case of SBO to know the time in which critical functions are to be restored to prevent a severe accident (to be done also in coordination with the CSNI Working Group on Analysis and Management of Accidents (WGAMA)).

APPENDIX 1
WORKSHOP PROGRAMME

TUESDAY, 1 April 2014

08:00 – 10:00 Registration of the participants

10:00 OPENING SESSION

Session chaired by *Pascal REGNIER – Workshop Chair (IRSN, France)*

10:05/0.01 **NEA WELCOME AND REMARKS**
Andrew White, NEA Nuclear Safety Division

10:15/0.02 **IRSN WELCOME AND REMARKS**
Jacques Repussard, IRSN Director General

10:30/0.03 **SEMINAR ORGANISATION & LOGISTICS**
NEA Secretariat

10:40/0.04 **ROBELSYS WORKSHOP BACKGROUND, OBJECTIVES, SCOPE, GOALS**
John Bickel (*Evergreen Safety & Reliability Technologies, USA*)

**Session 1 NATIONAL PROGRAMMES ON EVOLUTION OF ONSITE
AND OFFSITE ELECTRIC POWER SYSTEMS**

11:00 Session chaired by *Kevin PEPPER (ONR, UK)*

11:05/1.01 **TEMPORARY AND LONG TERM DESIGN
PROVISIONS TAKEN ON THE FRENCH NPP FLEET TO COPE WITH
EXTENDED STATION BLACK OUT IN CASE OF RARE AND SEVERE
EXTERNAL EVENTS**

Patricia Dupuy, Carine Delafond, Alexandre Dubois (*IRSN, France*)

11:30/1.02 **ELECTRICAL SYSTEM DESIGN APPLICATIONS ON JAPANESE BWR PLANTS IN THE LIGHT OF THE FUKUSHIMA ACCIDENT AND HITACHI EXPERIENCE OF THE SOLID STATE POWER EQUIPMENT IN JAPANESE BWR**

Masashi Sugiyama (*Hitachi-GE Nuclear Energy, Japan*)

11:55/1.03 **ELECTRIC POWER SUPPLY OF GERMAN NPPS: DEFENCE IN DEPTH, PROTECTION AGAINST EXTERNAL HAZARDS AND RETROFITTING AS A CONSEQUENCE OF THE FUKUSHIMA ACCIDENT**

Sebastian A. Meiss (*BfS, Germany*), Robert Arians (*GRS, Germany*)

12:30 ***Lunch Break***

Session 1 NATIONAL PROGRAMMES ON EVOLUTION OF ONSITE AND OFFSITE ELECTRIC POWER SYSTEMS (*contd.*)

13:35/1.05 **ELECTRICAL SYSTEMS AT LAGUNA VERDE NUCLEAR POWER PLANT (LVNPP) AFTER THE FUKUSHIMA ACCIDENT**

José Francisco López Jiménez (*CNSNS, Mexico*)

14:00/1.06 **STATUS OF THE REVIEW OF ELECTRIC ITEMS IN SPAIN RELATED TO THE POST-FUKUSHIMA STRESS TEST PROGRAMME**

Manuel R. Martínez Moreno, Alfonso Pérez Rodríguez, (*CSN, Spain*)

14:25/1.07 **EVOLUTION OF ONSITE AND OFFSITE POWER SYSTEMS IN US NUCLEAR POWER PLANTS**

Roy Mathew (*NRC, USA*)

14:50 **PANEL SESSION 1**

Open discussion from the floor with all the presenters in the Session 1

15:05 ***Coffee Break***

**Session 2 ROLE OF ELECTRIC POWER IN SEVERE ACCIDENT
MANAGEMENT**

15:30 Chaired by *Andre VANDEWALLE (NSSS, Belgium)*

15:35/2.01 **IMPLICATIONS OF EXTENSION OF STATION BLACKOUT
COPINGCAPABILITY ON NUCLEAR POWER PLANT SAFETY**

Andrija Volkanovski (JSI, Slovenia)

16:00/2.02 **DC BATTERIES IN NPP, PRESENT AND FUTURE SOLUTIONS**

Gery Bonduelle (ENERSYS, Sweden)

16:25/2.03 **SWISS SOLUTIONS FOR PROVIDING ELECTRICAL POWER IN
CASES OF LONG-TERM BLACK-OUT OF THE GRID**

Franz Altkind, Daniel Schmid (ENSI, Switzerland)

16:50/2.04 **STRENGTHENING THE FIRST LINE OF DEFENCE: DELAYED
TURBINE TRIP AT SCRAM IN WESTINGHOUSE TYPE NPPS**

Marcel van Berlo (KFD, The Netherlands)

17:15 PANEL SESSION 2

Open discussion from the floor with all the presenters in the Session 2

17:35 **End of the First Day**

WEDNESDAY, 2 APRIL 2014

**Session 3 REQUIREMENTS FOR ROBUSTNESS OF ONSITE
ELECTRIC POWER SYSTEMS**

09:00 Session chaired by *Shinji KAWANAGO (MHI, Japan)*

09:05/3.01 **ELECTRICAL SYSTEMS DESIGN APPLICATIONS ON JAPANESE
PWR PLANTS IN LIGHT OF THE FUKUSHIMA DAIICHI ACCIDENT**

Tsutomu Nomoto (*MHI, Japan*)

09:30/3.02 **EFFECTS OF COMMON CAUSE FAILURE ON ELECTRICAL
SYSTEMS**

Kevin Pepper (*ONR, UK*)

09:55/3.03 **A SURVEY OF THE HAZARDS TO ELECTRICAL POWER SYSTEMS**

Gary Johnson (*Independent Consultant, USA*)

10:20/3.04 **MODERNIZATION OF UNIT 2 AT OSKARSHAMN NPP – MAIN
OBJECTIVES, EXPERIENCE FROM DESIGN, SEPARATION OF
OPERATIONAL AND NUCLEAR SAFETY EQUIPMENT – LESSONS
LEARNED**

Salah Kanaan (*E.ON/OKG, Sweden*)

10:45 *Coffee Break*

**Session 3 REQUIREMENTS FOR ROBUSTNESS OF ONSITE
ELECTRIC POWER SYSTEMS (*contd.*)**

11:15/3.05 **RCC-E A DESIGN CODE FOR I&C AND ELECTRICAL SYSTEMS**

Jean-Michel Haure (*EDF, France*)

11:40/3.06 **OVERALL STRATEGY AND ARCHITECTURE FOR POST-
FUKUSHIMA-MITIGATION AND MITIGATION ON OTHER EVENTS
IN THE ELECTRICAL SYSTEM**

Waldemar Geissler (*AREVA, Germany*)

12:05/3.07 **COMPARISON BETWEEN DIFFERENT POWER SOURCES FOR EMERGENCY POWER SUPPLY AT NUCLEAR POWER PLANTS**

Magnus Lenasson (*Solvina AB/Sweden*)

12:30/3.08 **ADVANCING RUGGEDNESS OF NUCLEAR STATIONS BY EXPANDING DEFENCE IN DEPTH IN CRITICAL AREAS**

Thomas Koshy (*IAEA*)

12:55 **PANEL SESSION 3**

Open discussion from the floor with all the presenters in the Session 3

13:15 *Lunch Break*

Session 4 SIMULATION OF TRANSIENTS WITHIN NPP PLANT DISTRIBUTION SYSTEMS

14:15 Session chaired by *Thierry-Victorin RICHARD (EDF, France)*

14:20/4.01 **VERIFICATION OF SIMULATION TOOLS**

Thierry Richard (*EDF, France*)

14:45/4.02 **STANDARD PROCEDURE FOR GRID INTERACTION ANALYSIS**

Bertil Svensson, Sture Lindahl, Daniel Karlsson (*Gothia Power AB, Sweden*),
Jonas Jönsson, Fredrik Heyman (*OKG AB, Sweden*)

15:10/4.03 **ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK**

Per Lamell (*Forsmarks Kraftgrupp AB, Sweden*)

15:35/4.05 **INTRODUCTION OF ELECTRICAL SYSTEM SIMULATION ANALYSIS USED IN KOREAN NUCLEAR POWER PLANT**

Sang Hak Kim, Woo Sung Jeong (*KEPCO, Korea*)

16:00 *Coffee Break*

Session 4 **SIMULATION OF TRANSIENTS WITHIN NPP PLANT
DISTRIBUTION SYSTEMS** (*contd.*)

16:30/4.06 **COMPUTER SIMULATION OF COMPLEX POWER SYSTEM FAULTS
UNDER VARIOUS OPERATING CONDITIONS**
Tanuj Khandelwal, Cedric Bayle (*ETAP, France*)

16:55 **PANEL SESSION 4**

Open discussion from the floor with all the presenters in the Session 4

17:35 **End of the Second Day**

THURSDAY, 3 APRIL 2014

**Session 5 REQUIREMENTS FOR EQUIPMENT USED
FOR EMERGENCY RESPONSE**

09:00 Session chaired by *Pascal REGNIER (IRSN, France)*

09:05/5.01 **DESIGN PROVISIONS FOR STATION BLACKOUT AT NUCLEAR
POWER PLANTS**

Alexander Duchac (*IAEA*)

09:30/5.02 **TIMING CRITERIA FOR SUPPLEMENTAL BWR EMERGENCY
RESPONSE EQUIPMENT**

John H. Bickel (*ESRT, USA*)

09:55/5.03 **RESILIENCE IMPROVEMENTS TO UK NUCLEAR POWER PLANTS**

Kevin Pepper (*ONR, UK*)

10:20/5.04 **EMERGENCY MITIGATING EQUIPMENTS – POST FUKUSHIMA
ACTIONS AT CANADIAN NUCLEAR POWER PLANTS – PORTABLE
AC POWER SOURCES**

Jasmina Vucetic, Ram Kameswaran (*CNSC, Canada*)

10:45 *Coffee Break*

**Session 5 REQUIREMENTS FOR EQUIPMENT USED
FOR EMERGENCY RESPONSE (*contd.*)**

11:15/5.05 **FUNDAMENTAL DESIGN BASES FOR INDEPENDENT CORE
COOLING IN SWEDISH NUCLEAR POWER REACTORS**

Tomas Jelinek (*SSM, Sweden*)

11:40/5.06 **ULTIMATE ELECTRICAL MEANS FOR SEVERE ACCIDENT AND
MULTI UNIT EVENT MANAGEMENT**

Xavier Hubert Rene Guisez (*Electrabel, Belgium*)

12:05 PANEL SESSION 5

Open discussion from the floor with all the presenters in the Session 5

12:30 Lunch Break**Session 6 MARGIN ASSESSMENTS FOR MODERN POWER ELECTRONICS**

13:30 Chaired by *Tage ERIKSSON (SSM, Sweden)*

13:35/6.01 **RECENT OPERATING EXPERIENCE INVOLVING POWER ELECTRONICS FAILURE IN KOREAN NUCLEAR POWER PLANTS**

Jaedo Lee (*KINS, Korea*)

14:00/6.03 **HOW TO SECURE UPS OPERATION AND SUPPLY OF SAFETY CRITICAL LOAD DURING ABNORMAL CONDITIONS IN UPSTREAM SUPPLY**

Gert Andersen, Silvan Kissling, Joerg Laaser (*GUTOR, Switzerland*)

14:25/6.04 **MODIFICATION TO BATTERY CHARGERS & INVERTERS UNITS**

Florent Raison (*AEG Power Solutions, Germany*)

14:50 PANEL SESSION 6

Open discussion from the floor with all the presenters in the Session 6

Others RELATED ACTIVITIES AT CSNI/WGRISK

15:35 **PROBABILISTIC SAFETY ASSESSMENT RELATING TO THE LOSS OF ELECTRICAL SOURCES**

Jeanne-Marie Lanore (*IRSN, France*)

16:00 **End of the Third Day**

FRIDAY, 4 APRIL 2014

Session 7 DIGITAL COMPONENTS IN POWER SYSTEMS

09:00 Chaired by *Gary JOHNSON (IEEE, USA)*

09:05/7.01 **DIGITAL COMPONENTS IN SWEDISH NPP POWER SYSTEMS**

Mattias Karlsson, Tage Eriksson (*SSM, Sweden*)

09:30/7.02 **OPERATING EXPERIENCE OF DIGITAL, SOFTWARE-BASED COMPONENTS USED IN I&C AND ELECTRICAL SYSTEMS IN GERMAN NPPS**

Stefanie Blum, André Lochthofen, Claudia Quester, Robert Arians (*GRS, Germany*)

09:55/7.03 **SMART DEVICES IN THE UK NUCLEAR SECTOR: A REGULATOR'S PERSPECTIVE**

Kevin Pepper *on behalf of Steve FROST (ONR, UK)*

10:20/7.04 **MASS ALARMS IN MAIN CONTROL ROOM CAUSED CONDENSATE ON THE INSTRUMENTATION AND CONTROL CARDS IN TURBINE BUILDING**

Cheol-Soo Goo (*KINS, Korea*)

10:45 **PANEL SESSION 7**

Open discussion from the floor with all the presenters in the Session 7

11:00 *Coffee Break*

11:30 **CONCLUDING SESSION**

Session chaired by *Pascal REGNIER – Workshop Chair (IRSN, France)* and co-chaired by *John BICKEL (ESRT, USA)*

- 11:35 **SESSION CHAIRS REMARKS, SUMMARY AND CONCLUSIONS**
Kevin Pepper, Andre Vandewalle, Shinji Kawanago, Thierry-Victorin Richard, Pascal Regnier, Tage Eriksson, Gary Johnson
- 12:10 **DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS**
- 13:00 **Closure of the Workshop.**

APPENDIX 2. PAPERS/PRESENTATIONS

OPENING SESSION

IRSN Welcome and Remarks

Jacques Repussard, IRSN Director General

ROBELSYS Workshop Background, Objectives, Scope, Goals

John Bickel (Evergreen Safety & Reliability Technologies, USA)



IRSN
INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Enhancing Nuclear Safety

ROBELSYS,
Welcoming remarks

AEN
NEA

Jacques REPUSSARD, Director General of IRSN



A Robust electrical system is of prime importance for the safety of NPPs (1/2)

■ Forsmark INES 2 event (July 2006)

- Sensitivity of internal electrical systems to:
 - External events,
 - Timing (transients/sequencing),
 - Latent faults/maintenance errors.
- Has triggered DIDEYSYS 1

■ FUKUSHIMA accident (March 2011)

- Sensitivity to extreme external hazards,
 - Wider questioning regarding the type and severity of events to consider.
- Has triggered many reviews (e.g. stress tests, ...) and ROBELSYS

A Robust electrical system is of prime importance for the safety of NPPs (2/2)

Lessons from reliability and PSA studies:

- Need to significantly rely on the external electrical power source (which is the most reliable but cannot be safety classified).
- In PSAs, the loss of electrical sources is the major contributing family to core melt frequency in most existing and new reactors.

→ Scenarios with extended loss of electrical power are being explored by PSAs.

→ OECD/CSNI/WGRISK has launched a specific task on PSA insights regarding the loss of electrical sources.

External sources are exposed to various and potentially extreme perturbations

Exceptional natural events affecting the grid infrastructure:

- Extreme T°, wind, (ice) storm, Flooding, earthquake, solar storms ...

Events causing potentially major electrical transients impacting NPPs:

- Lightning, Ferroresonance,
- Maintenance errors/ equipment failures on the grid,
- Intermittent power sources (renewable energies).


➤ Wide range of topics to address, experience showing that some of them deserve additional attention.

➤ Possible long term and "whole site" effects.


The electrical system within a NPP is a complex system

- CCF prone system: by nature current “irrigates” all the plant and hence may propagate failure(s).
- Reinforcing the robustness of electrical supplies is not just about bringing more diesel generators: electrical distribution to the loads matters!
- Global tendency to rely more and more on electrical actuation systems (compared to hydraulic/pneumatic) in new reactor designs as in avionics.
- Advent of the digital technology in electrical equipment.

- Emerging technical challenges ahead of us
- Computer Simulation will help.


ROBELSYS Welcoming remarks, J. Repussard - April 1st, 2014

5/6

International activities / Safety of electrical systems in NPPs



The diagram illustrates international activities from 2006 to 2014. Key events include the Forsmark incident (2006) and Fukushima accident (2011). Activities are categorized into Technical exchanges (AEN/NEA, DIDELSYS 1 & 2, ROBELSYS, WGRISK project), Safety Requirements (IAEA DS430, IAEA Tec Doc), and Standards (IEC, Dedicated IEC 45A WG).

- Internationally, the topic is finding its audience.

ROBELSYS Welcoming remarks, J. Repussard - April 1st, 2014

5/6

Robustness in Electrical Systems “ROBELSYS”

Workshop Sponsored by OECD Nuclear Energy Agency
Paris, France
April 1-4, 2014

Welcoming Remarks by
Dr. John H. Bickel
ESRT, LLC

Why We are here:

- Currently operating NPPs rely upon active cooling..... *which ultimately depends on AC power*
- Even NPPs using steam driven pumps still require electrical instruments..... *which ultimately depends on AC power*
- Remove **AC power long enough** nuclear safety is compromised

We are here this week to discuss:

- How **robust** are existing nuclear power plant electrical systems?
- What are **appropriate issues** to consider in AC power “robustness”?
- What can **reasonably be done** to improve AC power “robustness”?

Prior NEA Efforts on AC Power:

- July 2006 switchyard event at Forsmark NPP in Sweden
 - Forsmark BWRs utilize *all electric* decay heat removal systems
 - Event involved **voltage surge** not envisioned during power electronics modernization in 1990's
 - Voltage surge failed multiple battery chargers – inverter units
 - 2/4 diesels trains and AC power to decay heat removal disabled
 - Failed instrument buses lead to depressurization
- Joint CSNI/CNRA Working Group “DIDELSYS” - Defense in Depth of Electrical Systems and Grid Interaction formed
 - Working Group activities: April 2008 - December 2011
 - International Workshops held in May 2009, May 2011
 - DIDELSYS Working Group Report issued November 2009
 - DIDELSYS Technical Opinion Report issued

DIDELSYS recommendations

- **Reduce** NPP-grid interaction challenges to NPP electrical systems
 - Improve **Robustness of NPP electrical systems** to cope with grid, and internal NPP electrical faults should they occur
 - Improve NPP training, procedures, display capabilities to deal with degraded electrical systems
 - Improve **Coping Capability** of NPP to deal with NPP electrical power system failures
 - Improve **Capability to recover offsite grid** to support NPP electrical power systems
- DIDELSYS **did not address** issues associated with extreme external phenomena – such as seismic, tsunami*

Fukushima AC power issues

- Coping with total destruction of offsite grid – rather than momentary interruption
- Consideration of extreme external events capable of total destruction of NPP electrical systems
- Need to analyze available coping times for emergency response
- Need for supplemental emergency response equipment
 - Battery chargers, bottled N2 gas, portable pumps

ROBELSYS Charter

- Review lessons learned from Fukushima accident concerning robustness of electrical systems
 - Measures planned or already taken in OECD countries
 - Review possibilities to reconnect portable power close to loads
 - Review protection of distribution systems against external hazards
- Identify current analysis practices for NPP electrical systems
 - Simulation of AC and DC power transients
- Identify approaches/difficulties in fully testing NPP electrical systems



The ROBELSYS effort is important to safety
of operating and planned NPPs

So, Let's get to work !

SESSION ONE :

"National Programmes on Evolution of Onsite and Offsite Electric and Power Systems"

Temporary and Long Term Design Provisions Taken on the French NPP Fleet to Cope with Extended Station Black out in Case of Rare and Severe External Events

Patricia Dupuy, Carine Delafond, Alexandre Dubois (IRSN, France)

Electrical System Design Applications on Japanese BWR Plants in the Light of the Fukushima Accident and Hitachi Experience of the Solid State Power Equipment in Japanese BWR

Masashi Sugiyama (Hitachi-GE Nuclear Energy, Japan)

Electric Power Supply of German NPPS: Defence in Depth, Protection against External Hazards and Retrofitting as a Consequence of the Fukushima Accident

Sebastian A. Meiss (BjS, Germany), Robert Arians (GRS, Germany)

Electrical Systems at Laguna Verde Nuclear Power Plant (LVNPP) after the Fukushima Accident

José Francisco Lopez Jiménez (CNSNS, Mexico)

Status of the Review of Electric Items in Spain Related to the Post-Fukushima Stress Test Programme

Manuel R. Martinez Moreno, Alfonso Pérez Rodríguez (CSN, Spain)

Evolution of Onsite and Offsite Power Systems in US Nuclear Power Plants

Roy Matthew (NRC, USA)

Temporary and Long Term Design Provisions Taken on the French NPP Fleet to Cope with Extended Station Black out in case of Rare and Severe External Events

Patricia Dupuy, Carine Delafond, Alexandre Dubois
IRSN, France

Abstract

Following the events at Fukushima, the Institute for Radiological Protection and Nuclear Safety (IRSN) has been strongly involved in a series of reviews related to the robustness of French nuclear power plants in case of “rare and severe” external hazards. These reviews included in particular the “stress tests” performed in 2011 as required by the European Commission.

Those reviews, and the proposal made by EDF to reinforce NPPs robustness in such situation, led to the introduction of the concept of a hardened safety core (HSC) to avoid massive releases and prolonged effects in the environment in case of rare and severe natural hazards. This concept will be explained in the paper and the new specific electrical equipment as well as the interfaces with the existing electrical distribution required to implement this HSC will be explained.

As the detailed design, manufacturing and installation of the HSC in all NPP sites will take several years, temporary measures have been adopted. This paper will also present the electrical sources and the distribution related to those temporary measures.

The specific situation of the new built EPR reactor in Flamanville is also addressed.

Lastly, in complement to the above on-site design provisions, a Nuclear Rapid Response Force has been set up by EDF to bring off-site support to French NPPs in case of emergency. The paper will describe the type of electrical equipment to be delivered and the principle for distributing the electrical power to the required loads.

1. Provisions to cope with a loss of electrical supplies at French nuclear power plants and new issues raised by the Fukushima accident

Provisions were defined from the design stage of existing French Nuclear Power Plants (NPPs) to cope with a Loss Of Off-site Power (LOOP). They mainly consist of two emergency diesel generators (EDGs) per reactor, each being able to back-up one of the two redundant electrical trains in order to power supply the safety systems and thus ensure the safety functions. In case of a multiple failure situation corresponding to a total loss of all external and internal electrical sources (diesels unavailable), the steam generators can be fed by the turbine-driven pump of the auxiliary feed water system. Additional electrical diversified features have been implemented since the design stage to cope with such a situation: a turbine generator “LLS” supplying an electrical pump able to inject water to the seals of the coolant system pumps and supplying part of I&C and lighting in the rooms. Additional means were also settled to allow the recovery of electrical power sources in a short time (on-site gas turbine or diesel generator).

Other types of improvements have been defined on the occasion of periodic safety reassessments of French NPPs or in order to take into account the lessons learned from operating experience. Discussions since 2009 between the French NPPs’ operator (EDF), the Institute for Radiological Protection and Nuclear Safety (IRSN) and the French Nuclear Safety Authority (ASN) on the program for new improvements in the frame of a long term operation of French NPPs have pointed out the need to reinforce the provisions to cope with situations of total loss of all external and internal electrical sources (station black-out) or total Loss of the Ultimate Heat Sink (LUHS). The interest of these improvements initiated before 2011 has been reinforced by the Fukushima accident.

Regarding the robustness against natural hazards, safety equipment needed for design basis accidents are generally protected against design basis hazards, which is in particular the case for safety equipment required in case of a LOOP (e.g. diesel generators). Simultaneous occurrence of an external hazard with a multiple failures situation, such as the total loss of all electrical sources, was not systematically postulated. However, according to “defence-in-depth” and recognizing that both LOOP and LUHS of long duration are likely to be induced by some natural hazards, some equipment used to manage these situations are protected against some hazards. Equipment required in severe accidents are generally not designed to resist to natural hazards as it is considered that such hazards could not lead to core damage.

The Fukushima accident raised questions about the following issues for which further improvements were considered as necessary:

- Management of prolonged LOOP, LUHS or severe accident that may be induced by a natural hazard and affect all the site units (reactors and fuel pools),
- Behavior of a NPP in case of “beyond design” hazards or combinations of hazards not considered at the design stage or during periodic reviews,
- Emergency response for beyond design hazards affecting several units at a same site.

2. The French “Hardened Safety Core” concept

“Hardened Safety Core” objectives and principles

Following the “robustness analyses” (stress tests) performed by EDF for the French NPPs after the Fukushima accident and their reviews performed by IRSN, it was decided to increase the protection of these NPPs against extreme natural hazards by reinforcing some parts of the installations and implementing complementary equipment in order to limit the releases in case of beyond design hazards (earthquake, external flooding and natural hazards that may be combined with the previous) and in particular in case of a station blackout or a loss of the ultimate heat sink or a severe accident induced by these extreme hazards. This set of equipment is called the post-Fukushima “Hardened Safety Core” (HSC).

The preliminary proposals of the operator about the main objectives and principles were reviewed by IRSN in 2012. IRSN considered the following principles as satisfactory:

-HSC consisting of fixed Systems Structures and Components (SSCs) on each plant, with a sufficient autonomy to maintain the safety functions at least until off-site provisions are set in place, i.e. during 72 hours. Off-site resources will then be deployed to back up on-site equipment and to manage accidental situations in the long-term (e.g. human resources, mobile electrical supplies, pumps, fuel oil...). EDF is setting up a Nuclear Rapid Response Force (FARN) in this objective;

-HSC consisting of a limited number of SSCs resistant against the postulated extreme hazards and covering all reactor states. Discussions are still on-going in France to define the “beyond design basis hazards”, including associated characteristics, and the methodologies to design or verify HSC provisions.

The IRSN and ASN considered that efforts should be made by EDF in order to ensure that the HSC:

-prevents core melt in the postulated situations and allow cooling by the secondary circuit (when the primary circuit is pressurized). This objective has led EDF to modify the operating strategy and the safety functions initially defined for the HSC (namely, feed and bleed strategy, combined with the venting and filtration of the containment). Detailed definition of the HSC strategy and SSCs is in progress;

-is protected against the induced effects of the extreme external hazards (for example loads drops, internal fires or flooding, bursts), which is a rather difficult but important issue to be addressed.

Requirements for the “Hardened Safety Core”

On the operating NPPs, the HSC will include new provisions such as for example (please note that these are currently being defined): an ultimate diesel generator, ultimate means to fill the steam generators (feed water pump and tank), an ultimate make-up system to refill the ultimate feed water tank, the re-flooding water storage tank and the spent fuel pool, an additional pump to inject water into the primary circuit, dedicated ultimate I&C.

Even if it consists of new robust SSCs, the HSC will necessarily stand in interface with some existing SSCs (e.g. reactor coolant system and connected systems up to the first isolation components, steam generators, isolation devices of the containment...).

When assessing the preliminary principles applied to the HSC by EDF, IRSN insisted on the following key requirements to be considered:

-The existing SSCs in interface with the HSC should meet strong requirements in terms of resistance to extreme hazards (earthquake, flooding and all phenomena that can be linked to flooding, such as lightning, extreme winds, tornadoes) and their induced effects. IRSN also pointed out the interest for the HSC to withstand some other extreme hazards (air temperatures);

-Main SSCs of the HSC and their support (such as electrical distribution and switchgears for example) should be as far as possible:

- independent from the existing SSCs, to ensure that the HSC constitutes the expected ultimate line of defense and isn't affected by the potential failures that may occur on the other parts of the installation,
- diversified from the existing SSCs to limit the risks of common cause failures, notwithstanding the objective of sufficient reliability of new equipment;

-In addition, the implementation of the HSC functions should require limited local actions by the staff.

It has to be noticed that on the existing plants, implementation of significant design improvements such as HSC modifications should take into account some constraints such as the difficulties pointed out by the operator to set up additional equipment in some buildings or site areas (for example in the electrical rooms). Therefore, even if the definition of HSC results from generic analyses for all existing plants, its detailed definition and implementation may be adapted from one site to another.

One major point is to provide the SSCs of the HSC with a robust electrical supply, in any situation, especially in case of a station black-out induced by extreme natural hazards. This issue is presented in the next part.

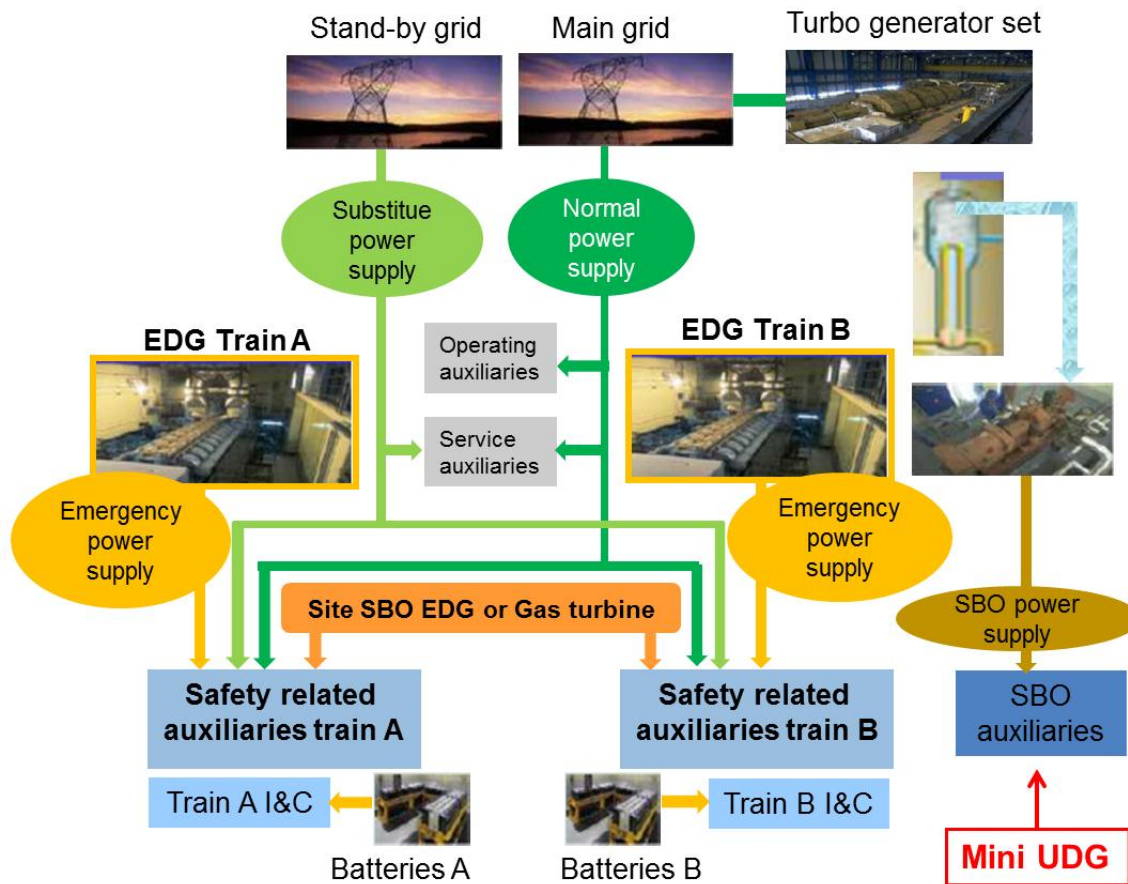
3. Main electrical improvements expected in the frame of the HSC

On French NPPs, each reactor is dotted with two emergency diesel generators (EDG), designed to supply 6.6 kV switchboards with power. These boards, called "LHA" and "LHB", are the electrical support of two redundant safety trains, namely A train and B train, as shown on Diagram 1.

In the frame of the HSC, an ultimate backup diesel generator (called "UDG") will be added on each operating plant to improve the mitigation of station black-out situations and to allow the mitigation of SBO induced by beyond design earthquake or external flooding. It must be noticed that given the timing of the industrial program of the HSC, a progressive deployment of this ultimate diesel generator and of the associated electrical distribution is scheduled.

This part shortly presents the safety objectives, the design principles and main functional characteristics of this UDG and of the associated electrical distribution as currently presented by the operator EDF. It should be noted that the design options may evolve. Moreover, even if the main principles of the HSC and of its support electrical equipment were analysed by IRSN in 2011-2012, the detailed design assumptions have not been examined by IRSN neither approved by ASN yet.

Diagram 1. Current electrical architecture on French PWRs: off site and on site power supply.



SSCs power supplied by the UDG:

Some SSCs will be power supplied by the UDG through an additional 6.6 kV switchboard called “LHC”, dedicated to the UDG.

In the short term, in order to enhance the mitigation of station black-out situations, some existing safety equipment will be power supplied by the UDG using the existing electrical distribution and an additional connection between an existing 6.6 kV switchboard and the new “LHC” switchboard. This will allow back-up power supply to some existing equipment necessary in a SBO situation such as the emergency feed water system, the minimum I&C, control room venting and lightening, some equipment necessary for the confinement function (containment isolation valves, annulus venting system, containment pressure measures...), provisions to refill the steam generators water tank, the re-flooding water storage tank and the spent fuel pool, a reactor make-up water pump, some measurements.

In the final step, a dedicated electrical architecture associated with the UDG will constitute the electrical support function of the HSC. Therefore, this electrical network will be part of the HSC and will be subject to the same stringent requirements. Following a SBO accident, power supply towards the HSC will thus be performed by the UDG. Next, in order to enhance the robustness of the system in duration,

external means brought by the Rapid Nuclear Response Force may be connected to the “LHC” switchboard.

Operating the UDG in extreme conditions:

A connection coming from normal or substitute power supply will provide in normal operating conditions the UDG auxiliaries (settled in the UDG building) with continuous power supply.

In extreme situations, the UDG and the associated ultimate electrical distribution will be activated and the power supplies of the necessary equipment will be switched from the normal sources to the ultimate ones.

It must be noted that in case of a SBO, the data requested to operate the damaged reactor unit are available by means of batteries. Therefore, these data will become no longer available in the control room after batteries depletion. In the aftermath of the Fukushima accident, IRSN and ASN requested that the autonomy of the batteries be enhanced. The operator asserted that the current safety-related batteries used in case of a SBO can generate autonomy higher than design autonomy of one hour which may enable automatic or manual switch to be carried out in order to restore power supply from UDG.

The UDG fuel oil autonomy is about 72 hours at full load, additional supplies being provided by the Rapid Nuclear Response Force.

Electrical architecture associated with the UDG:

In the final stage, the electrical architecture associated with the UDG will be characterized by the integration of voltage transformation means, transportation network and low voltage sources, for instance to provide the ultimate I&C with power. It will also include electrical connections towards all the new components of the HSC as well as towards some existing equipment also included in the HSC. IRSN emphasized the importance to get a dedicated electrical distribution network to ensure independency and thus limit the potential risks of common cause failure. It raises difficulties when it comes to ensure the switching of power sources for existing equipment. New provisions are needed in order to supply the existing components that are part of the HSC with power and to switch between normal power supply sources and those of the UDG. Following the conclusions of IRSN analysis of the HSC principles, the operator will look for a technological diversification as far as 6.6 kV switchboards are concerned.

Location of new electrical equipment:

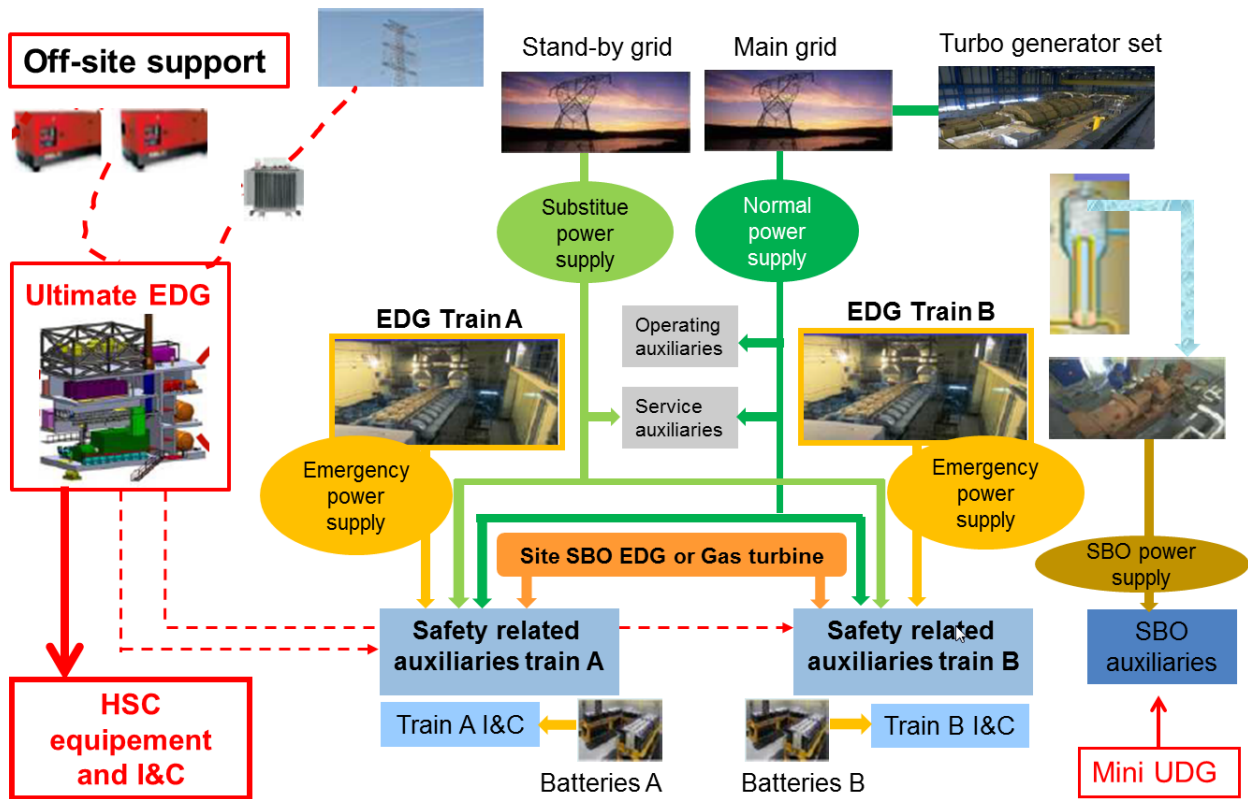
A new UDG building will be implemented and will include the base of the HSC electrical architecture, namely:

- the ultimate diesel generator UDG,
- the 6.6 kV switchboard "LHC",
- 380 V panel board feeding I&C of the UDG and the auxiliaries of UDG.

On many units, the local difficulties to settle the UDG building potentially result in a remote location from the nuclear island. Therefore, an additional electrical building closer to the HSC components will house the low voltage electrical distribution of the new equipment and of the ultimate I&C of the HSC.

The following diagram shows the future implementation scheduled for the UDG in the current electrical network on French NPPs.

Diagram 2. Future electrical architecture on French PWRs including Ultimate Diesel Generators.



Temporary measures

The future electrical network and ultimate diesel generator will be settled in several years' time. In the meantime some temporary measures are implemented as additional provisions to deal with a loss of external and internal power supplies.

In particular a small diesel generator (so called "Mini UDG") will enable to supply back-up power (by manual actuations) notably to the minimum I&C necessary in a SBO situation, the venting and the lightning in the control room and the annulus venting system (on 1300 and 1450 MWe reactor units). This diesel may also be rescued by the Rapid Nuclear Response Force by plugging a mobile device.

This small diesel generator is settled in a container located near the electrical building.

The Mini UDGs have already been installed on operating units (one per unit) and the dedicated electrical distributions will be finalized by 2016.

IRSN assessed that this new equipment didn't induce any loss of reliability for the unit.

4. The Nuclear Rapid Response Force: off-site support

The on-site fixed provisions aimed at managing the short-term phase after an extreme accident will be backed up by off-site means to be brought on site by a specialized emergency team called the “Nuclear Rapid Response Force”. Indeed, right after the first analysis of the Fukushima event, EDF decided to reinforce its national crisis organization, in particular by implementing national means, able to quickly provide a nuclear plant facing extreme conditions with human and equipment support.

The Nuclear Rapid Response Force will strengthen the overall national and local crisis and will be activated on the basis of an analysis of the situation. This team is expected to be operational within 24 hours on a site facing an extreme accident. To define this team, the operator assumed that only one site (out of the 19 French NPPs) faces a severe accident, having caused major destruction of the infrastructures (including the access to the site), full or partial unavailability of local teams (current shift teams, on-call emergency staff). The team would be able to work in severe environment, facing radiological and/or chemical hazards.

The Nuclear Rapid Response Force’s purpose will be to re-supply water, power and air, by means of mobile devices used within the first 24 hours or extra heavy equipment which could be brought afterwards (mobile emergency diesel generators, mobile motor-pump....). Thus, hook up points will be settled on existing plants to allow these operations.

IRSN and ASN considered this ultimate Nuclear Rapid Response Force as a satisfactory organizational improvement in addition to the fixed features of the HSC.

5. Future European Pressurized Reactor (EPR)

IRSN safety assessment of the detailed design of EPR Flamanville safety systems is in progress. Anyhow, in comparison with the operating reactors, the design of the EPR differs in terms of prevention of situations involving total loss of power supply or heat sink. At this stage, its design notably includes four main emergency diesel generators and two ultimate diesel generators (called “SBO diesels”) that could power supply some key safety systems and that should be independent and diversified from the four main diesel generators. It also includes an alternative heat sink in addition to the main one. Moreover, provisions have been defined since the design stage of the EPR for the mitigation of severe accidents. Finally, it is also considered that EPR Flamanville is better protected against external hazards such as earthquake (there being a common basement for the whole nuclear island, for example) and flooding (the location of the platform taking into account changes of the sea level up to the year 2080).

Nevertheless, some improvements of the design of this reactor are under analysis in order to limit the risk of beyond design hazards or situations. IRSN considered in particular that improvements should be studied by EDF in order to increase the autonomy of systems in case of prolonged loss of external power supply and all the diesel generators and/or total loss of heat sink due to extreme hazards affecting the whole Flamanville site (the EPR plant and the two PWR units in operation).

Some potential improvements are under study, such as:


- Provisions to increase the fuel oil autonomy of the SBO diesel generators (currently limited to 24 hours) by means of an additional pump to transfer the fuel oil from the EDG fuel tanks to the SBO diesels tanks,

- Provisions to increase the secondary water tanks autonomy by filling the tanks with the water reserve located on the top of the cliff,
- Extension from 12 hours to 24 hours of the autonomy of the “severe accident batteries”,
- Additional features to remove the heat from the containment in case of a prolonged loss of external power supply and all EDGs where the containment heat removal system is unavailable, and thus increase the available time for power recovery before containment damage,
- Some reinforcements of the protection of particular equipment against extreme hazards.

ASN requested the operator to provide, in the frame of the application for EPR Flamanville commissioning expected in the near future, justifications on the reliability of the electrical sources and distribution, and of the I&C in case of extreme situations.

Moreover, the EPR plant would take benefit in case of an extreme accident of the development of the EDF “Nuclear Rapid Response Force”.

- - -




Institut
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Enhancing Nuclear Safety

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs
in Light of the Fukushima Daiichi Accident**
April 1-4, 2014

**Temporary and Long Term Design Provisions Taken on the
French NPP Fleet to Cope with Extended Station Black out in
case of Rare and Severe External Events**

Patricia Dupuy, Carine Delafond, Alexandre Dubois
IRSN



Context

- Accident at Fukushima Daiichi has raised major concerns about:
 - Resistance of nuclear plants against extreme natural hazards
 - Multi-units accidents (reactors and spent fuel pools) of long duration
 - Emergency plans in case of multi-units accidents and extreme hazards



■ Which improvements taken for the French plants considering the lessons-learnt from Fukushima, in particular to strengthen the electrical systems?

ROBELSYS Workshop - April 1-4, 2014



2

Context

The French Nuclear Power Plants (NPPs):

- 58 PWR reactors in operation
- A very homogeneous operating fleet:
3 series of 900, 1300 and 1450 MWe
- One EPR reactor (PWR GEN III) under construction at Flamanville
- All NPPs operated by a single utility:
Electricité de France (EDF)

■ Réacteur du palier 900 MWe
▲ Réacteur du palier 1300 MWe
▼ Réacteur du palier 1450 MWe

ROBELSYS Workshop - April 1-4, 2014 **IRSN** 3

Context

Provisions were initially defined and additional significant enhancements have been implemented since the design stage (*Periodic Safety Reviews, lessons-learned from operating experience, insights of the Probabilistic Safety Assessments ...*) to :

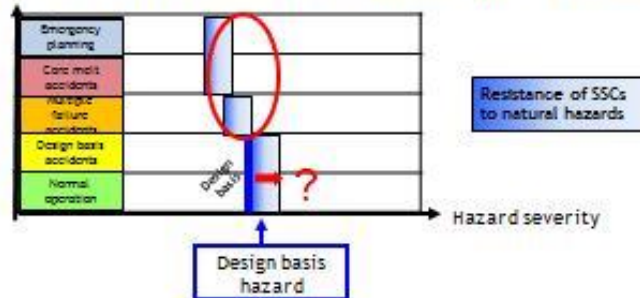
- Ensure protection of the safety SSCs against **natural hazards** (review of design basis hazards, improvement of protections...)
- Cope with a **total loss of all external and internal power supplies, a total loss of the heat sink and core melt accidents**
- Adapt **accidental procedures and emergency plans** to deal with **multi-units accidents**

ROBELSYS Workshop - April 1-4, 2014 **IRSN** 4

Context

The Fukushima accident has pointed out the need to go further:

- To ensure robustness against **more severe hazards (beyond design)**



- To cope with **prolonged multi-units accidents**: loss of AC power, loss of the heat sink, core melt accidents

Following EDF “stress tests” it was decided to implement significant additional provisions ➔ The « **Hardened Safety Core** » concept

The « Hardened Safety Core » (HSC) concept

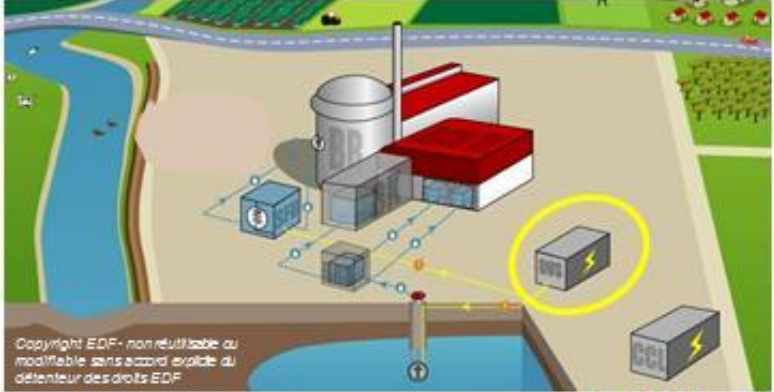
- ▮ To avoid large releases in extreme situations (postulated prolonged multi-units loss of AC power and of the heat sink induced by extreme hazards)
- ▮ Covering prevention and mitigation of core melt + emergency management
- ▮ Designed against hazards higher than design levels (earthquake, flooding and associated hazards): discussions in progress



The « Hardened Safety Core » (HSC) concept


- Main additional ultimate features envisaged:
 - > Means to fill in the steam generators
 - > Make-up to fill: the secondary water tanks, the primary water storage tank, the fuel pool
 - > New pump to inject into the primary circuit + cooling system (recirculation)
 - > A diesel generator and associated electrical distribution, dedicated I&C
 - > On-site crisis center

- + Improvement of emergency organization
- + “Nuclear Rapid Response Force”



Copyright EDF - non réutilisable ou modifiable sans accord explicite du détenteur des droits EDF

ROBELSYS Workshop - April 1-4, 2014


7

The « Hardened Safety Core » (HSC) concept



Copyright EDF - non réutilisable ou modifiable sans accord explicite du détenteur des droits EDF

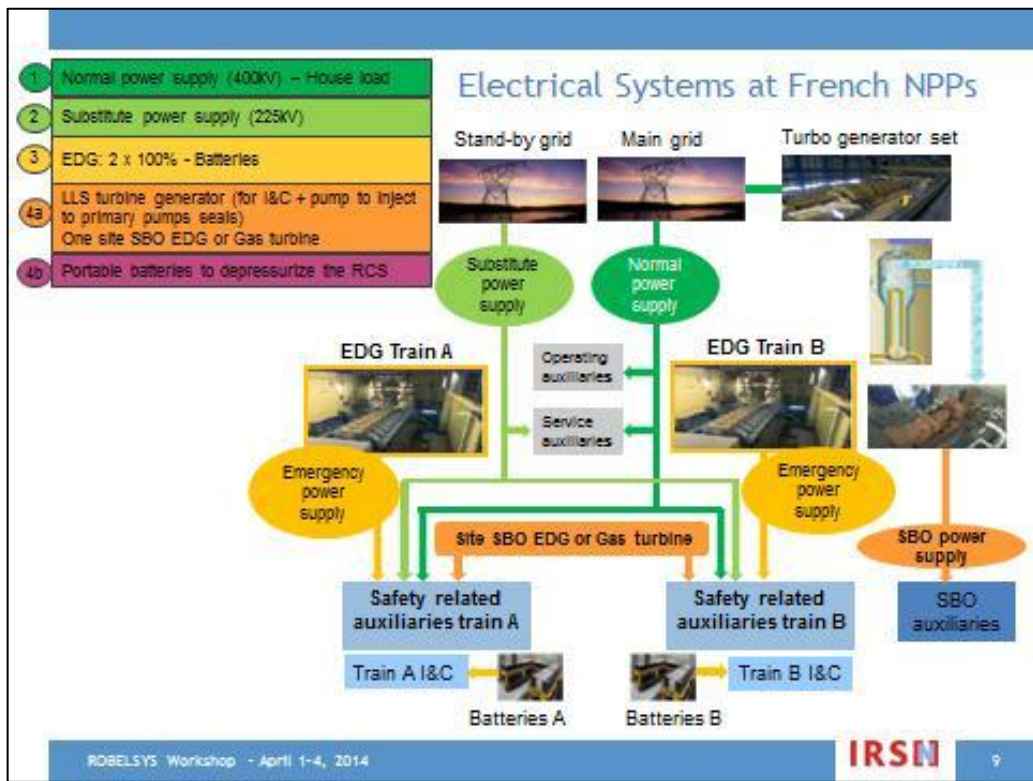
- HSC main principles presented by EDF and examined by IRSN in 2011-2012
- On the basis of IRSN analysis reports, ASN issued regulatory requirements related to the HSC



Detailed technical solutions for the HSC design still in progress at EDF (accident strategy to be confirmed, list of the new SSCs to be completed) and not approved by IRSN and ASN yet

ROBELSYS Workshop - April 1-4, 2014


8



Electrical Systems at French NPPs

- 1 Normal power supply - House load
- 2 Substitute power supply
- 3 EDG: 2 x 100% - Batteries
- 4a LLS turbine generator (I&C + pump) One site SBO EDG or Gas turbine
- 4b Portable batteries

Substantial existing provisions to cope with SBO situation (LOOP+EDG unavailable)

- > Some safety equipment operable without AC power (mobile diesel pump to inject into the primary circuit, turbine-driven AFW5 pump)
- > Dedicated SBO equipment + procedures implemented since the design stage
- > Safeguard electrical systems generally protected against external hazards

However to be reinforced/completed to cope with beyond design situations

- > Insufficient margins for some electrical equipment to cope with extreme hazards
- > Need to deal with prolonged multi-units SBO
- > Need for a "robust ultimate electrical line of defense" to support the HSC

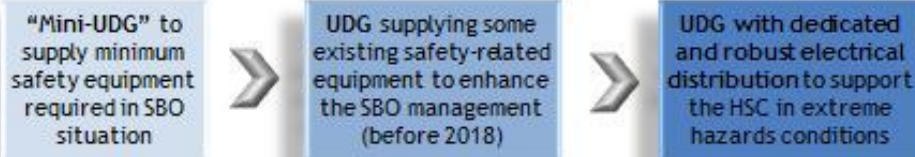
ROBELSYS Workshop - April 1-4, 2014 IRSN 10

Post-Fukushima electrical improvements

Implementation of an Ultimate Diesel Generator (UDG) and associated electrical distribution to support the Hardened Safety Core functions

- > One permanent UDG / unit (about 3 MW)
- > Nominal UDG voltage 6.6kV, supplying a new ultimate 6.6kV switchboard

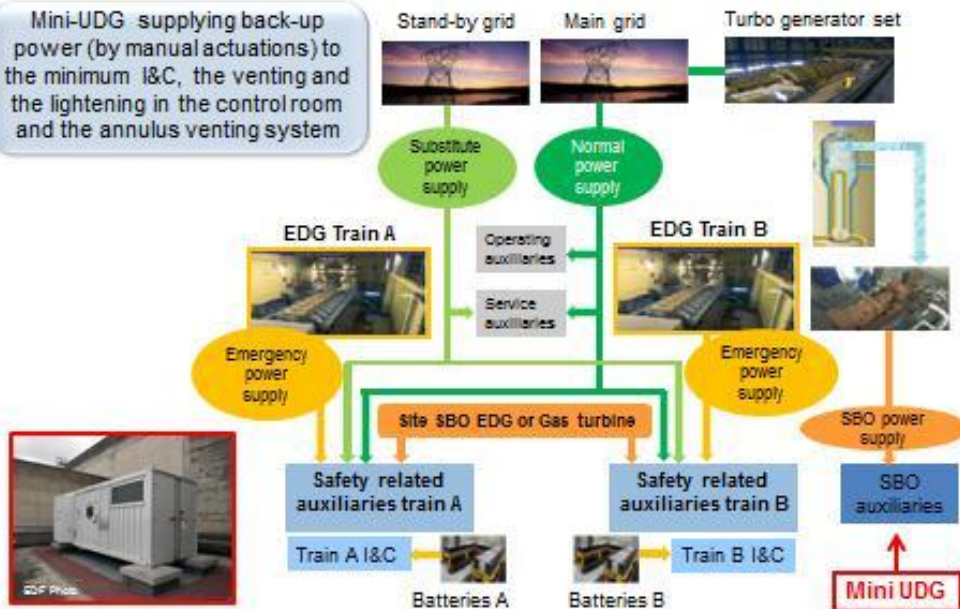
Gradual improvements:

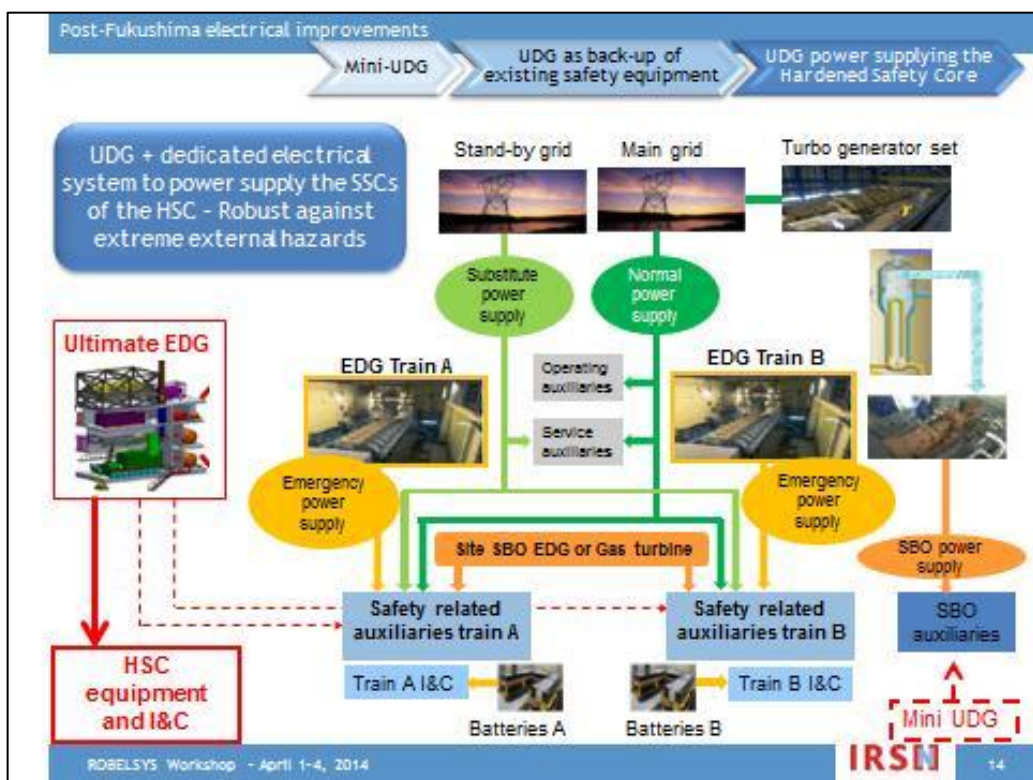
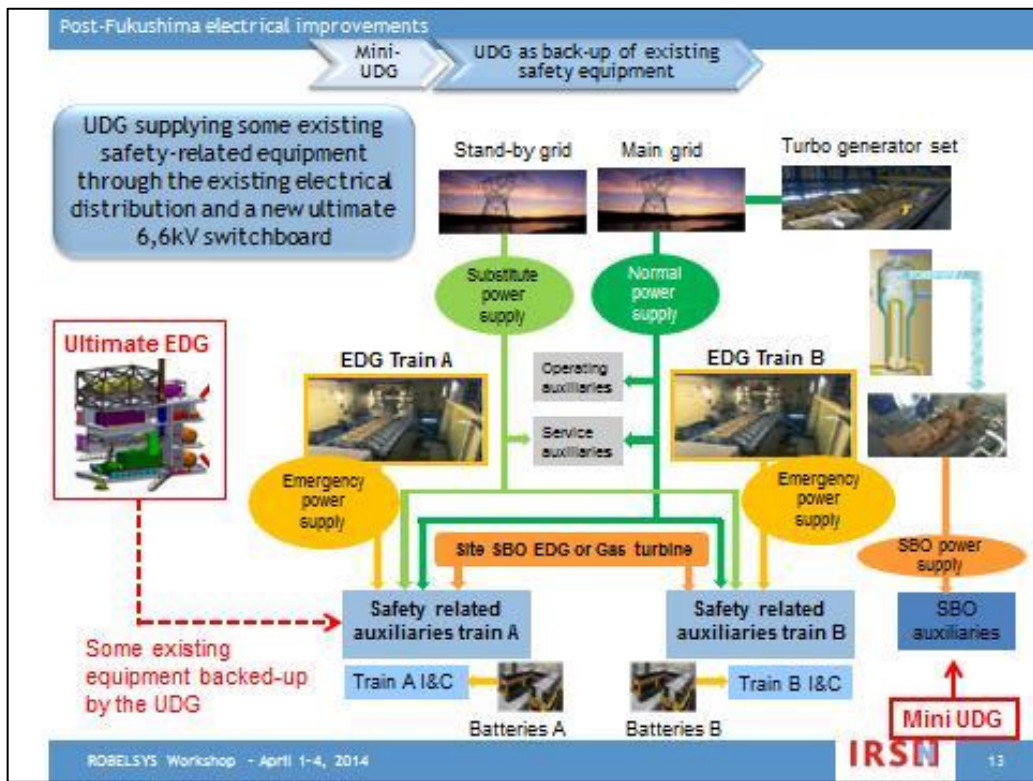


Post-Fukushima electrical improvements

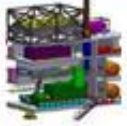
Mini-UDG

Mini-UDG supplying back-up power (by manual actuations) to the minimum I&C, the venting and the lightening in the control room and the annulus venting system






Post-Fukushima electrical improvements




- General architecture and layout
 - New UDG building (UDG, ultimate 6,6kV switchboard, electrical distribution to UDG auxiliaries)
 - Similar architecture envisaged for the 58 plants, however with adaptations due to plants specifics and constraints
 - At many sites, need for an intermediate electrical building (6,6kV/380V transformer, low voltage electrical distribution and I&C of the HSC)
 - Underground cables between buildings



Copyright EDF - non réutilisable ou modifiable sans accord explicite du titulaire des droits EDF


ROBELSYS Workshop - April 1-4, 2014


15

Post-Fukushima electrical improvements

- Some general characteristics
 - Independence between the electrical systems of the HSC and the “normal” systems as far as possible
 - Diversification of ultimate equipment desirable, notwithstanding the prior objective of sufficient reliability
 - The HSC comprises mainly new SSCs but also some existing robust equipment (ex: containment isolation valves) → Devices necessary to switch their power supplies to the “UDG systems” in extreme situations (not defined yet)
 - Manual switching by the operator to the ultimate systems (switching and UDG start criteria to be defined)

ROBELSYS Workshop - April 1-4, 2014


16

Post-Fukushima improvements at EPR Flamanville

Significant favorable design differences / operating NPPs

- > 6 EDG: 4 main + 2 ultimate "SBO" (diversified)
- > "Severe accident" batteries 12h
- > Diversified heat sink in addition to the main heat sink
- > Higher robustness to extreme flooding and earthquake at EPR Flamanville

Hardened Safety Core approach also applied to EPR: mainly existing SSCs

- > Ex: SBO diesel generators, batteries, HVAC of HSC SSCs...



Post-Fukushima improvements at EPR Flamanville

However some enhancements under study

- > Reinforcements of some equipment / extreme hazards
- > Extension to 24h of the "severe accident" batteries
- > Provisions to increase fuel oil SBO-DG autonomy
- > Provisions to fill the secondary water tanks (water storage on the top of the cliff)
- > Additional features to remove the heat from the containment in prolonged loss of external power supply and all EDGs



A Nuclear Rapid Response Force to complement the HSC

- Phase 1: On-site HSC permanent equipment**
 - > At least during the first 24 hours without any off-site support
 - > Fuel oil autonomy of the UDG = 72 hours (at full load)
 - > Mission time of the HSC SSCs = 15 days without maintenance
- Phase 2: Off-site support from EDF Nuclear Rapid Response Force to bring human means and mobile equipment after 24 hours (+ hook-up points)**

Total loss of electrical supplies or heat sink

On-site permanent Hardened Safety Core SSCs

Human means, mobile equipment

Heavy equipment

Recovery actions...

Off-site support

24 hours 3 days 15 days

ROBELSYS Workshop - April 1-4, 2014 **IRSN** 19

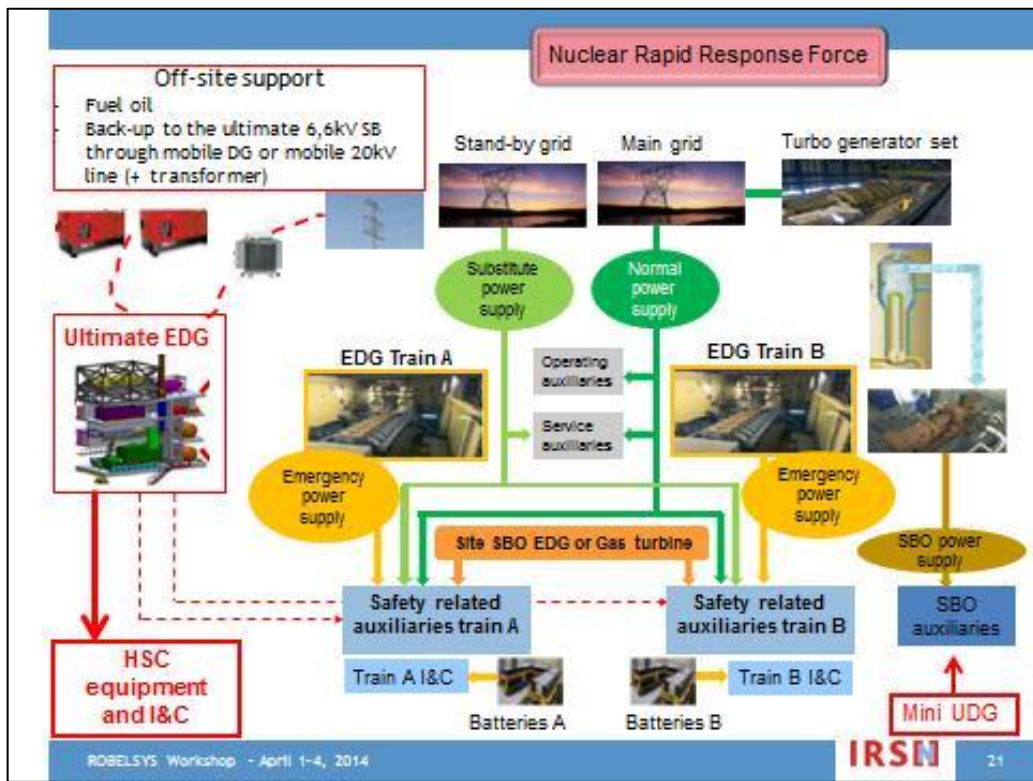
A Nuclear Rapid Response Force to complement the HSC

Provisions (some of them already implemented)

- Electricity (diesel generators, cables, electrical cubicles...)
- Water make-up (water capacities, pumps ...)
- Air compressor
- Communication means
- Protections against radiations
- Logistic (helicopter(s), vehicles, fuel oil ...)

- 1 national headquarter
- ▲ 1 national equipment base (heavy equipment)
- 4 regional equipment and human resources bases
- Rear bases (4 predefined for each NPP)

ROBELSYS Workshop - April 1-4, 2014 **IRSN** 20



Conclusion

- The Fukushima accident has pointed out the need:
 - > For design improvements to reinforce the electrical and cooling systems: studies were already ongoing in France on these issues before FKS
 - > To cope with beyond design hazards
- The Hardened Safety Core and the Nuclear Rapid Response Force will bring about significant enhancements
- The HSC will rely on ultimate robust electrical equipment and distribution



For more information: www.irsn.fr

**Electrical System Design Application on Japanese BWR Plants
in the Light of the Fukushima Accident
and Hitachi Experience of the Solid State Power Equipment
in Japanese BWR**

Masashi Sugiyama

Hitachi-GE Nuclear Energy, Japan

Abstract

After the Fukushima Daiichi accident (Loss of all AC and DC power sources and the distribution panels), several design enhancements have been incorporated or are under consideration to Japanese BWRs.

Especially, there are several important enhancements in the area of the electrical system design.

In this paper, the design enhancements related to the following systems will be introduced.

Supplemental AC power supply system

Enhancement on DC Battery system

In addition, this paper will show our practice of the solid state equipment in Japanese BWRs which have some special specifications, considering the special condition in the NPP's auxiliary electrical power system.

1. SBO & DC power blackout in Fukushima Daiichi NPP

At the Fukushima Daiichi NPP, Units 1 to 3 were in rated power operation before the earthquake which had occurred on March 11th, 2011. Units 4 to 6 had been shut down and had been in the outage for the periodic inspection. Of these three units, at Unit 4, all fuel was removed from the RPV and being stored and cooled in the SFP for the shroud replacement work. The outage for Unit 5 was nearly complete, fuel was loaded into the RPV and the water pressure leak tests were underway to verify its integrity. Unit 6 was also near completing outage, and fuel was already loaded into the RPV.

On March 11, 2011 at 14:46, the earthquake caused an automatic reactor scram at Unit 1 to 3, and all control rods were inserted at 14:47. Due to the loss of off-site power, two D/Gs started up automatically at 14:47.

Off-site power for the Fukushima Daiichi NPP consists of a total of 7 lines with six transmission lines from the Shin-Fukushima Substation (275kV Okuma Line 1L to 4L and 66kV Yonomori Line 1L and 2L) and one 66kV transmission line for the standby off-site power to the Unit 1 from the Tohoku Electric Power Company (66kV TEPCO Genshiryoku Line). Of the transmission lines from the Shin Fukushima Substation, the Okuma Line 1L and 2L connect to the Unit 1 and Unit 2 and Okuma Line 3L and 4L connect to the Unit 3 and Unit 4.

The Yonomori Line 1L and 2L connect to the Unit 5 and Unit 6. The TEPCO Genshiryoku Line was connected to the Unit 1 normal M/C (Metal-Clad Switchgear) via the standby switchyard.

On the day of the earthquake, the Okuma Line 3L was under repairs and out of service.

The Remaining all transmission lines were lost their power by the earthquake and caused loss of the off-site power.

The causes were as follows,

Okuma Line 1L and 2L; The electrical equipments in the switchyard, the CBs and the DSs were damaged by the earthquake. They were an air –blast type.

Okuma Line 4L ; The switchyard was flooded by the Tsunami.

The CBs have replaced to the GCBs already. They were not damaged by the earthquake.

Yonomori Line 1L and 2L: The transmission tower collapsed due to the landslip of the embankment near it. The switchyard was flooded by Tsunami.

After loss of the off-site power, the D/Gs started up and provided their power. However, at 15:35, the second tsunami hit, shortly after which all of the D/Gs were lost except Unit 6, D/G 6B which was added in 1996 and had an air-cooling heat sink.

As the result of the Tsunami flooding the entire area around major buildings, water flowed into the buildings, and most of the electrical equipment inside them lost their functions. The water-cooled D/Gs themselves at Unit 5 and Unit 6 were not damaged by water, but became inoperable due to the loss of their sea water cooling pumps. All of the water-cooled D/Gs at Unit 1 to Unit 4 were shut down due to the flooding by the Tsunami. On the other hand, Unit 2, D/G 2B, Unit 4, D/G 4B and Unit 6, 6B are air-cooled D/Gs and did not have sea water cooling pumps, thus there was no impact on their cooling systems caused by the Tsunami. D/Gs 2B and 4B were installed in the Common SFP building to the southwest of Unit 4 R/B, although there was no water to the D/Gs themselves, however the electrical equipment room in the basement of the building was flooded, submerging D/Gs excitation system panels and M/Cs causing them to lose their functions. As the result, all of the D/Gs for Unit 1 to Unit 5 were shut down, causing their station blackout. Only Unit 6 air-cooled D/G, 6B continued its operation and maintained its power.

At Units 1 to 5, all middle voltage switchgears (M/Cs) were damaged by sea water due to the Tsunami.

Therefore, it would not have been possible to supply power to the necessary equipment even-if D/Gs had been operable. Most of the low voltage switchgears (P/Cs) were also damaged by sea water.

In regard to the DC systems, they were damaged by sea water at Unit 1,2 and 4, but not at Unit 3,5 and 6. Flooding sea water most appeared on the lowest basement levels and at the main entrance area of the T/B where was just behind the T/B main entrance shutter, because the Tsunami had broken into the T/B main entrance shutter and flooding sea water, ingressed from the T/B main entrance and the intake air louvers for D/Gs. There were some penetrations such as ducts or trenches in the building, which were both water ingress pathways, therefore most of the underground level floors were flooded by the Tsunami.

For Unit 6, there was no damage to not only the air-cooled D/G 6B but also the M/Cs and the DC systems, thus the emergency on-site power for Unit 6 was available.

For Unit 5, there was the bus-tie connection between Unit 5 and Unit 6 low voltage MCCs as an one of the accident management countermeasures, thus Unit 5 on-site power could be restored.

2. Restoration of on-site power in Fukushima Daiichi NPP

In order to restore the onsite power of Unit 1 and Unit 2, TEPCO dispatched a power truck and tried to connect it to the low voltage switchgear P/C 2C of Unit 2 which was the only usable switchgear in Unit 1 and Unit 2 and was located in Unit 2 T/B B1. However immediately after the connection, around 15:30 on March 12, the Hydrogen explosion of Unit 1 disturbed the connection.

Meanwhile, in order to restore on site power of Unit 3 and Unit 4, a power truck connected to the low voltage switchgear of P/C 4D at 14:00 on March 13, 2011, but the Unit 3 hydrogen explosion occurred on March 14 interrupted its operation.

On March 12, the TEPCO power recovery team initially determined that it would be difficult to quickly restore the 275kV Okuma Lines because of the damage and flooding of the switchyards at Fukushima Daiichi NPP and decided to use the 66kV Yonomori Line 1L and 2L as 6.9kV lines to restore power using of mobile 66kV/6.9kV step down transformer truck at the Shin-Fukushima Substation. 66kV Yonomori Lines are originally connected to Unit 5 & 6, in order to place power as close as possible to Units 1 to 4, which needed off-site power the most, it was decided to connect the Yonomori 1L to Okuma Line 3L, which was the transmission line to supply power from Shin-Fukushima Substation to the Unit 3 and 4. 66kV Yonomori Line 2L to supply power to Unit 5 & 6. On March 15, the 66kV TEPCO Genshiryoku Line was charged up until the disconnecter on the standby switchyard, and facility integrity was verified. Due to the damage on the secondary cable to the Unit 1 and the damage of M/Cs in Unit 1, temporary M/C which was on the truck arrived at the Fukushima Daiichi NPP and stopped at the street north side of the Unit 1 T/B was laid on March 17th, and the cable from temporary M/C to the low voltage switchgear P/C 2C was laid on March 17 and 18, and about 1.5km cable from the standby switchyard to temporary M/C was laid on March 19th. After that, Unit 2 off-site power was restored on March 20. The former cabling work was done by the TEPCO power distribution division by using the cable laying car. The latter cabling work was done by about 100 Hitachi managers by the manual cable laying work under Hitachi supervisors because of the high level radiation after hydrogen explosions. On March 15, the Okuma Line 3L was connected to the Yonomori Line 1L on the transmission tower then connected to the mobile mini-clad switchgear (installed by the TEPCO Transmission Division), and charged up on March 18. On March 19, Multi-circuit breakers and the cable between the mobile mini-clad switchgear and the Multi-circuit breakers were installed by the TEPCO Distribution Division.

On March 21, about 100 Hitachi managers also laid the cable from the mini-clad switchgear to P/C 4D in the Unit 4 T/B by the manual cable laying work. On March 22, P/C 4D, which was the on-site power of Unit 3 and Unit 4, was restored.

In addition, 66V Yonomori Line 2L was restored with a new transmission route using 500kV Futaba Line No.2 tower instead of the collapsed No.27 tower of 66kV Yonomori Line. At the same time, integrity of the equipment (Start up transformers, circuit breakers, etc.) was verified and cables were installed on March 20, It was charged up to the Unit 5 and 6 Start up transformers, then off-site power of Unit 5 and Unit 6 was restored on March 21.

To enhance the supply reliability of the off-site power, the following actions have been done. The Okuma lines voltage changed from 6.9kV to 66kV in April, 2011. New switchyard with 66kV/6.9kV 30MVA transformer constructed for Unit 1 to Unit 4, and new 66/6.9kV transformer was installed at the standby switchyard and in the both of new and the stand-by switchyard, new M/Cs were installed. Air cooled D/Gs 2B and 4B in the Common spent fuel pool building have been restored by the replacement of

their excitation panels and M/Cs in June(4B) , 2011 and Jan. 2012(2B) .The endeavour to enhance the reliability of the on-site and off-site power of the Fukushima Daiichi is still on the way now.

3. New Safety Guide for Electrical System in Japan

The Nuclear Regulation Authority in Japan submitted a new safety standards for nuclear power stations based on the lessons learned from the Fukushima Daiichi Accident. The Standards consists of three parts; Design basis Safety Standards, Severe Accident Measures and Safety Standards relative to Earthquake and Tsunami.

3.1 Off-site power;

The off-site power shall be connected to the electrical power system with two or more transmission lines, which are connected to two or more independent substations or switchyards in which at least one line out of these lines is physically separated from the other lines. Also, in the case of that multiple reactors are sitting at a nuclear power station, it shall be designed so that loss of any two lines of the power transmission lines may not cause the loss of its off-site power at the same time in these nuclear power facilities.

3.2 Sever Accident Measures;

Prepare equipment and procedures for securing electricity required to prevent a severe core damage, prevent a containment vessel failure, etc., against loss of power beyond the design base accidents.

AC power;

- a) Alternative system shall be independent and dispersed at different locations to the equipment for the design basis requirements.
- b) Mobile alternative power sources (for example, power trucks) shall be made available and ready to use.
- c) Install permanent alternative power sources (for example, gas turbine generators).

DC power

- a) On site permanent DC power source shall have the capacity to keep supplying electricity 8 hours without load shedding. In addition, the electricity supply shall be assured for 24 hours in total, to cover 16 hours by load shedding.
- b) The mobile DC power equipment shall be prepared for a capable for 24 hours in total including 8 hours without load shedding.
- c) For further improvement of reliability, one more system (namely 3rd system) of permanent onsite DC power supply shall be prepared.
- d) Connection of mobile power supply and start of power supply shall be feasible with sufficient time allowance within the time where onsite permanent DC system can continue to provide DC power.

Power Sharing;

Power sharing among the units shall be feasible.

- a) Prepare cables in advanced and facilitate the manual connection.
- b) Prepare a stand-by electrical cable in order to cope with the situation where installed electrical cable may not be usable

Alternative on-site power supply;

Install alternative onsite power supply (MCC, P/C, M/C etc.)

- a) Alternative on-site power supply as well as design basis facilities shall not lose its function caused by the common cause, maintain its function provided by at least one line, and allow personnel access.

4. Example of Assessment against New Safety Guide

Shimane Unit 2 is a 2436MWt BWR5 owned by the Chugoku electric power company and started its commercial operation in 1989. Unit 2 had 2(two) 220kV transmission lines which were connected to Kita-Matsue Substation.

According to the New Safety Guide, they built 66kV back-up switchyard which is fed from the 66kV transmission line which is connected to the other substation named Tsuda Substation.

They also built an emergency electrical panel building which has a back-up switchgear in it. Through the back-up switchgear, Unit 2 can be fed from 500kV transmission lines via Unit 3.

As for the on-site power, they prepared the gas-turbine generator power trucks as alternative, independent and diverse AC power source which are located at high elevation area against Tsunami. In addition, they prepared the mobile power trucks and the terminal boxes for their cables connection.

As for DC power, they updated the existing DC batteries to cope with the 24 hours operation and they added the DC system for Sever Accident Measure equipment. In addition, they have prepared the DC power trucks with incoming middle voltage cubicle, rectifier and batteries to cope with 24 hours operation of the DC loads including RCIC pumps and valves combined with using AC power trucks.. These DC loads require an inrush current periodically about every 90minutes, so to keep the load terminal voltage properly, Hitachi has developed the new DC power truck with both rectifier and batteries to feed the inrush current properly and to keep the reasonable equipment's sizes. They can be mounted on 11ton truck.

5. Hitachi Experience of Solid state power equipment in Japanese BWRs


Hitachi has supplied UPSs and ASDs (Adjustable Speed drives) for more than 30 years in Japanese BWRs. As for the ASD, the first one and the second one are both current source-type, PAM control Thyristor inverters for PLR pumps. The third one is a voltage-source type, PAM control GTO inverter for RIP and the fourth one is a voltage-source type, PWM control IGBT 2 level inverter for RIP. The fifth and the latest one is a voltage-source type, PWM control IGBT multi cell inverter for RIP.


We, Hitachi applies the proven Power device and the main circuit design in which is the industry standard to avoid the initial failure due to the new design. In addition, Hitachi applies the Power equipment which has its sufficient de-rating, to ride through the electrical variations in NPP, such as over voltage due to the load rejection of main generator, etc. and to get the long life time.

Our ASDs for nuclear power plant have a special characteristics of duplex controller and seismic proof design to improve the reliability.

References

- 1) Fukushima Nuclear Accident Analysis Report, June 20, 2012
Tokyo Electric Power Company Inc.
- 2) Draft New Safety Standards of Electrical Systems for Nuclear Power Stations
NRA, Japan
- 3) The Outline of the assignment against New Safety Standards in Shimane Unit 2
January 6, 2014, Chugoku Electric Power Company Inc.

	HITACHI 
Robustness of Electrical Systems of NPPs in Light of the Fukushima Daiichi Accident OECD/NEA CSNI Workshop	
Electrical System Design on Japanese BWR plants in the Light of the Fukushima Daiichi Accident and Hitachi Experience of the Solid state power equipment in Japanese BWRs.	
2014/04/01	
Hitachi-GE Nuclear Energy, Ltd	
Masashi Sugiyama	

Contents	HITACHI 
1. SBO in Fukushima-Daiichi nuclear Power Station	
2. New Safety Guide of Electrical Systems in Japan	
3. Example of assessment against New Safety Guide	
4. Hitachi Experience of Solid state power equipment in Japanese BWRs	

1-1. SBO & DC blackout has occurred in unit 1-4 HITACHI

Fukushima-Daiichi unit 1-unit4

1. The Off-site Power was lost due to the earthquake.
2. The On-site power, D/Gs and DC power supply were lost due to the Tsunami.
3. The Emergency switchgears were lost their function by flooding due to the Tsunami.

>>> SBO & DC Blackout >>> Fuel Melt down

Fukushima-Daiichi unit 5 & 6

1. The Off-site Power was lost due to the earthquake.
2. One of 5 D/Gs which was cooled by Air Fin Cooler continued its operation successfully, the other D/Gs were lost due to the loss of their heat sinks by Tsunami.

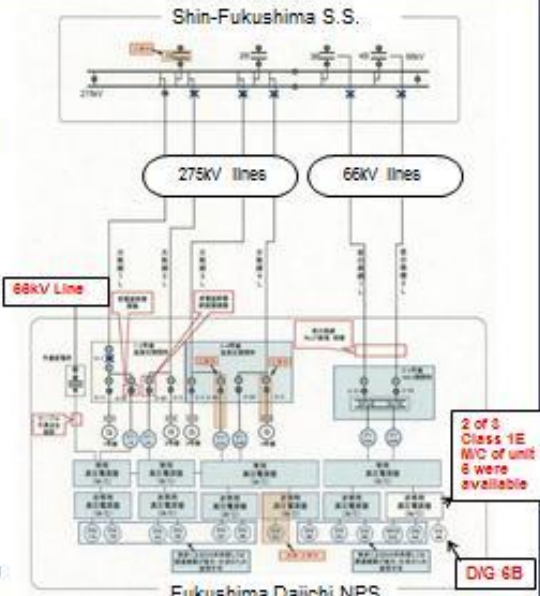
>>> Cool shutdown Successfully

© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 2

1-2. AC power system HITACHI

- 1) There are 4 (four) 275kV transmission lines on two physically independent 2 transmission raceways for unit 1-4.
- 2) There are 2 (two) 66kV transmission lines for unit 5&6.
- 3) They were connected to the same substation and all of them were lost.
- 4) 1 (one) 66kV transmission line which was connected to the other substation was available.
- 5) Only one D/G, 6B which was air-cooled could operate after the Tsunami.

Under outage
 Flooded by Tsunami
X Trip



© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 3

68

1-3. DC power system HITACHI

Fukushima-Daiichi unit 1-unit4

- DC Power systems were lost due to the Tsunami (Flooding) except unit 3.
- Unit 3 DC was lost its power more than 1 day after the Tsunami due to SBO.

Fukushima-Daiichi unit 5 & 6

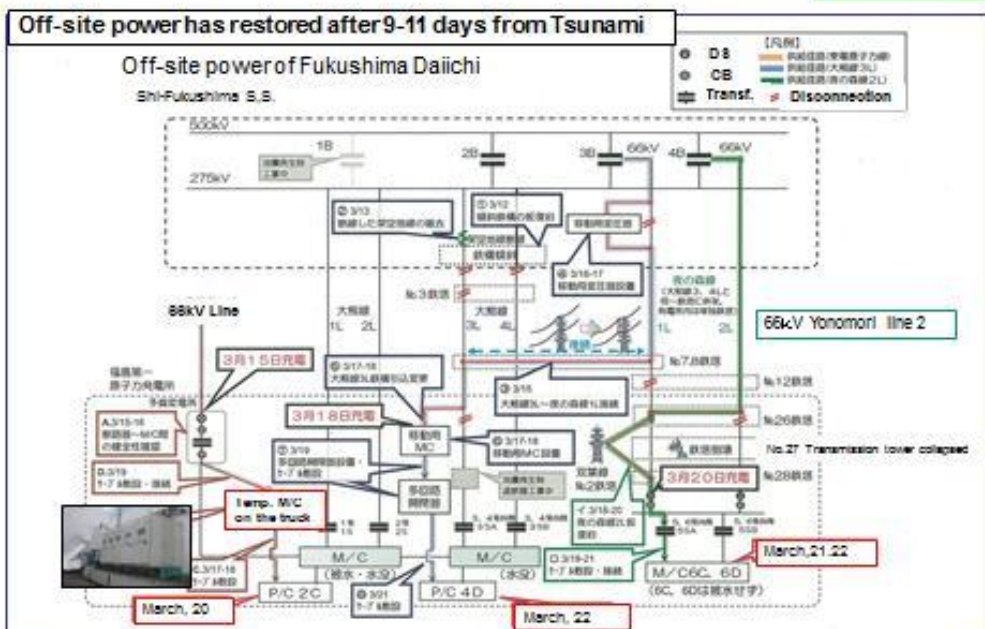
- Both of unit 5 & 6 DC system were available after the earthquake and Tsunami.
- D/G 6B was available and using the Accident management system (Connection between adjacent units), unit 5 AC system was restored.

© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 4


1-4. Restoration of Fukushima Daiichi Offsite power HITACHI


Off-site power has restored after 9-11 days from Tsunami



Off-site power of Fukushima Daiichi
Shi-Fukushima S.S.





© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 5

<h2>2. New Safety Guide of ELS in Japan</h2>	
<div data-bbox="331 385 683 430"> <h3>2.1 Off-site power</h3> </div> <div data-bbox="354 443 1295 748"> <p>The off-site power shall be connected to the electrical power system with two or more transmission lines, which are connected to two or more independent substations or switchyards in which at least one line out of these lines is physically separated from other lines. Also, in the case of that multiple reactors are sitting at a nuclear power station, it shall be designed so that loss of any two lines of the power transmission lines may not cause the loss of its off-site power at the same time in these nuclear power facilities.</p> </div> <div data-bbox="874 1012 1321 1034" style="text-align: right;"> <small>© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 6</small> </div>	

<h2>2. New Safety Guide</h2>	
<div data-bbox="331 1205 922 1249"> <h3>2.2 Severe Accident Measures</h3> </div> <div data-bbox="402 1258 1305 1370"> <p>Prepare equipments and procedures for securing electricity required to prevent a severe core damage, prevent a containment vessel failure, etc., against loss of power beyond the design base accidents.</p> </div> <div data-bbox="331 1415 539 1451"> <h4>2.2.1 AC Power</h4> </div> <div data-bbox="402 1460 1279 1697"> <ol style="list-style-type: none"> a) Alternative system shall be independent and dispersed at different locations to equipment for the design basis requirements. b) Mobile alternative power sources (for example, power trucks) shall be made available and ready to use. c) Install permanent alternative power sources (for example, gas turbine generators) </div> <div data-bbox="874 1832 1321 1854" style="text-align: right;"> <small>© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 7</small> </div>	

2. New Safety Guide	 
2.2 Severe Accident Measures	
2.2.2 DC Power	
<ul style="list-style-type: none"> a) On site permanent DC power source shall have the capacity to keep supplying electricity 8 hours without load shedding. In addition, the electricity supply shall be assured for 24 hours in total, to cover 16 hours by load shedding. b) The mobile DC power equipment shall be prepared capable for 24 hours in total including 8 hours without load shedding. c) For further improvement of reliability, one more system (namely 3rd system) of permanent onsite DC power supply shall be prepared. d) Connection of mobile power supply and start of power supply shall be feasible with sufficient time allowance within the time where onsite permanent DC system can continue to provide DC power. 	
<small>© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved.</small>	
8	

2. New Safety Guide	 
2.2 Severe Accident Measures	
2.2.3 Power Sharing	
Power sharing among the units shall be feasible.	
<ul style="list-style-type: none"> a) Prepare cables in advanced and facilitate the manual connection. b) Prepare stand-by electrical cable in order to cope with the situation where installed electrical cable may not be usable. 	
2.2.4 Alternative onsite power supply	
Install alternative onsite power supply (MCC, PC, MC etc.)	
<ul style="list-style-type: none"> a) Alternative on-site power supply as well as design basis facilities shall not lose its function caused by the common cause, maintain its function provided by at least one line, and allow personnel access. 	
<small>© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved.</small>	
9	

3. Example of assessment against New Safety Guide

3.1 Original
Unit 2 has 2 220kV Lines

3.2 Assessment against New Safety Guide

- 1) Unit 2 can be fed from 66kV line which is connected to the other S.S.
- 2) Unit 2 Class 1E buses can be fed from 2 500kV lines through Buck-up switchgear.
- 3) Unit 2 Class 1E buses can be fed from 66kV lines through Buck-up switchyard which is located at the high level area.

Off-site power

© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 10

3. Example of assessment against New Safety Guide

3.3 On-site Power

© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 11

3. Example of assessment against New Safety Guide

3.3.1 DC Power Truck

- RCIC loads require the periodic inrush current
- Middle voltage AC power trucks are available
- We improved DC power truck which has both Charger & Battery
- DC power truck can feed the inrush current with proper voltage drop.

DC Power Truck (Middle size truck)

© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 12

4. Hitachi Experience of Solid state power equipment in Japanese BWRs

4.1 Hitachi Experience


Hitachi has supplied UPSs and ASDs (Adjustable Speed drives) for more than 30 years in Japanese BWRs.

1993.0 Shika-1	Current Source Type - PAM control Thyristor Inverter Specification: 3.3kV/3400kVA, 50%×2	PLR : Primary Loop Recirculation RIP : Reactor Internal Pump GTO : Gate Turn Off Thyristor IGBT : Insulated Gate Bipolar Transistor PAM : Pulse Amplitude Modulation PWM : Pulse Width Modulation
1994.0 Kashiwazaki-Kariwa-4	Ditto Specification: 6.7kV/7000kVA, 50%×2	
1997.0 Kashiwazaki-Kariwa-7	Voltage Source Type - PAM control GTO Inverter Specification: 3.09kV/1250kVA, 11.1%×10	
2006.0 Shika-2	Voltage Source Type - PWM control IGBT Inverter Specification: .09kV/1250kVA, 11.1%×10	

History of the ASD for PLR & RIP in BWR

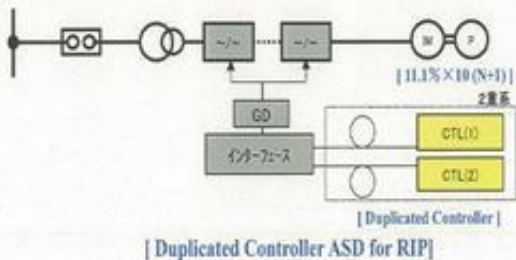
© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 13


4. Hitachi Experience of Solid state power equipment in Japanese BWRs



4.2 Our Concept

- a) Hitachi applies the proven Power device and main circuit design in which is the industry standard to avoid the initial failure due to the new design.
- b) Hitachi applies the Power equipment which has its sufficient de-rating, to ride through the electrical variations in NPP, such as over voltage due to the load rejection of main generator, etc. and to get the long life time.
- c) Hitachi applies the ASD for RIP which has duplex controller and seismic proof panel to improve the reliability.





© Hitachi-GE Nuclear Energy, Ltd. 2013. All rights reserved. 14

Thank you for your attention



Electric Power Supply of German NPPs: Defence in Depth, Protection against External Hazards and Retrofitting as a Consequence of the Fukushima Accident

Sebastian A. Meiß

Bundesamt für Strahlenschutz (BfS), Germany

Robert Arians

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Germany

Abstract

In this paper we give a concise overview over the history and present status of nuclear power in Germany. The changes in the regulatory framework and corresponding requirements, standards, recommendations etc. due to the Fukushima Daiichi accident, with respect to the robustness of the electric power supply of German nuclear power plants, are being described. On the example of a typical German Pressurized Water Reactor the concept of defence in depth in protecting the plant's electric power supply and the modifications to it due to the events in Chernobyl and Fukushima are shown.

1. History and status of nuclear power plants in Germany

The history of building and operating nuclear power plants (NPPs) in Germany dates back to the late 1950s and will come to an end in 2022. By then all NPPs still in operation will have to shut down in a defined sequence, according to the revisions made to the German Atomic Energy Act (AtG)¹ as a consequence of the accident at the Fukushima Daiichi NPP. Eight out of the 17 NPPs in operation in early 2011 have already been shut down permanently as a consequence. (Figure 1)

Of those nine NPPs still in operation, seven are Konvoi- or Vor-Konvoi-Type Plants based on Pressurized Water Reactors (PWR) and one twin-unit-NPP is based on Boiling Water Reactors (BWR) of type SWR 72.

2. Electrical power supply of German NPPs

Due to the progress in science and technology, the design of the electrical power supply of German NPPs got more complex and hardened against various scenarios with time.

¹. Atomgesetz in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 5 des Gesetzes vom 28. August 2013 (BGBl. I S. 3313) geändert worden ist, AtG / German Atomic Energy Act

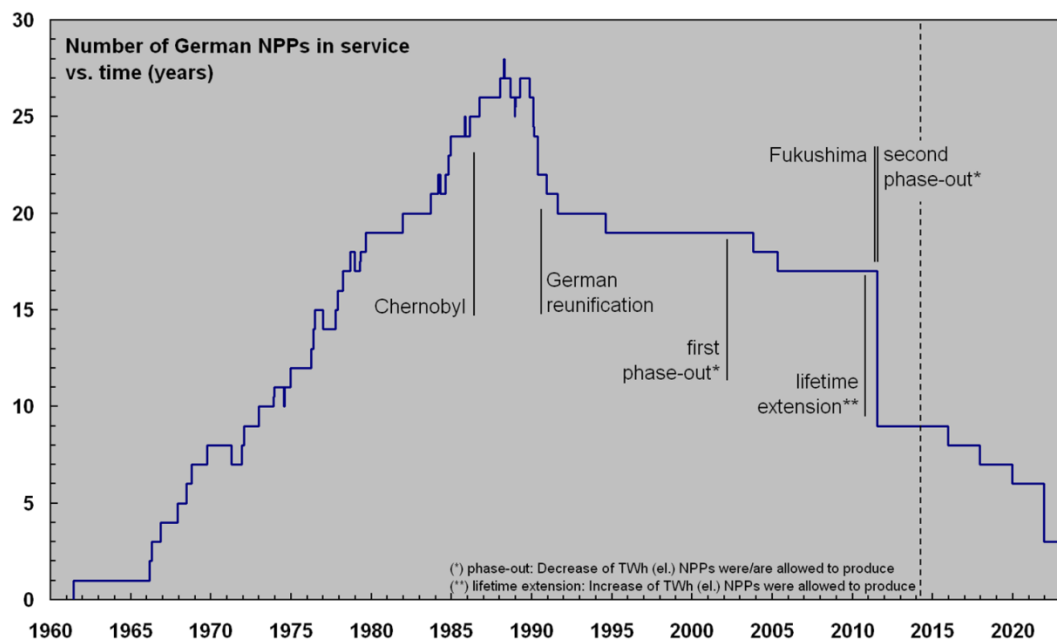


Figure 1: Concise overview over the history of German NPPs from the beginning of operation till the end of operation as scheduled by the German Atomic Energy Act (AtG)

The latest generation of NPPs built in Germany in the late 1980's - the pressurized water reactor of type Konvoi - was designed with a modern concept of Defence in Depth in mind. These NPPs are connected to several voltage levels of the power grid - e. g. 400 kV as the main grid and 110 kV as the standby grid connection. They feature two layers of AC emergency power systems, each of which fulfils the n+2 redundancy criteria. The secondary of those layers (D2-system) is especially hardened against the influence of certain internal and external events and is part of an emergency control system which can keep the plant in a safe state autonomously for 10 hours under certain conditions. As all German NPPs, they are equipped with a generator switch and are therefore capable of self-supply house-load operation. As part of accident management, emergency grid connections can be used. Those connections may connect the NPP e. g. to another, non-nuclear power plant that has a black-start capability. (Figure 2)

With this being the state of science and technology at that time in Germany, most of the older NPPs in operation had been retrofitted by 2011 with systems that were designed to partially compensate for those plants' weaker original design base.

Various events, such as the accident at the Chernobyl 4 NPP in 1986 and also the accident at the Fukushima Daiichi NPP in 2011, led to changes in the German regulatory framework and recommendations to the NPPs for further retrofitting activities. In the regime of electrical power supply, the latest changes in requirements and corresponding retrofitting of the NPPs in operation include mobile diesel generators with corresponding, redundant feeding points, an enhanced coping time for station blackouts with only DC-power left and measures to ensure bringing back AC-power within the coping time.

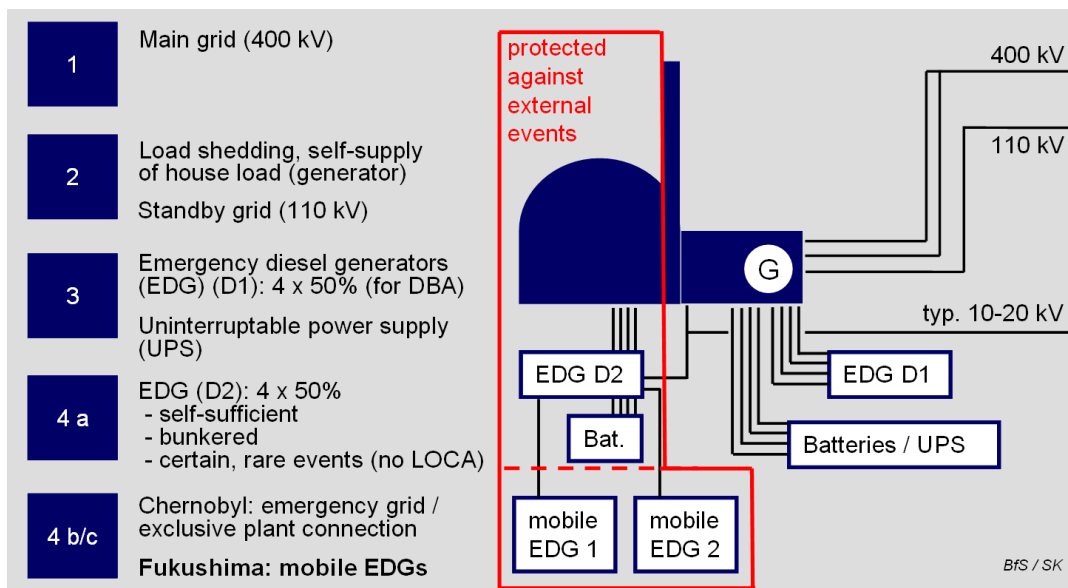


Figure 2: Defence in Depth of the Electric Power Supply in German NPPs. The example shown is based on a general PWR design of those German PWR based NPPs still in full service.

3. Regulatory framework after the events in Fukushima Daiichi

The introduction of mobile emergency diesel generators (EDG) is a consequence of the requirement of an increased coping for station blackout (SBO) scenarios for German NPPs. The mobile EDGs extend the purely battery based coping times of at least two hours, that were required before. This SBO-scenario is based on the postulate that all fixed mounted EDGs of the NPP might fail as a consequence of a common cause failure (CCF). Furthermore, typically at least one mobile EDG is designed to supply one redundancy of the emergency cooling and residual heat removal system with electric power.

Requirements and recommendations for an enhanced handling of a SBO can be found in the Information Notice on the Fukushima event², the Safety Requirements published in 2012³ and the recommendations of the German reactor safety commission (RSK) on the robustness of the German nuclear power plants⁴. The corresponding measures have been included in the German National Action Plan and are reported therein.⁵

². Weiterleitungsnachricht zu Ereignissen in ausländischen Kernkraftwerken (WLN 2012/02), Gesellschaft für Anlagen und

Reaktorsicherheit (GRS) mbH, Cologne, Germany, 15.02.2012

³. Sicherheitsanforderungen an Kernkraftwerke, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU), Bonn, Germany, 22.12.2012

⁴. Recommendations of the RSK on the robustness of the German nuclear power plants, Appendix 1 to the minutes of the 450th meeting of the Reactor Safety Commission (RSK) on 26./27.09.2012, RSK/ESK-Geschäftsstelle beim Bundesamt für Strahlenschutz, Bonn, 2012

⁵. German Action Plan for the implementation of measures after the Fukushima Dai-Ichi reactor accident, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU), Bonn, Germany, 31.12.2012

Further requirements introduced as a consequence of the Fukushima Daiichi accident include a diverse heat sink, usable e. g. for the cooling of EDGs, being able to cope with extended grid-loss-scenarios. Accident management measures introduced already in the past as a consequence to the events of Chernobyl in 1986 been made mandatory - e. g. the emergency grid connections mentioned earlier.



Figure 3: a) Two medium sized (550 kVA) mobile EDG in trailer-container; feeding point. (Source: RWE). b) Small sized (200 kVA) mobile EDG that can be handled without machinery; connector cable and housing. c) Big sized (1250 kVA) mobile EDG; multiple connector cables for manual manageability; trailer-container for big sized EDG. (Source b) and c) : e.on)

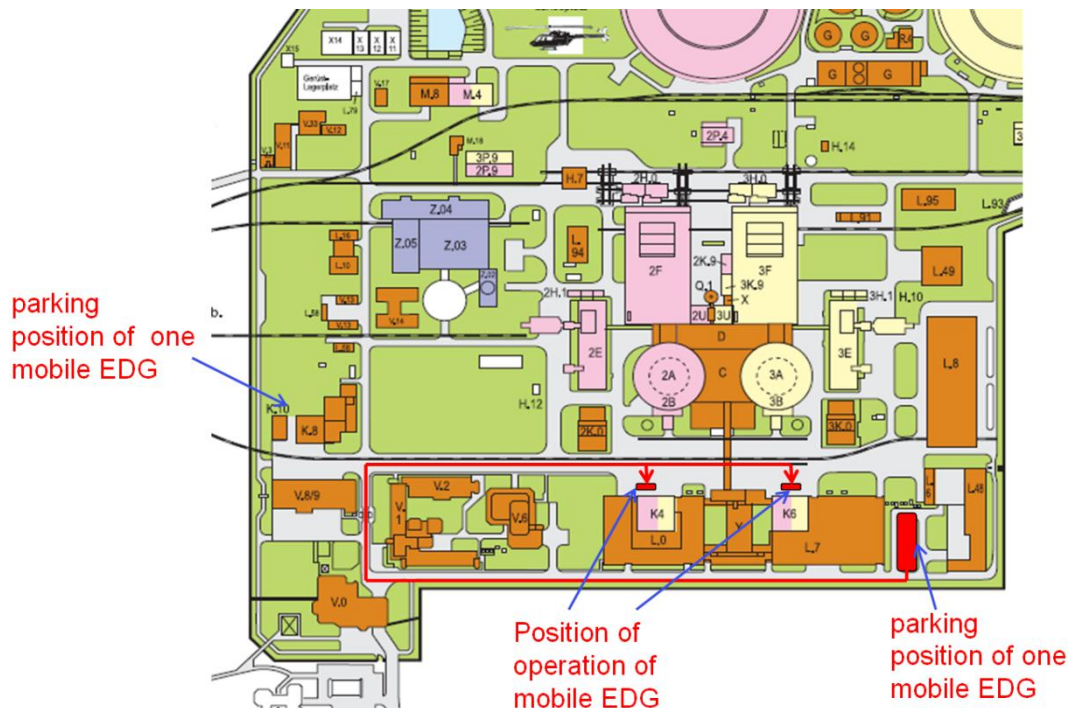


Figure 4: Parking positions and positions of operation of the two mobile EDG at Gundremmingen NPP (KGG). KGG is a twin-unit with BWRs of type SWR 72. (Source: KGG)

4. Mobile emergency diesel generators

German NPPs introduced mobile emergency diesel generators as a consequence of the Fukushima Daiichi accidents. Different concepts concerning those mobile EDGs exist. Some concepts include two mid-sized EDGs of roughly half electric power output each that is needed to supply one redundancy of the emergency cooling and residual heat removal system. They can be run in parallel or separately, to fulfil different tasks. Another concept includes a small, mobile EDG that can be handled without machinery for a rapid usability to extend the battery lifetime and one mobile EDG on a trailer that needs some time to be put in operation, but is capable of supplying one redundancy of the emergency cooling and residual heat removal system with electric power by itself. (Figure 3)

The heavier mobile EDGs are installed in containers on trailers and are – as all mobile EDGs – protected against external hazards. Multiple feeding points have been installed and also been protected against external hazards. For example, at the twin-unit Gundremmingen NPP (KGG) - the only site in Germany with two reactors still in full operation - two EDGs with 810 kW motor power each and 1 100 kVA generators have been implemented to supply power to a calculated sum of 526 kVA in electric loads (up to 700 kVA including additional measures).

As can be seen in Figure 4, the two mobile EDG are parked at spatially separated positions. At two locations a total of four feeding points have been installed at the KGG site.

5. Conclusions

As stated in the conclusions of the National Report of Germany of the EU Stresstest⁶ "The German licensees reported no shortfalls regarding safety precautions for the nuclear power plants participating in the EU stress tests. Likewise, no cliff edge effects were detected. The German regulatory body confirms this finding as far as the licensing basis and the basic safety design is concerned. Nevertheless, the results documented in the Chapters 2 to 6 in the report reflect the view of the regulatory body, that further improvement of the safety remains an important obligation for the licensees based on operation experience and further safety insights, and constitutes as well a constant issue for the competent authorities in their respective roles and functions in the regulatory oversight process."

Later on the Report mentions - with concern to the electric power supply of German NPPs - the two topics "Station blackout" and "Loss of offsite power" that required further work. These issues have now been addressed by the introduction of new measures, including those on-site mobile EDGs as mentioned above - further enhancing the robustness of electrical systems of German NPPs in the light of the Fukushima accident.

⁶. EU Stresstest - National Report of Germany, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU), Bonn, Germany, 31.12.2012

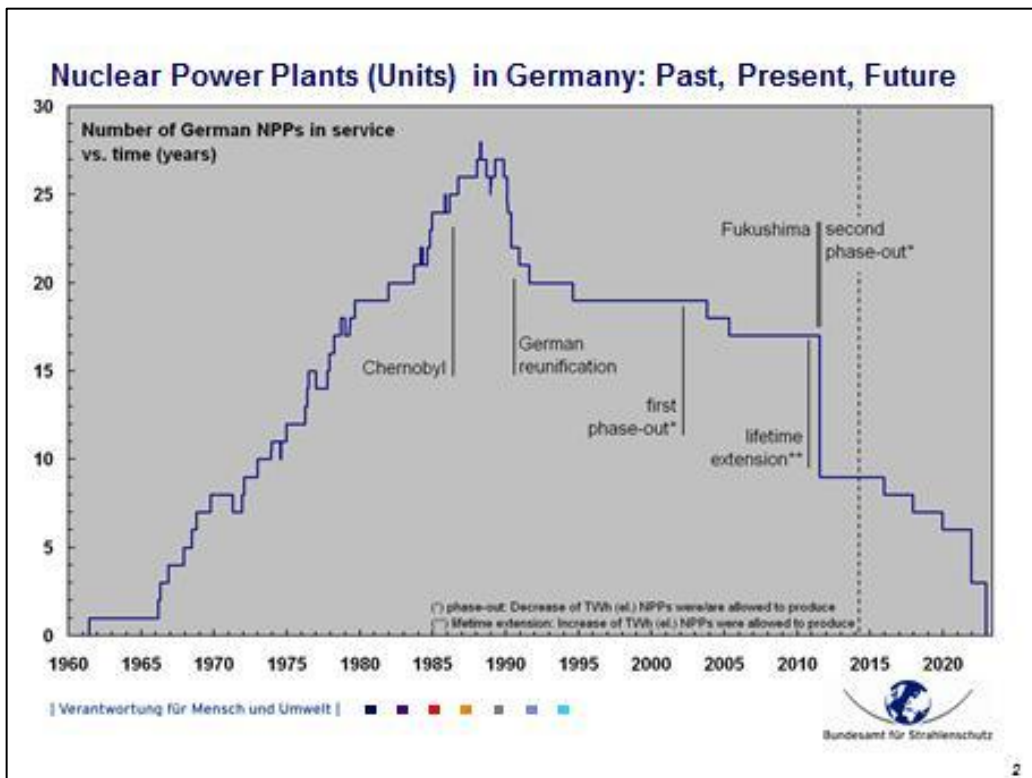
Electric Power Supply of German NPPs: Defence in Depth, Protection Against External Hazards and Retrofitting as a Consequence of the Fukushima Accident

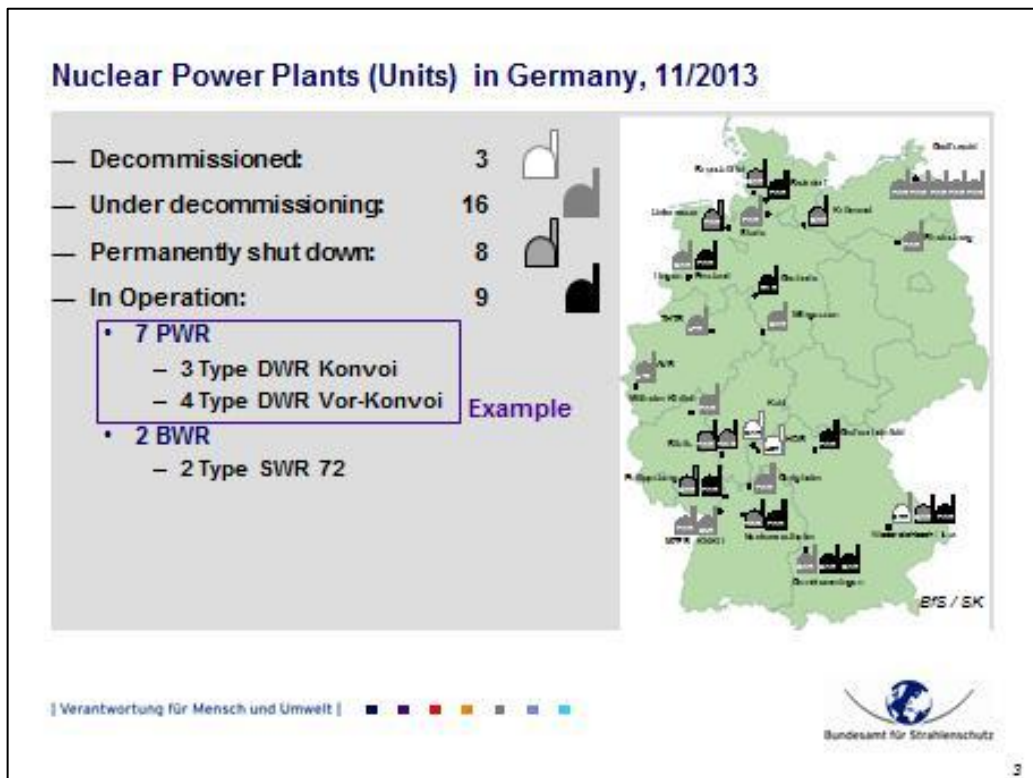
Sebastian A. Meiss (BfS), Robert Arians (GRS)

1 - 4 April 2014

Workshop on the
Robustness of Electrical Systems of NPPs
in the Light of the Fukushima Accident
OECD/NEA, Paris, France

| Verantwortung für Mensch und Umwelt |





- ### Overview regulatory framework, changes after or due to Fukushima
- Atomic Energy Act (AtG)
 - Permanently shutting down 8 NPP and phasing out till 2022
 - Accident management obligatory (§ 7 d)
 - New "Safety Requirements for NPPs" with interpretations
 - Emergency grid connection obligatory
 - Differentiation between loss of offsite power < 10 h and loss off offsite power > 10 h
 - RSK (Reactor Safety Commission)
 - National safety review
 - Recommendations of the RSK on the robustness of the German NPP
 - natural and man-made external hazards, internal hazards, CCF postulate
 - 1-week grid loss, guaranteed fuel supply for EDG also in case of external events
 - 10h SBO, mobile EDGs allowed to extend battery lifetime (typ. > 2 h)
 - Diverse heat sink (Cooling of EDG guaranteed after loss of primary heat sink)
 - KTA Rules
 - 3701 (Power Supply), 3702 (EDG), 3703 (UPS), 2201.x (Seismic), etc.
 - Information notice by GRS on Fukushima
 - 10h SBO: mobile EDGs usable in case of external events with redundant feeding points
 - Diverse heat sink, usable for EDG cooling also in case of external events
 - Tools to regain access to buildings after external events
- | Verantwortung für Mensch und Umwelt |
- Bundesamt für Strahlenschutz
- 4

Mobile Emergency Diesel Generators PWR

(2/3)

Two Concepts (both: two mobile EDG, with flexible, prepared feeding points)

- Concept 1: small sized (200 kVA) + big sized (1250 kVA) mobile EDG



| Verantwortung für Mensch und Umwelt |



7

Mobile Emergency Diesel Generators PWR

(3/3)

Two Concepts (both: two mobile EDG, with flexible, prepared feeding points)

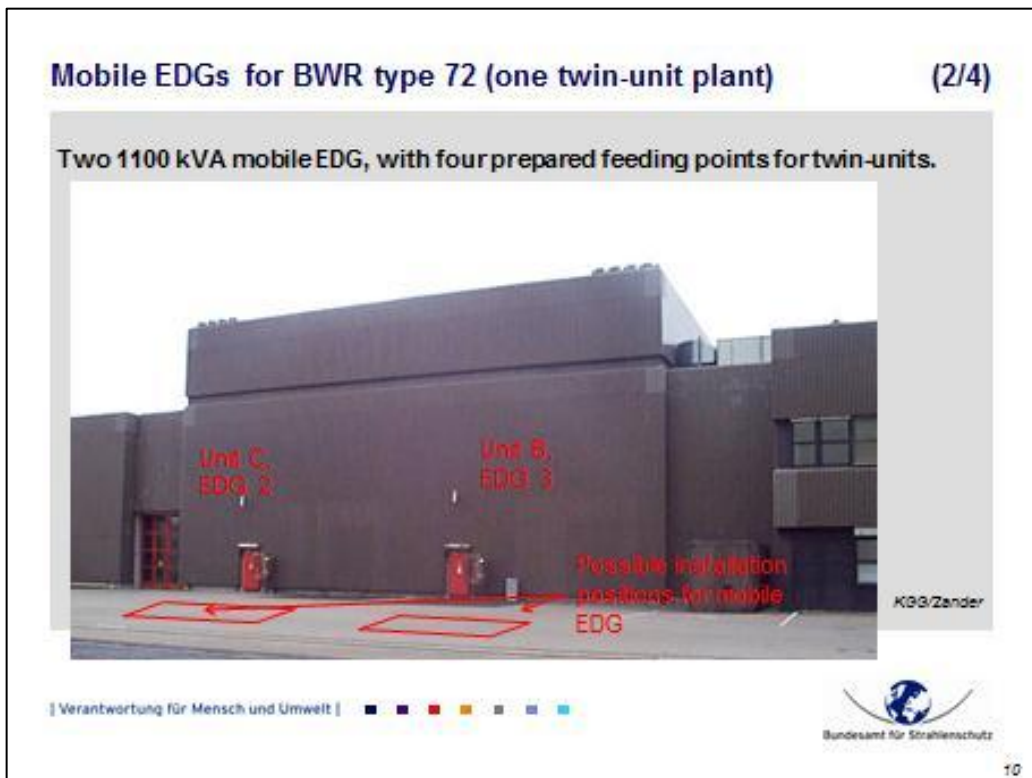
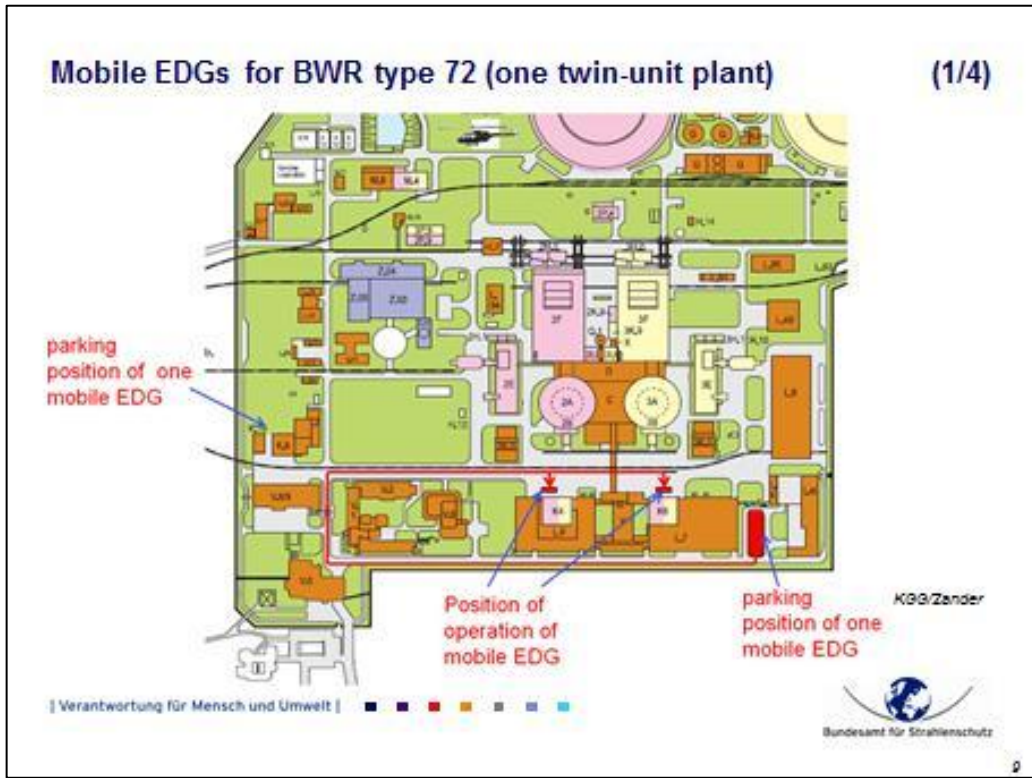
- Concept 2: two medium sized (550 kVA) mobile EDG



| Verantwortung für Mensch und Umwelt |



8



Mobile EDGs for BWR type 72 (one twin-unit plant) (3/4)

Modified circuit breaker

EDG building

Supply connection

mobile EDG

KGG/Zander

Verantwortung für Mensch und Umwelt

Bundesamt für Strahlenschutz

11

Mobile EDGs for BWR type 72 (one twin-unit plant) (4/4)

Supply connection for mobile EDG

Supplied bus bars

KGG/Zander

Verantwortung für Mensch und Umwelt

Bundesamt für Strahlenschutz

12

Summary

- **History and Status of Nuclear Power Plants in Germany**
- **Changes in the regulatory Framework etc. after Fukushima**
 - 10 h coping time for Station Blackout
 - Postulated loss of all stationary EDG
 - Long time loss of grid connection (e.g. fuel supply)
 - Diverse heat sink
- **Design Basis of Electrical Power Supply in German NPPs**
 - Example: PWR
 - Defense-in-depth-concept
- **Robustness of Electrical System in German NPP: Chernobyl**
 - Emergency grid connection
- **Robustness of Electrical System in German NPP: Fukushima**
 - Examples of implementing Mobile Emergency Diesel Generators

Thanks !



Sebastian A. Meiss
Physicist (Scientific Officer)

Office: Bundesamt für Strahlenschutz
Willy-Brandt-Strasse 5
D-38226 Salzgitter, Germany

Postal address: P.O. Box 10 01 49
D-38201 Salzgitter, Germany

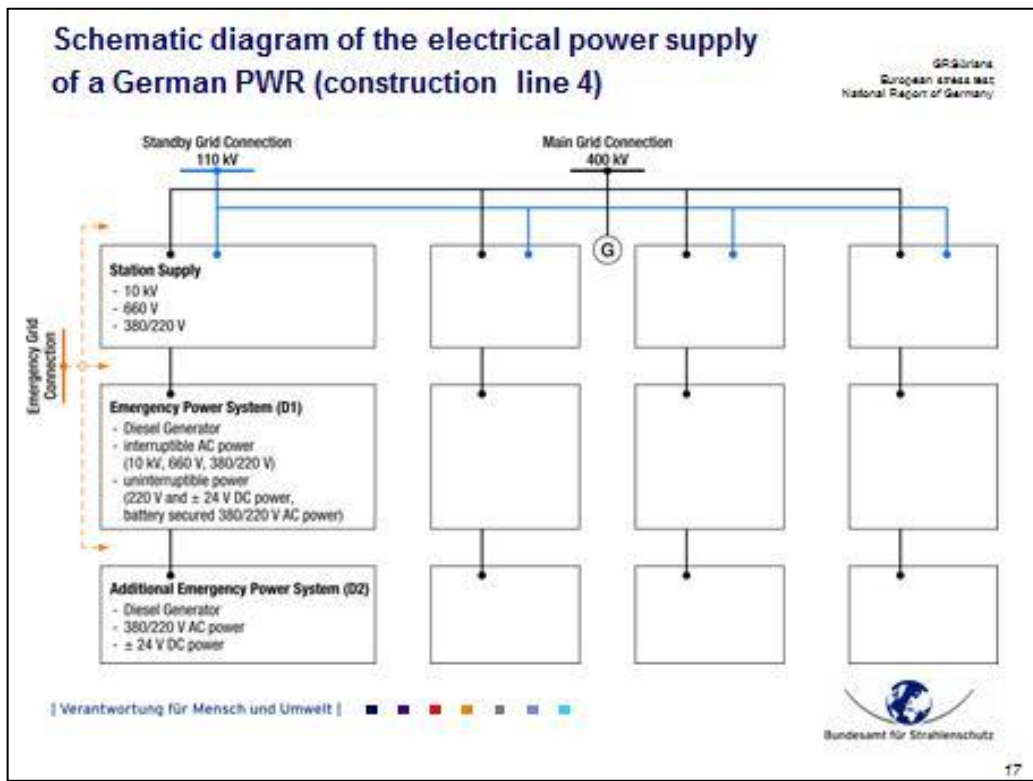
Phone: +49 (0) 30 18333-1062
Fax: +49 (0) 30 18333-1075
E-mail: smeis@bfs.de

ERS

▼ ▼ Extra Slides ▼ ▼

Status of implementation

- All *backfitting measures* after Fukushima are summarized in the German Action Plan, e.g.
 - Purchasing of emergency power generators and installation of protected connection points
 - DC power for at least 10 h (with mobile diesels)
 - Installation of fixed pipelines for fuel pool feeding
 - Analysis of fuel pool integrity, instrumentation etc. in case of steaming
 - SAMGs for all NPPs
 - Creation of diverse service water supply
 - Improvement of robustness of communication tools
- Status
 - Lots of measures are already implemented
 - Nearly all measures will be finalized in the near future
 - Analyses are on-going



Electric power supply, PWR

Design characteristics	Construction line 1 KWO	Construction line 2 KWB-A/B GKNI KKI	Construction line 3 KBR, KKG, KWG, KKP-2	Construction line 4 KKE, KKI-2, GKNI-8
Number of independent off-site power supplies	2	At least 3		
Generator circuit breaker	Not applicable	Yes		
Station supply in the case of loss of off-site power	Not applicable	Yes, load rejection to house-load operation		
Emergency power supply	2 trains with 1 diesel each	4 trains with 1 diesel each	4 trains with 1 diesel each + 1 diesel (physically separated)	4 trains with 1 diesel each (D1 emergency power system)
Emergency power supply to cope with external events	Both trains are protected against external hazards	9 connections between both units + 2 trains with 1 additional diesel each (RZ)	2 of 4 trains are protected against external hazards + 1 additional diesel	4 trains with 1 additional diesel each (D2 additional emergency feed power system)
Uninterruptible DC power supply (battery-buffered)	2 trains with ±24 V each	2 trains with ±24 V each + 4 trains with 220 V each	4 trains with 220 V, ±24 V each + 2 trains with ±24 V each	4 trains with 220 V, ±24 V each (D1-system) + 4 trains with ±24 V each (D2-system)
Battery secured power supply		At least 2 hours		

] Verantwortung für Mensch und Umwelt]
Bundesamt für Strahlenschutz


15

Electric power supply, BWR

Design characteristics	Construction line 69				Construction line 72 KRB B-B/C
	KKB	KKG-1	KKK	KKP-1	
Number of independent off-site power supplies	At least 3				
Generator circuit breaker	Yes				
Station supply in the case of loss of off-site power	Yes, load rejection to house-load operation				
Emergency power supply	4 trains with 1 diesel each	4 trains with 1 diesel each	6 trains with 1 diesel each	2 trains with 2 diesels each	3 trains with 1 diesel each + 2 trains with 1 diesel each
Emergency power supply to cope with external events	2 trains with 1 additional diesel each (UNS)	2 of 4 trains are protected against external hazards	2 of 6 trains are protected against external hazards	2 trains with 1 additional diesel each (USUS)	2 of 3 trains are protected against external hazards + 1 train with 1 additional diesel (ZUNA) + manual connections between both units
Uninterruptible DC power supply (battery-buffered)	2 trains with 220 V, 4 trains with 24 V each + 2 trains with 220 V, 24 V each (UNS)	4 trains with 220 V, 24 V each	6 trains with 220 V, 24 V each	2 trains with 220 V, 24 V each + 2 trains with 220 V, 24 V each (USUS)	3 trains with 220 V, 24 V each + 2 trains with 220 V, 24 V each + 1 train with 24 V each (ZUNA)
Battery secured power supply	At least 2 hours				

GR Gärtringen
European stress test National Region of Germany

] Verantwortung für Mensch und Umwelt | ■ ■ ■ ■ ■ ■ ■

Bundesamt für Strahlenschutz 

19

Design of Mobile EDG at Gundremmingen NPP (BWR72)

Data of mobile EDG:

- diesel engine: Type MTU, 16V 2000 G25, 810 kW
- generator: Type Mecc Alte, 1100 kVA, 400 V
- transformer: 400 V/ 10 kV

-> these three components are part of a single unit on a 40' trailer container

- 10 kV single core cables 1 x 25 mm²
- 10 kV modified circuit breaker

-> these components are stored in the emergency diesel buildings

HGG Zander

] Verantwortung für Mensch und Umwelt | ■ ■ ■ ■ ■ ■ ■

Bundesamt für Strahlenschutz 

20

Demand for Mobile EDG at Gundremmingen Site (BWR72)

- Total Loss of Offsite Power (i.e. 2 main grids + 1 auxiliary grid + 1 emergency grid) +
- 2 out of 2 Main Generators fail to supply House Load +
- 12 out of 12 existing EDG fail to start = Total Loss of AC Power

Leads to

- Initiation of mobile fire fighting pumps (or trucks) to feed water into RPV in both units (twice appr. 1 hour)

followed by

- Initiation of mobile EDG to power one safety train per unit (in total appr. 90 min.)

KGG/Zander

| Verantwortung für Mensch und Umwelt |

21

Implementation of Mobile EDG at Gundremmingen NPP (BWR72)

Consumers supplied by mobile EDG in case of demand:

24-V-converter	27 kVA
220-V-converter	145 kVA
Ventilation in RB	132 kVA
Ventilation in EDG-B	106 kVA
Lighting in RB	66 kVA
Lighting in EDG-B	50 kVA
Sum:	526 kVA

Air compressor for EDG	106 kVA (for start of EDG after repair)
Pressure holding pump	68 kVA (for additional RPV water injection)
Sum:	700 kVA

KGG/Zander

| Verantwortung für Mensch und Umwelt |

22

**Electrical Systems at Laguna Verde Nuclear Power Plant (LVNPP)
after the Fukushima accident**

José Francisco López Jiménez

National Commission for Nuclear Safety and Safeguards, Mexico

Abstract

During the accident occurred in Fukushima Daiichi Nuclear Power Station in Japan, the onsite and offsite electrical systems were affected and lost for a long time with irreversible consequences, therefore, the Mexican Regulatory Body known as the National Commission for Nuclear Safety and Safeguards (CNSNS: for its acronym in Spanish) has taken several actions to review the current capacity of the electrical systems installed at Laguna Verde NPP to cope with an event beyond of the design basis.

The first action was to require to Laguna Verde NPP the compliance with Information Notice 2011-05 “Tohoku-Taiheiyu-Okai earthquake effects on Japanese Nuclear Power Plants” and with 10 CFR 50.54 “Conditions of licenses” section “hh”, both documents were issued by the United States Nuclear Regulatory Commission (USNRC). Additionally, CNSNS has taken into account the response actions emitted by other countries after the Fukushima accident. This involved the review of documents generated by Germany, Canada, United Arab Emirates, Finland, France, the United Kingdom and the Western European Nuclear Regulator's Association (WENRA).

CNSNS made special inspections to verify the current capacity of the electrical systems of AC and DC. As a result of these inspections, CNSNS issued requirements that must be addressed by Laguna Verde NPP to demonstrate that it has the capacity to cope with events beyond the design basis. Parallel to the above, Mexico has participated in the Iberoamerican Forum to address matters related to the “Resistance Tests”, the evaluations of the Forum have reached similar conclusions to those required by European Nuclear Safety Regulators Group (ENSREG), under the format proposed by WENRA. The actions carried out here are closely linked to the requirements established by the USNRC.

It is also important to mention that: 1) the Extended Power Uprate project was implemented in both Units of the Laguna Verde NPP before the accident in Fukushima Daiichi, for this reason the main electrical equipment belonging to the offsite power system was changed and the electrical analysis was reviewed (such as: short-circuit, load flow, electrical stability analysis, etc.), 2) Generic Letter 2006-02 “Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power” is in process of implementation, this aims to verify that it maintains compliance with regulatory requirements which govern electrical systems and 3) the USNRC is in the process of reviewing the 10 CFR 50.63 and Regulatory Guide 1.155 “Station Blackout”, once issued, CNSNS will require its implementation at Laguna Verde NPP.

Based on the above, CNSNS concludes that all actions are being taken to enhance the robustness of Laguna Verde NPP’s electrical systems, in order to increase their reliability, safety and operation as required in order to cope with events beyond design basis as that occurred at Fukushima Daiichi and avoid as far as possible damage to the reactor core.

1. Introduction

The purpose of this paper is to share information on the actions taken by Laguna Verde NPP to strengthen its electrical systems that will support the response to events beyond the design basis; therefore, there is a general description of the electrical systems of the plant, the regulatory aspects concerned with safety issues and the use of the learned lessons from international nuclear community developed from the accident occurred at the Fukushima Daiichi Plant in Japan.

2. General description

2.1 Site

LVNPP has two units with type reactors, of the type BWR5 (Boiling Water Reactor), supplied by General Electric, with primary containment Mark II design, the main condenser is cooled by sea water, from the Gulf of Mexico, both units have a temporary permit to operate at extended power 2,317 MWt (810 MWe). It is owned by the Federal Electricity Commission (CFE) and is located in Punta Limon, municipality of Alto Lucero, on Veracruz State (Figure 1).

2.2 Regulations

The regulation used for the LVNPP is that of the country of origin of the reactor, Title 10, "Energy" Code of Federal Regulations, regulations issued by the Nuclear Regulatory Commission of the United States, including industry standards and guidelines derived from such regulation; additionally, there are the safety standards and guidelines of the International Atomic Energy Agency (IAEA).

2.3 Description ⁽¹⁾ of the electrical systems at LVNPP

These systems are divided into offsite power system and onsite power system, both systems provide enough electric power, whether alternating current (AC) or direct current (DC) to feed the electric loads that lead to LVNPP to the safety shutdown and long term cooling (Figure 2).

2.3.1 Offsite power system

This system is designed to provide a minimum of two reliable sources of electric power from the exterior that provide electrical power to auxiliary systems during starting and shut down of the LVNPP, or at any time when AC power is unavailable from the main generator. This system also has DC power system.

LVNPP is connected to the "Región Oriental" of the national electrical system through electric substations of 400 KV and 230 KV, the connection is made through 7 transmission lines (5 lines of 400 KV system and 2 lines of 230 KV system), these electric substations serve both, Units 1 and 2 at the LVNPP, and are interconnected through an autotransformer.

Some general aspects of the national electrical system ⁽²⁾ are: at December 31, 2010, the effective installed capacity of generation was 52,947 MW, with a total of 833.081 km of transmission and distribution lines. The power plants are of the type: thermoelectric, combined cycle, gas turbines,

(1) Final Safety Analysis Report – LVNPP Units 1 & 2

(2) Programa de Obras e Inversiones del Sector Eléctrico (POISE) 2012-2026

carboelectric, hydroelectric, nuclear power, geothermoelectric. The national electrical system is organized into nine regions: Central, Eastern, Western, Northwest, North, Northeast, Baja California, Baja California Sur and Peninsular, operated under the responsibility of eight control centers, which are managed by the National Center of Energy Control, ensuring coordination for dispatching electric power, operation and security of supply.

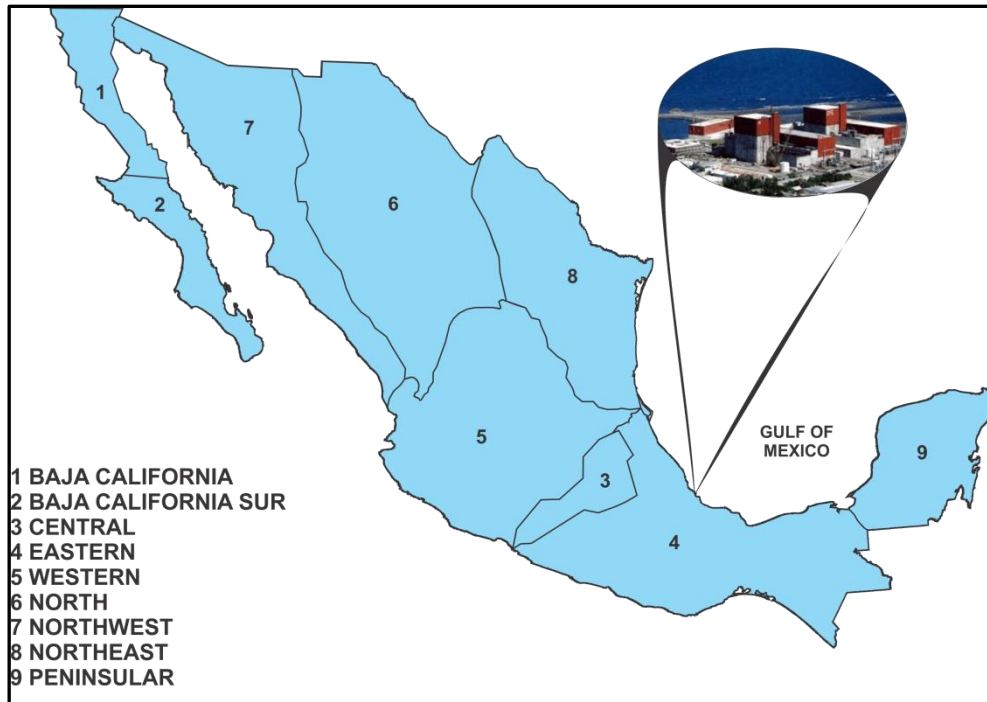


Figure 1 - Location of LVNPP and regions of the national electrical system in Mexico

The following major electrical equipment is part of offsite power system: the main generator, main transformer, normal auxiliary transformer, standby transformer, backup transformer, as well as buses and associated power equipment.

The normal auxiliary transformer supplies the electric power to all auxiliary loads in normal operation, it is used as a source of power during startup and scheduled shut down when the main switch is open and this is the first source of external AC power. The second source of offsite power is the standby transformer that provides backup electric power for all auxiliary loads, it is energized at all times by the 34.5 KV bus 31 and it is only used when the normal auxiliary transformer is inoperable. The normal auxiliary and standby transformers have the same capacity, they reduce the voltage of 34.5 KV to 4.16 KV, are connected to the non-Class 1E Divisions A and B, and provide electric power to the Class 1E Divisions I, II and III.

A third source of offsite power is available from the bus 32 of 34.5 KV connected to the 230 KV system and through the backup transformer provides electric power solely Class 1E Division I or II, when there is an electric power loss from the normal auxiliary and standby transformers, and one standby diesel generator Division I or II fails during safety shutdown. This transformer is used in periodic testing of standby diesel generator Division I or II, it is connected manually and is continuously energized.

The offsite power system also has DC power systems consisting of 250 V_{DC} batteries, 125 V_{DC} batteries and 48 V_{DC} batteries.

2.3.2 Onsite power System

The system is designed to ensure reliable availability of electric power to take the nuclear plant to a safety shutdown and keep it in a safe condition following a design basis accident coincident with the external power loss. For the operation of electric loads, the LVNPP has AC and DC power systems.

The AC power system is formed by Class 1E Division and non-Class 1E Division, both are 4160 V_{AC}. The non-Class 1E Division is formed by Division A (buses 1A/2A and buses 1B/2B bus) and Division B (buses 1C/2C bus): The non-Class 1E Divisions are connected with Class 1E Divisions (Division I for critical bus 1A1/2A1, Division II for critical bus 1B1/2B1 and Division III for critical bus 1C1/2C1), this connection complies with regulatory requirements for physical and electrical separation. Any Class 1E Division I or II is used for the safety shutdown of the reactor or to mitigate the consequences of a loss of coolant accident (LOCA) and/or event loss of offsite power (LOOP). The Division III provides power to the high pressure core spray pump motor and its auxiliary equipment. Both non-Class 1E Divisions and Class 1E Divisions have unit substations to reduce the voltage of 4160 V_{AC} to 480 V_{AC}, these substations feed motor control centers. Furthermore have 120/240 V_{AC} Class 1E uninterruptible power system. During a LOCA event and/or LOOP event, each bus of Class 1E Divisions I, II and III has a standby diesel generator, the capacity for each diesel generator Division I or II is 3676 KW and the capacity for diesel generator Division III is 2200 KW, they generate voltage to 4160 V_{AC} and 60 Hz.

The onsite power system also has DC power system integrated by batteries and associated auxiliary equipment of 24 V_{DC} (Divisions I and II), 125 V_{DC} (Divisions I, II and III) and 250 V_{DC} (Division D). The DC systems are independent, redundant, meet the single failure criterion, have the ability and reliability to supply DC power to all loads Class 1E and non-Class 1E.

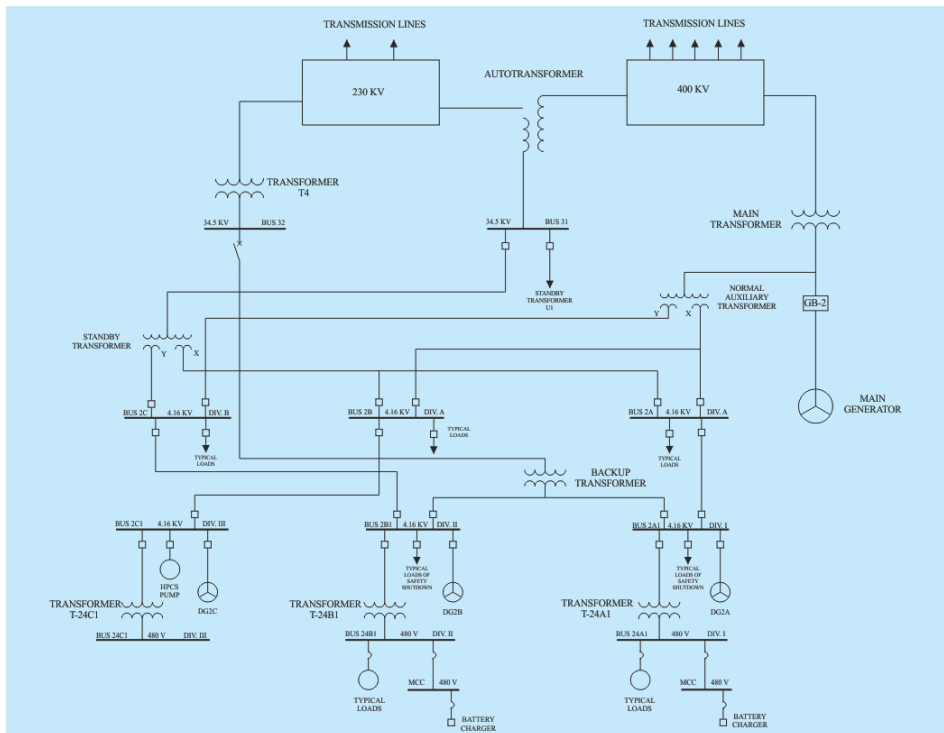


Figure 2 - Simplified Diagram of Electrical Systems in LVNPP-U2

3. Actions at LVNPP before the Fukushima event

It has implemented the power uprate project and it continues with the implementation of the Generic Letter 2006-02, evaluations have considered the concept defense in depth such as design, maintenance, quality assurance and operation, in order to ensure the electric equipment will operate correctly, the following actions are considered contributors in the robustness of the electrical systems and consequently in the robustness of the nuclear plant to cope with events beyond design basis.

3.1 Generic Letter 2006-02 "Grid Reliability and the Impact on Plant Risk and the Operability of offsite Power", this letter was issued by the USNRC after the electric power loss occurred on August 14, 2003, the event affected nine nuclear plants in the United States, in addition to the electrical system of Canada. Its objective is to determine that nuclear plants keep compliance with regulation 10 CFR 50.63 for the SBO rule, 10 CFR 50.65 for the maintenance rule, 10 CFR Part 50, Appendix A, General Design Criteria 2 and 17, 10 CFR 50.120 for training and qualification of personnel and 10 CFR 55.59 for requalification. Currently, implementation of this generic letter is in process and it will verify that the nuclear plant continues to meet the regulatory requirements specified in this the generic letter.

a) The use and management of protocols between LVNPP's operators and transmission system operators, is performed by the National Center of Energy Control, this national center plans, directs and supervises the generation of electric energy, and conducts studies of electrical stability, load flow and short circuit. The analysis tools used to perform electrical studies are used worldwide and Federal Electricity Commission.

- b) The information is considered by LVNPP on the condition monitoring of the electrical grid for risk assessments (10 CFR 50.65) in maintenance activities or maneuvers.
- c) LVNPP has procedures to restore electric power during a SBO in fulfillment with 10 CFR 50.63.

3.2 Power Uprate Project

- a) Main generator, main transformer, normal auxiliary transformer and 400 KV electric substation were changed, for each electric equipment was reviewed its compliance with 10 CFR 50 Appendix A, General Design Criteria (GDC) 2 requires that the nuclear plant is protected against natural phenomena and GDC 17 governs electrical systems.
- b) The electrical protection schemes at the 230 KV electric substation were changed from analog to digital, and two transmission lines of 400 KV were added to increase transmission capacity of the power generated.
- c) The following electrical analysis were reviewed: a) three-phase short circuit with U1 and U2 synchronized to electrical grid and with various operating conditions, the analysis used the software called "Electrical Transmission and Distribution System Analysis Programs and Designs (EDSA)", this software was validated with the IEEE std. 141-1993 "IEEE Recommended Practice for Electric Power Distribution". Currently there is a replacement program for circuit breaker with undersized capacity, b) Load Flow with Units synchronized to electrical grid and consider static state and dynamic state (motor starting), the analysis used the software called EDSA, this software was validated with IEEE std. 399-1997 "IEEE Recommended Practice for Industrial and Commercial Power Systems Analysis (Brown Book)". Although there were low levels of voltage at critical buses, they will not trip the second level of protection against low voltage, to ensure the above, TAP changes were recommended in transformers installed at LVNPP. The software used for both studies was certified according to quality assurance procedures of the LVNPP.
- d) The set points of relays of the second level of protection against low voltage on both units were reviewed, these set points keep compliance with the requirements established in the Branch Technical Position PSB-1 "Adequacy of station electric distribution system voltages" (NUREG 0800 Standard Review Plan).
- e) The electrical stability analysis determined behavior of the nuclear plant and its associated electrical grid in different scenarios, such as steady state and dynamic state, with single and double contingencies, cascading events and scheduled licenses. It is concluded that the electrical stability is kept in all scenarios analyzed.

4. Actions at LVNPP after the Fukushima event

In response to the events that occurred on March 11, 2011 at Fukushima Daiichi nuclear power plant in Japan, the Mexican regulatory body has taken actions at LVNPP, based on international information coming from the USNRC, IAEA and countries of the European Union to verify current capacity of the LVNPP or otherwise take steps to increase their robustness to cope with events beyond of design basis.

Based on the above and in accordance with the objective of the international workshop "Robustness of Electrical Systems of NPPs in Light of the Fukushima Daiichi Accident", it is related with exchange of information on the design and simulation of electrical systems related to plant safety nuclear, are described below the main activities which have been specifically made for electrical systems, emphasizing that such activities are an integral part of the actions taken to increase the robustness at LVNPP.

4.1 Information Notice (IN) 2011-05 "Tohoku - Taiheiyou -Oki earthquake effects on Japanese Nuclear Power Plants" requires ensuring the nuclear safety at nuclear plants to cope natural events beyond design basis and consider actions, as appropriate to avoid similar problems. This through the verification of the capability at NPPs to establish mitigation strategies that result from severe adverse events, a total loss of power to the NPPs, capability to mitigate flooding and the impact that floods have on inside and outside systems, and the identification of the potential for loss of function of the equipment during seismic events on the site. The verifications were considered during the special inspection IE-02/11-LV1, this information will be given later.

4.2 10 CFR 50.54 "Conditions of licenses" section (hh) (2) requires each licensee develop and implement guidelines and mitigation strategies to maintain or restore core cooling, containment, and the cooling capacity of spent fuel pool under circumstances associated with the loss of large areas of the plant due to explosions or fire and through these strategies should ensure nuclear safety to cope with events beyond the design basis.

The implementation of mitigation strategies are in process according to 10 CFR 50.54 (hh) (2) and NEI-06-12 Rev. 2 "B.5.b Phase 2 & 3 Submittal Guideline", these strategies that contribute to increase the robustness of the electrical systems at LVNPP during an extended SBO are the following:

- DC power supply to energize locally solenoid valves of the Automatic Depressurization System/Safety Relief Valves, to depressurize the Reactor Pressure Vessel (RPV) and inject water with portable pump.
- Using a diesel generator to recharge the Class 1E batteries.
- Using a portable diesel pump.

4.3 Inspection IE-02/11-LV1 "Special inspection to verify the measures applied in the Laguna Verde Nuclear Power Plant in response to the event of fuel damage at Fukushima Daiichi Nuclear Power", this inspection used the instructions of the inspection guide NRC-IM-IT 2515/183 "Followup to the Fukushima Daiichi Nuclear Station fuel damage event" and Information Notice 2011-05 to verify the current capacity of the electrical systems at LVNPP during a total loss of AC electrical power (SBO: Station Blackout), the following activities were performed:

- Verification through inspection of all required equipment are adequate and properly classified, tested and maintained.
- Verification of the capability to cope with a SBO.
- Use of international operational experience.

The following actions resulting from the inspection IE-02/11-LV1 are contributors to the robustness of electrical systems. Currently these topics are in process.

- a) Procedures to cope with a SBO event according to the current 10 CFR 50.63

Table 1 – Procedures to cope with a current SBO at LVNPP

Procedure	Title
Anormal Operation (OA-829)	Loss of external power with start failure of diesel generator
Anormal Operation (OA-853)	Loss of external and internal power
DTO-P9	Procedure to restore the system in case of total collapse
DTO-P10	Procedure for feeding own services at LVNPP from hydroelectric plant Temascal 1 in case of total collapse (115 KV)
DTO-P11	Procedure for feeding own services at LVNPP from hydroelectric plant Temascal 1 in case of total collapse (230 KV)
DTO-P16	Procedure for feeding own services at LVNPP from hydroelectric plant Mazatepec in case of total collapse

The OA-0853 procedure had comments, which have been attended.

- b) Analyze the interconnection of standby diesel generators between Unit 1 and Unit 2, to increase the capacity of the installed batteries, determine the probable recovery time of the external AC electric power and install a ventilating and air conditioning system in room 125 V_{DC} batteries (Division III). Currently, these topics are addressed.
- c) Nuclear plant operators and transmission system operators were trained for a scenario of current SBO, before to the accident of Fukushima Daiichi, this action was considered proactive and shows the interaction between staff of the nuclear power plant and staff of the transmission system organization, the training activities should consider the scenario of extended SBO.
- d) Some cells of batteries of 24 V_{DC}, 125 V_{DC} and 250 V_{DC} at LVNPP U1 were observed with degradation, this situation has been documented and controlled, LVNPP has taken actions related to this issue. During the conduct of inspections shall be verified that the physical condition of all electrical systems is maintained in good state.

4.4 Inspection IE-04/11-LV1 "Special inspection to verify implementation of the rule of total loss of AC electrical power "Station Blackout" (SBO) at LVNPP Units 1 and 2" programs, engineering analysis, procedures, training, equipment, systems and support documentation to implement the SBO rule, meet compliance with the requirements of the 10 CFR 50.63, this inspection was based on inspection guide NRC-IM -TI 2515/120, "Inspection of implementation of Station Blackout Rule Multi-Plan Action Item A-22." The following are the most important actions and contributors to the robustness of electrical systems at LVNPP.

Table 2 – Actions derived from the current SBO at LVNPP

Analysis	Observations
SBO-3.0	Revise reliability program of the standby diesel generators.
	Determine estimated time to restore external AC electric power from hydroelectric plant Temascal (115KV/230 KV) to LVNPP.
	Analyze the installation a DG as backup of the batteries at 230 KV electric substation.
	Establish clearly the responsibilities of LVNPP's operators and transmission system operators regarding 400 KV electric substation, so that this situation will not be an adverse factor that compromises the recovery of electric power for a current or extended SBO.
	Incorporate into the maintenance program the batteries and chargers of 48 V _{DC} and 250 V _{DC} of the 230 KV electrical substation, in addition replace these equipment to ensure that they will be able to feed the loads of the substation and will be available, for example for the restoration of the external electric power toward the LVNPP during a SBO event.
SBO-5.3.1	Tests of batteries from 125 V _{DC} and 250 V _{DC} should consider discharge profiles indicated in the SBO-5.3.1 and SBO 5.3.2 studies.
SBO-5.3.2 SBO-5.3.3	Perform short circuit analysis for CD power systems Class 1E and non-Class 1E, and analysis to determine the remaining capacity of the Class 1E batteries after a 4-hour SBO.
SBO-5.7	Check that all areas where recovery activities will be conducted during SBO have autonomous lighting units (ALU). Standardize maintenance frequency for ALU. Identify ALU by placing a label.

Based on observations from the special inspections IE-02/11-LV1 and IE-04/11-LV1 is important to make follow-up inspections to verify that they have taken the necessary actions in electrical systems to cope with current SBO and extended SBO.

4.5 Resistance tests

In accordance with the agreements established in the Iberoamerican Forum, currently are in the process actions related with "Resistance tests", the following actions are contributors in the robustness of the electrical systems and they are result outcome of the review to events related with LOOP, current SBO, extended SBO and loss of the ultimate heat sink coincident with SBO.

Table 3 – Actions derived from resistance tests at LVNPP

Analysis	Observations
LOOP with or without failure of a standby diesel generator	Procedures to restore a failed standby diesel generator or start the remaining diesel generators.
	Standby diesel generators Divisions I, II and III have availability of diesel fuel for 176 hours and LVNPP can cope with a LOOP for 72 hours, time set on the stage of the Resistance Tests.
Current SBO	Procedure to manually start the reactor core isolation cooling (RCIC) system or the high pressure core spray (HPCS) system.
	Procedures to feed own services at LVNPP from hydroelectric plants Mazatepec and Temascal One in case of total collapse.
	The cooling of the core is adequate during a 4-hour SBO.
	Sensitivity analysis to determine the response of the containment during a SBO event with more than 4 hours and to estimate the time when the Central can support a SBO without any external support before the inevitable occurrence of severe fuel damage.
Extended SBO	Evaluate the feasibility of extending the required minimum time from 4 hours to 8 hours, to cope with a SBO (coping time).
	Analysis for using diesel generator of the Compressed Air System (CAS) to feed battery chargers of 125 VDC and 250 VDC at U1 and analysis for using diesel generator of Integrated Information Process System (SIIP) to feed battery chargers of 125 VDC and 250 VDC at U2.
	Analysis for using portable diesel generators.

4.6 FLEX

LVNPP decided to implement the NEI 12-06 "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide" establishes as main objective the development a specific capacity of the plant to cope with simultaneous events such as "Extended loss of AC Power" (ELAP) and "Loss ultimate heat sink" (LUHS) for an indefinite time through combination of the installed capacity in the plant, onsite portable equipment and offsite resources. With these strategies the defense in depth will be increased to cope with events beyond of the design basis. Some of the strategies considered contributors in the robustness of the electrical systems and that are in process at LVNPP are:

- a) Electric distribution system AC and DC.
- b) Determination of the time for declaring ELAP/LUHS.
- c) Extending the duration of the DC Power.

4.7 The regulatory body has required to LVNPP to consider the information contained in the document NEA/CSNI/R (2009)10 "Defence in Depth of Electrical Systems and Grid Interaction", specifically the related to electrical systems that support a nuclear power plant, these systems can be characterized according with concept defense in depth, in addition to the description of the specific features that contribute to the robustness of such systems.

4.8 New regulation for extended SBO

Currently, the USNRC is in the process of reviewing of the 10 CFR 50.63 and Regulatory Guide 1.155, once issued the final review of the documents, the regulatory body will require their implementation at Laguna Verde NPP. Some relevant topics in the new regulation are:

- a) Establish a minimum coping time of 8 hours for a total loss of AC power.
- b) Establish the equipment, procedures and training required to implement the extended loss of all AC power with coping time of 72 hours for cooling the core and spent fuel pool, and the cooling system of the reactor and the integrity of the primary containment, as needed.
- c) Add offsite resources to support as indicated in the previous point.

5.0 Conclusions

Based on the above:

- Actions were taken prior and after to the Fukushima accident that are in compliance with regulatory requirements.
- These actions consider the concept of defense in depth and contribute to the robustness of the electrical systems.
- These systems will support the Nuclear Plant to increase its reliability, safety and operation to address events beyond the design basis and avoid the possible damage to the reactor cores, in order to protect the public and the environment.
- Future activities will be to follow up any new guidance regarding robustness of electrical systems developed by the external operational experience including the outcomes of this workshop.
- It is worth mentioning that all mitigation strategies will be reflected in the guidance of emergency management at LVNPP.

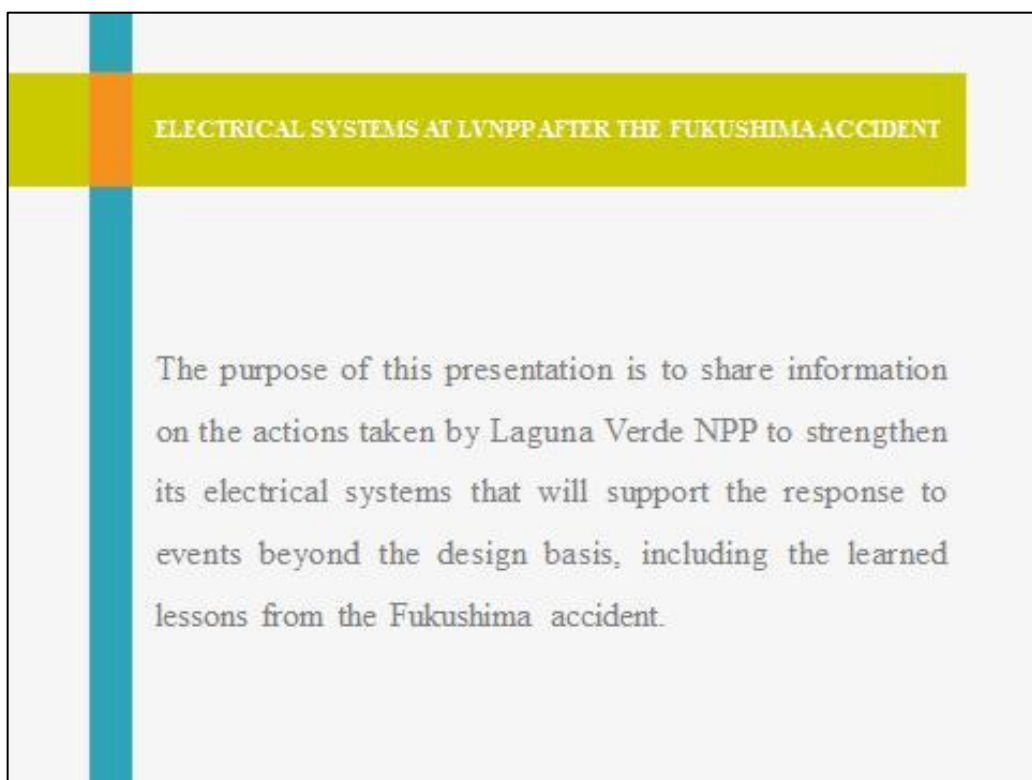


SENER
SECRETARÍA DE ENERGÍA

CNSNS
Comisión Nacional de
Seguridad Nuclear y Salvaguardas

**ELECTRICAL SYSTEMS AT LAGUNA VERDE
NUCLEAR POWER PLANT (LVNPP) AFTER THE
FUKUSHIMA ACCIDENT**

José Francisco López Jiménez
Nuclear Safety Division / Mexico
April, 2014



ELECTRICAL SYSTEMS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

The purpose of this presentation is to share information on the actions taken by Laguna Verde NPP to strengthen its electrical systems that will support the response to events beyond the design basis, including the learned lessons from the Fukushima accident.

ELECTRICAL SYSTEMS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT**OUTLINE**

1. General description of the electrical systems on the plant.
2. Regulatory aspects concerned with safety issues (before and after Fukushima accident).
3. Use of the learned lessons from international nuclear community developed from the accident occurred at the Fukushima.
4. Summary.
5. Conclusions.

ELECTRICAL SYSTEMS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT**GENERAL DESCRIPTION**

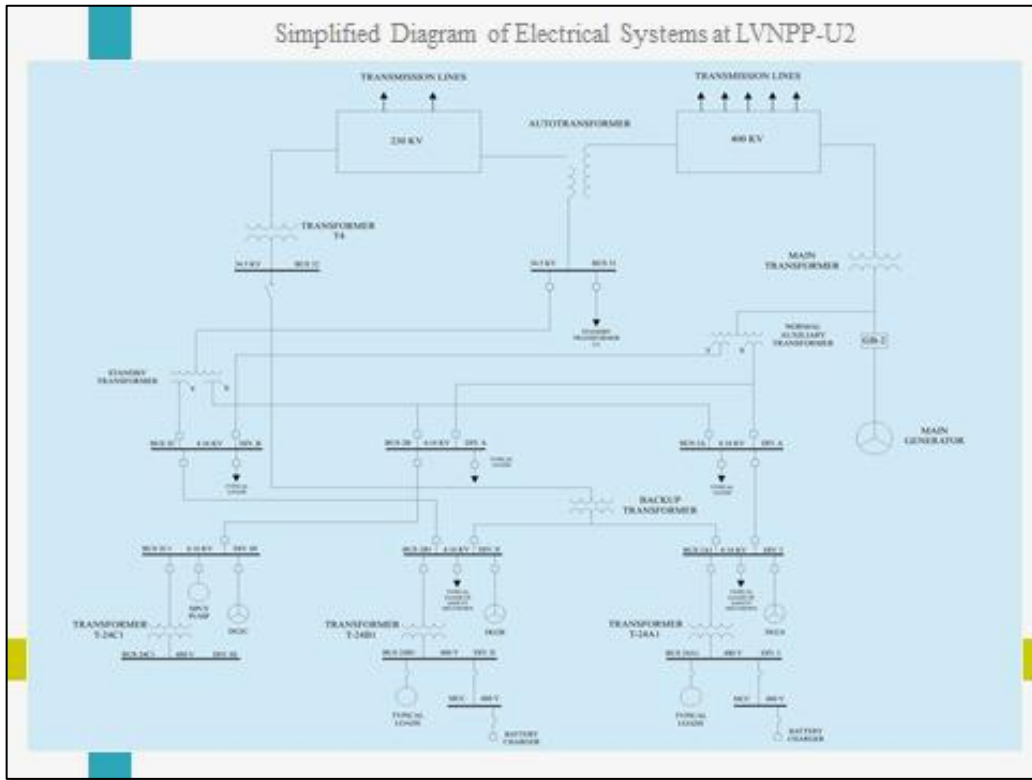
1. LVNPP has Unit 1 and Unit 2.
2. Each Unit is a BWR5 type reactor with primary containment Mark II type.
3. LVNPP is owned by the state owned Federal Electricity Commission (CFE) and is located in Punta Limón, municipality of Alto Lucero, in Veracruz in the Gulf of Mexico.



GENERAL DESCRIPTION

Electrical systems at LVNPP

These systems are divided into offsite power system and onsite power system, both systems provide enough electric power, whether alternating current (AC) or direct current (DC) to feed the electric loads that lead to LVNPP to the safety shutdown and long term cooling.



ACTIONS AT LVNPP BEFORE THE FUKUSHIMA ACCIDENT

Generic Letter 2006-02 "Grid Reliability and the Impact on Plant Risk and the Operability of offsite Power", the regulatory body required the implementation of this document.

- The use and management of protocols between LVNPP's operators and transmission system operators, is performed by the National Center of Energy Control (CENACE) which:
 - plans, directs and supervises the generation of electric energy and conducts electrical studies.
- This information is considered by LVNPP on the condition monitoring of the electrical grid for risk assessment (10 CFR 50.65) in maintenance activities or maneuvers.

ACTIONS AT LVNPP BEFORE THE FUKUSHIMA ACCIDENT

Power Uprate Project

The actions that contribute to increase the robustness of the electrical systems are:

1. The new electric equipment were reviewed and these meet with 10 CFR 50, Appendix A, General Design Criteria 2 and 17.
2. Two transmission lines of 400 KV were added.
3. The following electrical analysis were reviewed: Three-phase short circuit, Load Flow and Electrical stability

ACTIONS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

10 CFR 50.54 "Conditions of licenses" section (hh) (2)

The implementation of mitigation strategies are in process according to 10 CFR 50.54 (hh) (2) and NEI-06-12 Rev. 2 "B.5.b Phase 2 & 3 Submittal Guideline", strategies that contribute to increase the robustness of the electrical systems at LVNPP during an extended SBO are the following:

1. DC power supply to energize locally solenoid valves of the Automatic Depressurization System/Safety Relief Valves, to depressurize the Reactor Pressure Vessel (RPV) and inject water with portable pump.
2. Using a diesel generator to recharge the Class 1E batteries.

ACTIONS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

Inspection IE-02/11-LV1 "Special inspection to verify the measures applied at Laguna Verde Nuclear Power Plant in response to the event of fuel damage at Fukushima Daiichi Nuclear Power"

1. Analyze the interconnection of standby diesel generators between Units.
2. Install a ventilating and air conditioning system in room 125 V_{DC} battery (Division III).
3. Some cells of batteries of 24 V_{DC}, 125 V_{DC} and 250 V_{DC} at LVNPP U1 were observed with degradation, LVNPP has taken actions related to this issue.

ACTIONS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

Inspection IE-04/11-LV1 "Special inspection to verify implementation of the rule of total loss of AC electric power (SBO: Station Blackout)"

1. Analyze the installation a DG as backup of the batteries at 230 KV electric substation.
2. Establish clearly the responsibilities of the 400 KV electric substation.
3. Incorporate batteries and chargers of the 230 KV electric substation into the maintenance program.
4. Perform short circuit analysis for CD power systems Class 1E and non-Class 1E.
5. Review the reliability program for the standby diesel generators.

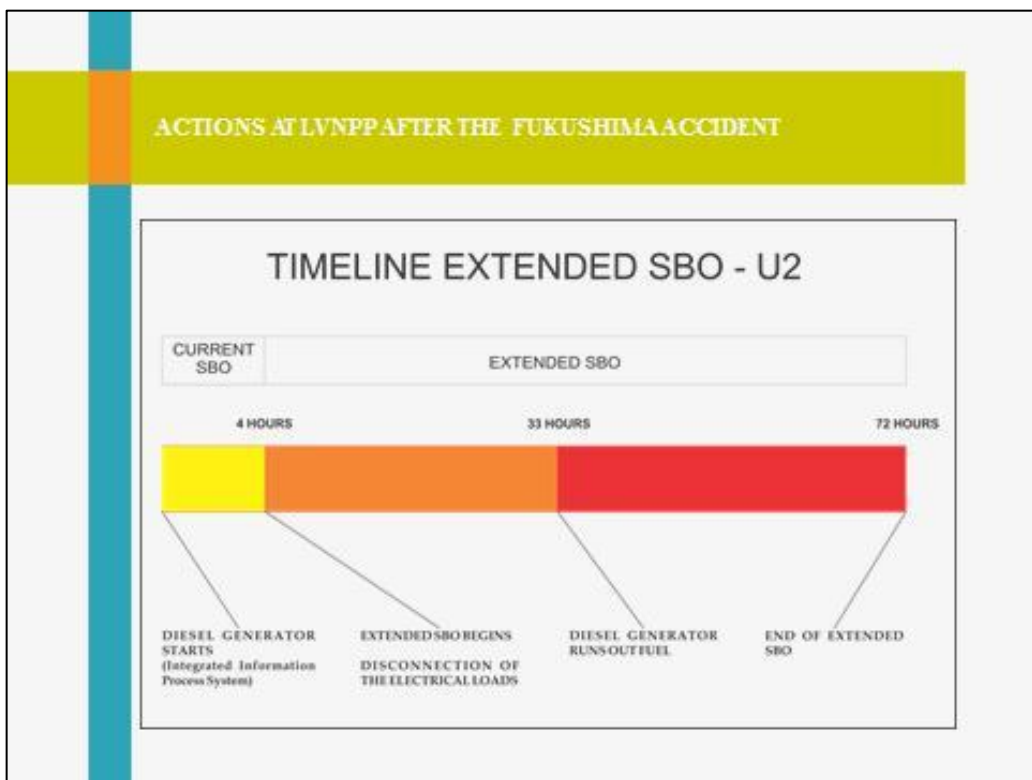
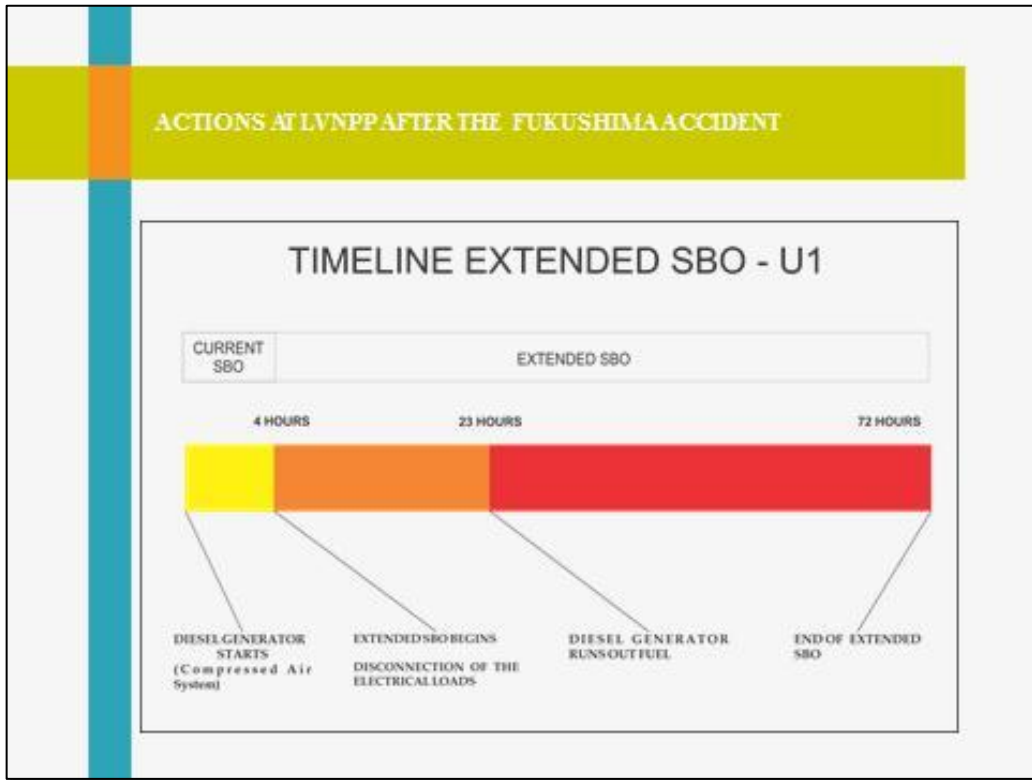
ACTIONS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT	
Resistance tests	
Analysis	Observations
Loss of offsite power (LOOP)	Standby diesel generators have availability of diesel fuel for 176 hours.
Current SBO	LVNPP meets the requirements established in 10 CFR 50.63
Extended SBO	Analysis to increase the coping time from 4 hours to 8 hours.
	Analysis to use diesel generators to feed battery chargers of 125 V _{DC} and 250 V _{DC} at LVNPP. Analysis for using portable diesel generators.

ACTIONS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

NEI-12-06 "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide"

LVNPP decided to implement NEI-12-06. It establishes the development a specific capacity of the plant to cope with simultaneous events such as "Extended loss of AC Power" (ELAP) and "Loss ultimate heat sink" (LUHS) for an indefinite time through combination of the installed capacity in the plant, onsite portable equipment and offsite resources.

1. Electric distribution system AC and DC.
2. Extending the duration of the DC Power.



ACTIONS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

NEA/CSNI/R (2009)10 "Defence in Depth of Electrical Systems and Grid Interaction"

The regulatory body has required to LVNPP to consider the information contained in this document, specifically for the electrical systems that support a nuclear power plant and these can be characterized according with concept of defense in depth, in addition to the description of the specific features that contribute to the robustness of such systems.

ACTIONS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

New regulation for extended SBO

Currently, the USNRC is in the process of reviewing of the 10 CFR 50.63 and Regulatory Guide 1.155. Some relevant topics in the new regulation are:

1. Establish a minimum coping time of 8 hours for a total loss of AC power.
2. Establish the equipment, procedures and training required to implement the extended SBO with coping time of 72 hours for cooling the core and spent fuel pool, and the cooling system of the reactor and the integrity of the primary containment, as needed.
3. Add offsite resources to support as indicated in the previous point.

ELECTRICAL SYSTEMS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

SUMMARY

The actions that were taken are in compliance with regulatory requirements established in:

Prior Fukushima Daiichi:

- Generic Letter 2006-02
- Power Uprate Project



ELECTRICAL SYSTEMS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

SUMMARY (cont.....)

After Fukushima Daiichi:

- 10 CFR 50.54
- NEI-06-12 Rev. 2
- Special inspections
- Resistance tests
- NEI-12-06
- NEA/CSNI/R (2009)10



It is worth mentioning that all mitigation strategies will be reflected in the guidance of emergency management at LVNPP.

ELECTRICAL SYSTEMS AT LVNPP AFTER THE FUKUSHIMA ACCIDENT

CONCLUSIONS

Based on the above:

1. These actions consider the concept of defense in depth and contribute to the robustness of the electrical systems.
2. These systems will support the Nuclear Plant to increase its reliability, safety and operation to address events beyond the design basis and avoid the possible damage to the reactor cores, in order to protect the public and the environment.
3. Future activities will be to follow up any new guidance regarding robustness of electrical systems developed by the external operational experience including the outcomes of this workshop.

Status of the Review of Electric Items in Spain Related to the Post-Fukushima Stress Test Programme

J

Martínez Moreno, Manuel R
Consejo de Seguridad Nuclear, Spain

Pérez Rodríguez, Alfonso
Consejo de Seguridad Nuclear, Spain

Abstract

Spain Authorities has established a comprehensive compilation of the actions currently related to the post-Fukushima program. It has been initiated both at national and international level and it is developed in an Action Plan. This Plan is aligned to the 6 topics identified in the August 2012 CNS-EOM report, and organized in four parts. One of these parts is related to the loss of electrical power and with a clear objective in implemented new features on increase robustness. This program has been reinforced and the task of Electric Issues has been incremented as a consequence of this Plan.

The normal tasks of the Electric Systems and I&C Branch will be presented with the Fukushima related issues as well.

The Consejo de Seguridad Nuclear -CSN-(Nuclear Safety Council) maintains a permanent program of control and surveillance of nuclear safety issues in Spanish Nuclear Power Plants.

The Electric Systems and I&C Branch of the CSN have different tasks related Electric Issues:

- Inspection, control and evaluation of different topics in normal and accidents operation.
- Surveillance Testing Inspections.
- Design Modifications Inspections and evaluation.
- Reactive inspections
- Other activities: Participation in Escered project (a before Fukushima Accident) with an objective of analyzed exterior grid stability and check that electric faults in the NPPs vicinity did not cause the simultaneous loss of the offsite supplies fault effects with interaction in inner related systems. Other task related with the management of aging and long-term operation.

Now, as a consequence, it has been incremented its task with some new Fukushima related topics:

- Analysis of beyond accident related with U.S. SBO Rule (Reg. Guide 1.155) is a part of the design bases for the Spanish plants designed by Westinghouse/ General Electric; switchyard/grid events and extreme weather events are considered, with 10 minutes to

connect an alternate source (if provided; if not, use of d.c. supplied systems is foreseen); possibility of SBO affecting to more than one unit simultaneously at the same site is not considered.

- Analysis of beyond accident related German standards that have been applied to Trillo plant; in particular, batteries were replaced to reach two hours autonomy. This plant has secondary feed&bleed capability (diesel pump); during 2013 will implement primary bleed&feed capability
- ENSREG Specifications. Electric issues assigned to Topic 2 (with Topic 1-external events- inputs); extended SBO, to all the units in the site; 24/72 hours criteria.
- Preliminar NPP reports; preliminary CSN report; final NPP reports; final CSN report (Spanish report). Actions proposed by NPPs were considered acceptable, and were completed with some additional requirements.
- Management 2012: questions/answers round between the European countries. Evaluations in Luxembourg. Topical reports, integrated into the country reports. Peer review inspections, that involved two Spanish NPPs .
- Also during 2012 (in March), CSN issued plant specific Fukushima orders (called ITC-3 instructions). Actions, to be performed in three stages (end of 2012, end of 2014, end of 2016).
- The branch has inspected, during 2011, 2012 and 2013, all the NPPs; in particular, Fukushima selected electric issues. Most important findings and experience shall be shown.
- Also in 2012, CSN issued orders (called ITC-2, ITC-4), related to great areas damages.

This presentation has the objective of describing the current status of the Plan related with Electric Topics in Spanish NPP, and new issues implemented. Additionally, we shall relate the lessons learned of new test and systems implemented in NPP and recent provisions of future actions related to increase on safety and robustness of Electric Systems. Body text [see above]

1. Introduction. Brief consideration of current CSN electrical activities.

The Consejo de Seguridad Nuclear -CSN-(Nuclear Safety Council) maintains a permanent program of control and surveillance of nuclear safety issues in Spanish Nuclear Power Plants.

Spain Authority has established a comprehensive compilation of the actions currently related to the post-Fukushima program. It has been initiated both at national and international level and it is developed in the National Action Plan (NACp). This Plan is aligned to the 6 topics identified in the August 2012 CNS-EOM report, and organized in four parts. One of these parts is related to the loss of electrical power and with a clear objective in implemented new features on increase robustness. This program has been reinforced and the task of Electric Issues has been incremented as a consequence of this Plan.

The current main tasks of the Electric Systems and I&C Branch (INEI, in CSN) are briefly be presented here together with the Fukushima related issues as well.

Tasks can be divided in three big blocks: inspection, evaluation, and follow up of generic issues.

Main types of inspections are:

- Design modifications (selected mainly of their apparent safety interest; are performed every two years).

- Design bases of selected components (selected on their PSA importance measure, or on deterministic basis, for instance due to operative experience considerations; are also performed every two years).

- Surveillance requirements (inspectors are present during the performance of selected surveillance procedures, or review the results of others previously performed; during refueling shutdown periods).

- Reactive inspections (subsequent to significant incidents; typically, one or two per year).

Main types of evaluations are:

- Technical Specification changes (all such changes require authorization from the CSN head).

- Design changes that require authorization, because of their nature, as regulated in the relevant specific rule (one recent example is the design change to install the primary system “bleed” in the KWU designed plant).

- Periodic Safety Review (every ten years) & Conditional Application Regulation (every ten years also, this refers to the possible implementation of new not mandatory standards; for instance, lightning protection according to USNRC Reg. Guide 1.204).

- Conclusions on specific generic issues (for instance, activities to solve the observed corrosion issue for MOV magnesium rotors).

Follow up of Generic Issues; for example,

- Process to establish stress/torque windows to set MOV torque switches (US MPR-2524-A document).

- Analysis of selected operational incidents.

- Plant grid interaction (Forsmark event conclusions, US Generic Letter 206-02).

-Electrical independence of remote shutdown panel from cable spreading room & main control room, in case of fire in these rooms.

2.-Nuclear power plants in Spain

There are six nuclear power plants in Spain, with a total of eight units.

- Almaraz (PWR, Westinghouse design, 3 loops; 2 units; located in the west of the country).
- Ascó (PWR, Westinghouse design, 3 loops; 2 units; north east located).
- Vandellós 2 (PWR, Westinghouse design, 3 loops; north east located, not far from the Ascó units).
- Trillo (PWR, KWU design, 3 loops; in the center of the country).
- Cofrentes (BWR-6, General Electric design, Mark III; in the east).

- Garoña (BWR-3, General Electric design, Mark I, on decommissioning process; this can change in some moths, this is addressed later).

3.-SBO considerations before Fukushima accident.

In relation with the US NSSS designed plants, SBO Rule (Reg. Guide 1.155) is a current design bases in Spain; switchyard/grid events and extreme weather events have been considered, with 10 minutes to connect an alternate source (if provided; if not, use of d.c. supplied systems is foreseen); possibility of SBO affecting to more than one unit simultaneously at the same site is not considered.

Related to Trillo plant, German standards have been applied; in particular, batteries were replaced to reach two hours autonomy. This plant, already in advance of the Fukushima accident, had secondary feed capability water injection apart from that supplied by four emergency diesels, because it has a permanent installed diesel pump; during 2013, as a modification unrelated with Fukushima issues, primary bleed capability has been implemented.

4.-Summary of Fukushima related activities, in Spain.

2011 Activities.

Preliminary NPP reports were issued, that were evaluated in the preliminary CSN report.

Some months later, final NPP reports were issued, evaluated in a final CSN report (the “Spanish report”). Actions proposed by NPPs were generally considered acceptable, when completed with some additional requirements.

CSN inspected, during 2011, all the NPPs; in particular, selected electric issues (ENSREG Topic 2 issues) were reviewed.

2012 Activities.

After a detailed questions/answers round between the European countries, evaluations were performed during the meeting in Luxembourg, in particular of the Topic 2 issues; topical reports were integrated into the country reports, together with Topic 1 and Topic 3 issues.

Peer review inspections, in the case of Spain for Almaraz (in March) and Trillo (in September), were performed. Basically, European peer reviews for Spanish NPPs did not include considerations about significant additional improvements considerations, in relation with ENSREG Topic 2 electrical issues.

CSN publishes plant specific Fukushima orders (called ITC-3 instructions). Required actions were schedules to be performed in three stages (end of 2012, end of 2014, end of 2016).

CSN publishes two additional orders (called ITC-2, ITC-4), related to great areas damages mitigation.

National Action Plan (NAcP) was completed, addressing the regulatory actions considered in the CSN (ITC-3) order and the peer review conclusions and ENSREG recommendations, plus Convention conclusions and great areas damage issues.

2013 Activities.

Questions/answers round on NAcPs between the European countries; final sessions on NAcPs, in April.

CSN inspected all the NPPs, in electrical & instrumentation issues. Checking of the work progress implementation was the main objective.

Garoña NPP decides that it will not continue operation. A new CSN Fukushima order was issued, after the evaluation of a plant proposal on that. This new order, in relation with electric & instrumentation requirements, now considers mainly spent fuel pool improvements, apart from some other extended SBO issues (provisions about electric supply & water pumping possibilities, availability of communications systems).

2014 Activities.

All the plants will be inspected. Electrical and instrumentation actions, in general, need to be concluded not later than Dec 31, 2014. Plants without refueling outage in 2014 have basically concluded their modifications.

Garoña has been authorized to ask for resuming its commercial operation, during 2014; final decision of the plant is not known, up to the moment.

5.-Main provisions considered in Spanish NPP

The first provisions were to establish a non-essential D.C. loads dislatching procedures, and proper training. Other was to execute a periodic test of nearby hydroelectric stations alignment.

The study of the impact of batteries loss at the beginning of the accident has been considered; and manual actions have been procedure.

Now, NPP has new equipment that permits the availability of in-plant low voltage mobile DGs and diesel pumps. Also, there have taken provisions to bring additional equipment in 24 hours from a central storage (or from other plants).

Other important provision is to establish additional portable autonomous instrumentation and enhancement of communications and lighting systems.

Finally, all plants have to design and build a new on-site alternative accident management center.

Then we proceed to describe the individual points according to the type of nuclear power plant

Westinghouse design PWR

An important strategy to recover the core cooling is the operation of AFWS turbodriven, d.c. controlled pump. In this case is establish a manual operation of AFWS turbodriven pump, in case of d.c. loss. The option is a local manual operation of secondary steam relief valves. Other provision is establish a backup diesel pump, as an alternative to the AFWS turbodriven pump. For an effective implementation of this strategy is necessary the preparation for the mobile DGs alignment, to supply selected pumps and electric & instrumentation loads.

KWU designe PWR

This plant has a different design of Westinghouse Plants. It has eight (4 safeguards, 4 emergency) safety qualified diesel generators. The initial response requires secondary steam relief valves and MOVs in the auxiliary feed water lines to be opened preferably using current from safeguard train batteries. Next step should be to start the operation of the dedicated fire pump for feeding SGs. This strategy is implemented because the plant has not a turbo driven pump.

Other provisions are the preparation for mobile DGs alignment to supply selected pumps. In this case the plant has incorporated three dedicated electric pumps, apart from some diesel pumps) and electric & instrumentation loads.

GE designe BWR-6

The main strategy is the operation of RCIC system. Its manual operation is not fully possible if additional d.c. controls have not been implemented locally.

In case that RCIC is successfully operated, the main concern is the suppression pool (SP) heating. Careful vessel depressurization, through SRVs is indicated with a simultaneous adequate preparation of water injection by means of diesel pumps in order to keep vessel level. Other additional provision is the SP spraying in order to avoid containment relief to atmosphere in case of unavailability of other heat removal options.

Like other plants the preparation for mobile DGs alignment to supply selected pumps and electric & instrumentation loads and the use of portable instrumentation, if necessary.

GE designed BWR-3

We have inspected this plant recently, during March 2014, in its actual (shutdown) status.

This plant has not a RCIC system; it relies on the operation of its Isolation Condenser (IC), an almost completely passive system.


If the plant confirms his decision of asking for a restart license, evaluations and inspections are expected, likely in the second 2014 semester.

One possible concern with the IC system is the case in which an isolation signal is generated, due to problems with d.c. system due to the accident, that is followed by the loss of the a.c. supplies after the inner isolation valves have been closed. In such condition, these isolation inner valves cannot be reopened

6.-Conclusions

We consider that NPPs in Spain have adequately addressed Fukushima related issues.

CSN has inspected, and continues doing it, all NPPs in Spain, about the electrical & instrumentation issues.



**CONSEJO DE
SEGURIDAD NUCLEAR**
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

1
CSNI. ROBELSYS. Paris, April 1-4, 2014

**STATUS OF THE REVIEW OF ELECTRIC ITEMS IN
SPAIN RELATED TO THE POST-FUKUSHIMA STRESS
TEST PROGRAMME**

Manuel R. Martínez, Alfonso Pérez (CSN, Spain)




**CONSEJO DE
SEGURIDAD NUCLEAR**
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

2
Nuclear Power Plants in SPAIN and Regulatory Body

- Six NPPs, in Spain (8 units).
 - Almaraz (PWR, Westinghouse designed, 3 loops; 2 units).
 - Ascó (PWR, Westinghouse designed, 3 loops; 2 units).
 - Vandellós 2 (PWR, Westinghouse designed, 3 loops).
 - Trillo (PWR, KWU designed, 3 loops).
 - Cofrentes (BWR-6, General Electric designed, Mark III).
 - Garoña (BWR-3, General Electric designed, Mark I, on decommissioning process).
- Regulatory Body :C.S.N. (Consejo de Seguridad Nuclear)



**CONSEJO DE
SEGURIDAD NUCLEAR**
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

3
CSN (INEI) Activities. Main Types of inspections.

- Electric Branch (INEI), in CSN, is mainly involved in inspections and evaluations.
- Main types of inspections are:
 - Design modifications (every two years).
 - Design bases of selected components (on a PSA, or deterministic, basis; every two years).
 - Surveillance requirements (during refueling shutdown periods).
 - Reactive inspections (subsequent to significant incidents).




**CONSEJO DE
SEGURIDAD NUCLEAR**
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

4
Main Types of evaluations

- Technical Specifications changes.
- Design changes that require authorization (f.i., primary system "bleed" installation in the KWU designed plant).
- Generic Issues (f.i., corrosion in MOV magnesium rotors).
- Periodic Safety Review (every ten years) & Conditional Application Regulation (every ten years also, this refers to the possible implementation of new not mandatory standards; f.i., lightning protection according to USNRC Reg. Guide 1.204).




**CONSEJO DE
SEGURIDAD NUCLEAR**
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

5
Fukushima Accidents Related Activities

- **2011**
 - Preliminary NPP and CSN report; final NPP and CSN report ("Spanish report"). Actions proposed by NPPs were considered acceptable, when completed with some additional requirements.
 - All the NPPs in Spain were inspected, by CSN.
- **2012.**
 - Questions/answers round between the European countries. Evaluations in Luxembourg. European evaluation process. Peer review inspections, that involved two Spanish NPPs (Almaraz in March, Trillo in September).
 - CSN issues plant specific Fukushima orders (called ITC-3 instructions), with actions to be performed basically in three stages (end of 2012, end of 2014, end of 2016).
 - CSN issues orders (called ITC-4 instructions), related to great areas damage.




**CONSEJO DE
SEGURIDAD NUCLEAR**
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

6
Fukushima Accidents Related Activities (cont.)


- European peer reviews for Spanish NPPs did not include considerations about convenience of additional significant improvements, in relation with ENSREG topic 2.
- National Action Plan (NACp) was prepared , that addresses CSN (ITC-3) order and peer review conclusions and ENSREG recommendations, plus Convention conclusions and great areas damage issues.
- **2013.**
 - Questions on NACPs, final sessions on NACPs.
 - CSN inspections to all the plants.
 - Garoña NPP decides that it will not continue operating. The CSN order was changed, now basically refers to the spent fuel pool.

 **CONSEJO DE SEGURIDAD NUCLEAR**
www.csn.es

CSNI International Workshop on ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs in Light of the Fukushima Dai-Ichi Accident

7 | Fukushima Accidents Related Activities (cont.)


- **2014.**
 - All the plants will be inspected. Electrical and instrumentation actions, in general, need to be concluded not later than Dec 31, 2014. Plants without refuelling outage in 2014 have basically concluded their modifications.
 - Garoña could ask for resuming its commercial operation, during 2014.

 **CONSEJO DE SEGURIDAD NUCLEAR**
www.csn.es

CSNI International Workshop on ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs in Light of the Fukushima Dai-Ichi Accident

8 | Main provisions considered

- Non-essential D.C. loads dislatching procedures, and training.
- Periodic test of nearby hydroelectric stations alignment.
- Impact of batteries loss at the accident beginning has been considered; manual actions have been procedured.
- Availability of in-plant low voltage mobile DGs and diesel pumps. Provisions to bring additional equipment in 24 hours from a central storage (or from other plants).
- Provision of portable autonomous instrumentation.
- Enhancement of communications and lighting systems.
- New on-site alternative accident management center.




CONSEJO DE
SEGURIDAD NUCLEAR
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

9
Main defence starting actions in Westinghouse designed PWR

- Operation of AFWS turbodriven, d.c. controlled, pump.
- Manual operation of AFWS turbodriven pump, in case of d.c. loss.
- Local manual operation of secondary steam relief valves.
- Provision of a backup diesel pump, as an alternative to the AFWS turbodriven pump.
- Preparation for mobile DGs alignment, to supply selected pumps and electric & instrumentation loads.
- Use of portable instrumentation, if necessary.



CONSEJO DE
SEGURIDAD NUCLEAR
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

10
Main defence starting actions in KWU designed PWR

- This plant has eight -4 safeguards, 4 emergency-, safety qualified diesel generators.
- Initial response requires secondary steam relief valves and MOVs in the auxiliary feed water lines to be opened (preferably using current from safeguard train batteries).
- Next step should be to start the operation of the dedicated fire pump for feeding SGs (the plant has not a turbo driven pump).
- Preparation for mobile DGs alignment, to supply selected pumps (the plant has incorporated three dedicated electric pumps, apart from some diesel pumps) and electric & instrumentation loads.
- Use of portable instrumentation, if necessary.




CONSEJO DE
SEGURIDAD NUCLEAR
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

11
Main defence starting actions in GE designed BWR-6

- Operation of RCIC system. Its manual operation is not fully possible, additional d.c. controls have been implemented, locally.
- If RCIC successfully operated, the main concern is the suppression pool (SP) heating. Careful vessel depressurization, through SRVs, is indicated, with a simultaneous adequate preparation of water injection by means of diesel pumps, to keep vessel level.
- SP spraying is indicated, in order to avoid containment relief to atmosphere in case of unavailability of other heat removal options.
- Preparation for mobile DGs alignment, to supply selected pumps and electric & instrumentation loads.
- Use of portable instrumentation, if necessary.



CONSEJO DE
SEGURIDAD NUCLEAR
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

12
Considerations for the case GE designed BWR-3

- We have inspected this plant recently, during March 2014, in its actual (shutdown) status.
- This plant has not a RCIC system, it relies on the operation of its Isolation Condenser (IC), an almost completely passive system.
- If the plant confirms his decision of asking for a restart license, evaluations and inspections are expected, likely in the second 2014 semester.
- One possible concern with the IC system is the case in which an isolation signal is generated, due to problems with d.c. system due to the accident, that is followed by the loss of the a.c. supplies after the inner isolation valves have been closed. In such condition, these isolation inner valves cannot be reopened.



CSN
CONSEJO DE
SEGURIDAD NUCLEAR
www.csn.es

**CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL
SYSTEMS OF NPPs in Light of the
Fukushima Dai-Ichi Accident**

13Conclusions

- We consider that NPPs in Spain have adequately addressed Fukushima related issues.

- CSN has inspected, and continues doing it, all the NPPs in Spain, about the electrical & instrumentation issues.

THANK FOR YOUR ATTENTION.

Evolution of Onsite and Offsite Power Systems in US Nuclear Power Plants

Roy K. Mathew

U.S. Nuclear Regulatory Commission, USA

Abstract

The AC electric power system is the source of power for station auxiliaries during normal operation and for the reactor protection system and emergency safety features during abnormal and accident conditions. Since the construction of early plants in US, the functional adequacy and requirements of the offsite power systems, safety and non safety related onsite electric power systems have changed considerably to ensure that these systems have adequate redundancy, independence, quality, maintenance and testability to support safe shutdown of the nuclear plant. The design of AC systems has evolved from a single train to multiple (up to four) redundant trains in the current evolutionary designs coupled with other auxiliary AC systems.

The early plants were designed to cope with a Loss of Offsite Power (LOOP) event through the use of onsite power supplies only. However operating experience has indicated that onsite and offsite power AC power systems can fail due to natural phenomena (earthquakes, lightning strikes, fires, geomagnetic storms, tsunamis, etc.) or operational abnormalities such as loss of a single phase, switching surges or human error. The onsite DC systems may not be adequately sized to support plant safe shutdown over an extended period if AC power cannot be restored within a reasonable time.

This paper will discuss the requirements to improve availability and reliability of offsite and onsite alternating current (AC) power sources to U.S. Nuclear Power Plants. In addition, the paper will discuss the requirements and guidance beyond design basis events.

1. Commission's Policy Statement and Safety Goals

Commission's Policy Statement on Safety Goals for the Operations of Nuclear Power Plants, which appeared in the Federal Register in August 1986 (51 FR 30028). The approach includes the agency's historical commitment to a defense-in-depth philosophy that ensures that the design basis includes multiple layers of defense.

The Policy Statement on Safety Goals sets forth two qualitative safety goals, which are supported by two quantitative supporting objectives. The following are the qualitative safety goals:

Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.

Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

The quantitative supporting objectives are as follows:

The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of

prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.

In the Policy Statement on Safety Goals, the Commission emphasized the importance of features such as containment, siting, and emergency planning as “integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy.” A cursory review of documents discussing the agency’s approach to defense-in-depth provides a range of explanations and applications.

The Commission’s policy on probabilistic risk assessment (PRA) (“Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities,” dated August 16, 1995), states the following:

Defense-in-depth is a philosophy used by the NRC to provide redundancy for facilities with “active” safety systems, e.g. a commercial nuclear power [plant], as well as the philosophy of a multiple-barrier approach against fission product releases.

An instructive discussion of the defense-in-depth philosophy also appears in director’s decisions relating to a petition on Davis-Besse (FirstEnergy Nuclear Operating Company (Davis-Besse Nuclear Power Station, Unit 1), DD-03-3, 58 NRC 151, 163 (2003)).

The decision described defense-in-depth as encompassing the following requirements:

- (1) require the application of conservative codes and standards to establish substantial safety margins in the design of nuclear plants;
- (2) require high quality in the design, construction, and operation of nuclear plants to reduce the likelihood of malfunctions, and promote the use of automatic safety system actuation features;
- (3) recognize that equipment can fail and operators can make mistakes and, therefore, require redundancy in safety systems and components to reduce the chance that malfunctions or mistakes will lead to accidents that release fission products from the fuel;
- (4) recognize that, in spite of these precautions, serious fuel-damage accidents may not be completely prevented and, therefore, require containment structures and safety features to prevent the release of fission products; and
- (5) further require that comprehensive emergency plans be prepared and periodically exercised to ensure that actions can and will be taken to notify and protect citizens in the vicinity of a nuclear facility.

2. General Design Requirements for Electric Power Systems

Under the provisions of Title 10 of the Code of Federal Regulations (CFR) 50.34, 52.47, 52.79, 52.137, and 52.157, an application for a construction permit, a design certification, combined license, design approval, or manufacturing license, respectively, must include the principal design criteria for a proposed facility. The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety; that is, structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

These General Design Criteria (GDC) establish minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have been issued by the Commission. The GDC are also considered to be generally applicable to other types of nuclear power units and are intended to provide guidance in establishing the principal design criteria for such other units. The principal design criteria for earlier Nuclear Power Plants (pre-GDC) follow the requirements specified by the Atomic Energy Commission (AEC) rules published for 10 Part 50 in the Federal Register on July 11, 1967, and February 10, 1971.

Two key GDCs for the electric power system are provided in GDCs 17 and 18. GDC 17, "Electric Power Systems," in Appendix A to Part 50 establishes design requirements for the electric power systems (both offsite and onsite power systems) of nuclear power plants. Specifically, GDC 17 states: An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components (SSCs) important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences, and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

GDC provides definition for single failure as applied to safety related systems. Specifically, it states that a single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions

GDC 17 explicitly states that the offsite and onsite power system design must meet the failure criterion on a system basis without loss of capability to provide power for all safety functions. By definition of single failure criterion, the complete onsite electric power system (Class 1E) must be capable of sustaining a single failure without loss of capability to provide power for the minimum required safety functions. Hence, the offsite and onsite power systems considered together must be capable of sustaining a double failure, one of which is complete loss of offsite power coupled with a single failure in the onsite power system without loss of capability to provide power for the minimum required safety functions.

The offsite power source is also the 'preferred power supply' as it is preferred to furnish electric energy under accident or post-accident conditions. It is highly reliable and available to mitigate the consequences of all anticipated operational occurrences. It is capable of: Starting and operating all required loads for normal operation and providing power for the shutdown of the station and for the operation of emergency systems and engineered safety features.

Operating experience and a number of probabilistic risk assessments have identified a number of issues significant to reactor safety. To improve the availability and reliability of electric power system evolutionary advanced light water reactors (ALWRs), the staff determined that feeding the safety buses from the offsite power sources through nonsafety buses or from a common transformer winding with nonsafety loads is not the most reliable configuration. Such an arrangement increases the difficulty in properly regulating voltage at the safety buses, subjects the safety loads to transients caused by the nonsafety loads, and adds additional failure points between the offsite power sources and safety loads. Therefore, it is the staff's position that at least one offsite circuit to each redundant safety division should be supplied directly from one of the offsite power sources with no intervening nonsafety buses in such a manner that the offsite source can power the safety buses upon a failure of any nonsafety bus. In addition, the staff recommended an additional source of power would significantly reduce the number of plant trips

that involve a loss of power to the nonsafety loads and require that the plant be shut down under natural circulation. Such an additional source of power would improve plant safety, because these events continue to be identified as more severe than the turbine-trip-only event in standard plant safety analysis reports. These proposed improvements were approved by the Commission on August 15, 1991.

GDC 18, "Inspection and Testing of Electric Power Systems," of Appendix A to 10 CFR Part 50 requires that electric power systems important to safety be designed to permit appropriate periodic inspection and testing to assess the continuity of the systems and the condition of their components.

Surveillance Requirements and Limiting Conditions for Operation

In accordance with GDC 17, an electric power system is required to supply power to loads important to safety in an NPP. Nuclear plants with more power sources than the number of sources required by GDC 17 may be able to withstand the multiple failures and still satisfy the limiting conditions for operation (LCOs). However, during the normal course of operation, any NPP may lose power sources to the extent that the LCOs are not met. Regulatory Guide 1.93, Revision 1, "Availability of Electric Power Sources," provides specific guidance to address situations in which the number of electric power source is less than the adequate number of power sources. During plant operation, the plants are required to have two qualified offsite power sources and two onsite power systems including redundant DC and vital AC power supplies (inverters).

Plant systems that can adversely impact safe shutdown capability have restrictions on outage times mandated by Federal Regulations. Specifically 10 CFR 50.36(c)(2), requires that the technical specifications (TS) include the limiting conditions for operation (LCOs), which are defined as the lowest functional capability or performance levels of equipment required for safe operation of the facility. Furthermore, the same regulations require that, when an LCO of a nuclear reactor is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the TS until the condition can be met. The operational restrictions in the TS are based on meeting the LCO, period of continued operation, and orderly shutdown. In addition, the same regulation in Section (c)(3) requires test, calibration, or inspection for equipment to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met. The surveillance requirements and their frequencies are specified in each NPP's TS.

Extension of Allowed Outage Times or LCOs for Electric Power Sources

Regulatory Guide (RG) 1.93 provides guidance with respect to operating restrictions, that is Allowed Outage Time (AOT), if the number of available onsite emergency diesel generators (EDGs) and offsite power sources is less than that required by the TS. In particular, this RG prescribes a maximum AOT of 72 hours for an inoperable onsite or offsite power source. The lessons learned from Blackout events in the U.S indicate that restoration of offsite power will take longer than previously considered, indicating that post-deregulation conditions in the U.S challenge grid reliability. The staff now requires that a supplemental power source be available as a backup to the inoperable EDG or offsite power source, to maintain the defense-in-depth design philosophy of the electrical system to meet its intended safety function. The supplemental source must have capacity to bring a unit to safe shutdown (cold shutdown) in case of a loss of offsite power (LOOP) concurrent with a single failure during plant operation. The staff's objective of requiring an extra (i.e., supplemental) power source for an inoperable EDG or offsite power source is to avoid a potential extended Station Blackout (SBO) event during the period of an extended AOT and to enable safe shutdown (cold shutdown) of the unit if normal power sources cannot be restored in a timely manner.

Grid Reliability

The transmission system is the source of power to the offsite power system. The transmission system is generally demonstrated to have higher availability and reliability than the on-site emergency power system because of the diverse and multiple generators connected to the transmission system. Hence NPPs generally consider offsite power as the primary source (preferred source) of power for cooling down the reactor during normal and emergency shutdowns. This means that the connections to the grid must have adequate capacity and capability to provide rated power to safety grade electrical equipment in the NPP to perform its function. The degree, to which the grid can maintain an uninterrupted power supply to the NPP with sufficient capacity, and with adequate voltage and frequency, is the measure of grid reliability from the point of view of the NPP.

Although NPPs are designed to cope with a LOOP event through the use of on-site power supplies, LOOP events are considered precursors to station blackout. An increase in the frequency or duration of LOOP events increases the probability of station blackout and hence of core damage. Hence it is important that the transmission system can provide a reliable electrical supply to an NPP, with adequate capacity. Faults on the grid system at a significant distance from a NPP can be the cause of reactor trips or the LOOP. In addition to requiring the grid system and the grid connection to the NPP to be reliable, NPPs also require the grid supply to have sufficient capacity, and to be of an appropriate quality, with both voltage and frequency to be maintained within defined ranges. U.S NPPs disconnect or shut down if the grid frequency goes outside the acceptable range, or if the grid voltage becomes so high or low that voltages within the plant are unacceptable. NPPs also require a stable and reliable grid for other reasons:

- So that the number of unplanned trips of the nuclear unit from power caused by grid faults or unusual grid behavior is small compared with the total number of unplanned trips allowed in the design and safety assessments;
- For commercial reasons so that the nuclear units can achieve a high load factor, unconstrained by grid restrictions or grid faults, and that trips caused by grid behavior do not shorten the life of the plant.

The U.S NRC initiated a regulation, 10 CFR 50.65 (a)(4) which requires NPP owners to assess and manage the increase in risk that may result from proposed maintenance activities before performing the maintenance activities. Grid stability and off-site power availability are examples of emergent conditions that may result in the need for action prior to conducting maintenance activities that could change the conditions of a previously performed assessment. Accordingly, NPP owners are required to perform grid reliability evaluations as part of the maintenance risk assessment before performing any grid-risk-sensitive maintenance activities (such as surveillances, post-maintenance testing, and preventive and corrective maintenance). Such activities could increase risk under existing or imminent degraded grid reliability conditions, including (1) conditions that could increase the likelihood of a plant trip, (2) conditions that could increase the likelihood of a LOOP or SBO, and (3) conditions that could have an impact on the plant's ability to cope with a LOOP or SBO event, such as out-of-service risk-significant equipment (for example, a diesel generator used for onsite power, a battery, a steam-driven pump, or an alternate ac power source).

On August 14, 2003, the largest power outage in U.S. history occurred in the Northeastern United States and parts of Canada. Nine U.S. NPPs tripped. Eight of these lost off-site power, along with one NPP that was already shut down. The length of time until power was available to the switchyard ranged from approximately 1 to 6½ hours. Although the on-site DGs functioned to maintain safe shutdown conditions, this event was significant in terms of the number of plants affected and the duration of the power outage. In response, the US nuclear industry developed protocols between the NPP and the transmission system

operator (TSO), independent system operator (ISO), or reliability coordinator/authority (RC/RA) and the use of transmission load flow analysis tools (analysis tools) by TSOs to assist NPPs in monitoring grid conditions to determine the operability of offsite power systems. (In US, after the deregulation of the electric power industry, the TSO, ISO, or RA/RC is responsible for preserving the reliability of the local transmission system. denote these entities). The use of NPP/TSO protocols and analysis tools by TSOs assist NPPs in monitoring grid conditions for consideration in maintenance risk assessments and any impending challenges to the off-site power systems. A communication interface with the plant's TSO, together with training and other local means to maintain NPP operator awareness of changes in the plant switchyard and off-site power grid, is important to enable the licensee to determine the effects of these changes on the operability of the off-site power system. Hence, these protocols and communications help NPP operators in making conservative decisions for onsite power systems to preclude SBO conditions in the event of a LOOP.

A robust grid that can withstand severe perturbations reduces the probability of a loss of off-site power at a NPP. The robustness of the grid system determines the reliability and availability of off-site power and is evaluated using the following contingencies:

- i. The trip of the nuclear power unit is an anticipated operational occurrence (AOO) that can result in reduced switchyard voltage, potentially actuating the plant's degraded voltage protection and separating the plant's safety buses from off-site power. It can also result in grid instability, potential grid collapse, inadequate switchyard voltages, and a subsequent LOOP due to loss of the real and/or reactive power support supplied to the grid from the nuclear unit.
- ii. Grid stability and off-site power availability conditions under postulated transients on the grid system need to be evaluated for grid reliability. The results of the grid stability analysis must show that the loss of the largest single supply to the grid does not result in the complete loss of preferred power. The analysis should consider the loss, through a single event, of the largest capacity being supplied to the grid, removal of the largest load from the grid, or loss of the most critical transmission line. This could be the total output of the station, the largest station on the grid, or possibly several large stations if these use a common transmission tower, transformer, or a breaker in a remote switchyard or substation.

Degraded Grid Voltage Protection

The operating events at U.S. operating plants that led to the NRC staff's position regarding degraded voltage protection for nuclear power plant Class 1E electrical safety buses for sustained degraded grid voltage conditions. Specifically, Electrical grid events at the Millstone Station, in July of 1976 demonstrated that when the Class 1E buses are supplied by the offsite power system, sustained degraded voltage conditions on the grid can cause adverse effects on the operation of Class 1E loads. These degraded voltage conditions will not be detected by the Loss-of-Voltage Relays (LVRs) which are designed to detect loss of power to the bus from the offsite circuit(s). The LVR's low voltage dropout setting is generally in the range of 0.7 per unit voltage or less, with a time delay of less than 2 seconds. As a result of further evaluation of the Millstone events, it was determined that improper voltage protection logic can also cause adverse effects on the Class 1E systems and equipment, such as spurious load shedding of Class 1E loads from the standby diesel generators and spurious separation of Class 1E systems from offsite power due to normal motor starting transients. Another degraded voltage event, in September of 1978, at ANO station demonstrated that degraded voltage conditions could exist on the Class 1E buses even with normal transmission network (grid) voltages, due to deficiencies in equipment between the grid and the Class 1E buses (Offsite/Station electric power system design) or by the starting transients experienced during certain accident events not originally considered in the sizing (design) of these circuits. The staff required all NPPs to implement a second level of undervoltage protection scheme with time delay to protect the Class 1E equipment. The staff positions and guidance to meet the NRC requirements are described in NRC Standard Review Plan, Branch Technical Position 8-6.

Open Phase Protection

NRC staff issued Bulletin 2012-01, "Design vulnerability in Electric Power Systems," after an operating event at Byron Unit 2 revealed a design vulnerability in the electric power system. Specifically, Byron Station, Unit 2 experienced an automatic reactor trip from full power because of an undervoltage condition on the 6.9-kV buses that power reactor coolant pumps. The undervoltage condition was caused by a broken insulator stack of the phase C conductor for the 345 kV power circuit that supplies both station auxiliary transformers. The open circuit created an unbalanced voltage condition on the two 6.9-kV nonsafety-related RCP buses and the two 4.16-kV engineered safety features (ESF) buses. ESF loads remained energized momentarily, relying on equipment protective devices to prevent damage from an unbalanced overcurrent condition. The overload condition caused several ESF loads to trip. For eight minutes, offsite and onsite power systems were not able to perform their safety functions. Operator manual actions were required to start the emergency diesel generators and energize the ESF buses. Recently, Bruce power plant in Canada and Forsmark, Unit 3, in Sweden reported similar events. The NRC is taking regulatory actions for NPPs to install open phase detection and protection schemes for addressing this design vulnerability.

Station Blackout

Station blackout means the complete loss of ac electric power to the essential and nonessential switchgear buses in a nuclear power plant (i.e., loss of offsite electric power system concurrent with turbine trip and unavailability of the onsite emergency ac power system). Station blackout does not include the loss of available ac power to buses fed by station batteries through inverters or by alternate ac sources as defined in this section, nor does it assume a concurrent single failure or design basis accident.

The station blackout (SBO) rule (10 CFR 50.63) evolved from the results of several plant-specific probabilistic safety studies, operating experience, and reliability, accident sequence, and consequence analyses completed between 1975 and 1988. WASH-1400, "Reactor Safety Study," issued 1975, indicated that SBO could be an important contributor to the total risk from nuclear power plant (NPP) accidents. This study concluded that if an SBO persists for a time beyond the capability of the ac-independent systems to remove decay heat, core melt and containment failure could follow.

In 1980, the Commission designated the issue of SBO as Unresolved Safety Issue (USI) A-44, "Station Blackout," and the staff completed several technical studies to determine if any additional safety requirements were needed. NUREG-1032, "Evaluation of Station Blackout at Nuclear Power Plants," issued June 1988, integrated the findings of the technical studies completed for USI A-44. NUREG-1032 presented the staff's major technical findings for the resolution of USI A-44 and provided the basis for the SBO rule and the accompanying Regulatory Guide (RG) 1.155, "Station Blackout," issued August 1988.

The NUREG-1032 evaluation of emergency diesel generator (EDG) train reliability used results and data from NUREG/CR-2989, "Reliability of Emergency AC Power Systems at Nuclear Power Plants," issued July 1983. NUREG/CR-2989 used the fault trees from 18 site probabilistic risk assessments (PRAs) and individual plant examinations (IPEs) to find the EDG failure boundary and classify failures. Consistent with the licensee PRAs/IPEs, the NUREG 1032 analyses of EDG unreliability considered planned and unplanned EDG demands and failures to start and load-run, EDG unavailability due to test and maintenance out-of-service (MOOS) while the reactor was in power and nonpower status, EDG failure recovery, and EDG common-cause failures. EDG MOOS while the reactor is at power can be an important consideration because the plant risk is potentially higher because of the possibility of a demand while the EDG is unavailable. EDG unavailability measurement can be based on the hours the EDG is unavailable or on the number of failures per demand. Both measures are unbiased estimates of EDG unavailability and are comparable so long as both measures are based on the same considerations (i.e., both consider MOOS).

In March 1986, the NRC issued draft RG 1.155, which presented an acceptable method to comply with the SBO rule based on plant-specific characteristics and the dominant risk factors from NUREG-1032. The NRC issued the final RG 1.155 in August 1988, which provided for selection of the SBO coping duration based on plant-specific characteristics, including past unit average EDG train performance criteria and emergency ac power system configuration. In general, the plants could select the 0.975 EDG target reliability level to achieve shorter coping durations.

In November 1987, the Nuclear Management and Resources Council (NUMARC) (subsequently renamed the Nuclear Energy Institute) submitted NUMARC 87-00, “Guidelines and Technical Bases for NUMARC Initiatives Addressing Station Blackout at Light Water Reactors,” issued November 1987, as an alternative to comply with the SBO rule. By reference in RG 1.155, the staff concluded that NUMARC 87-00 contains guidance acceptable to the staff for meeting the SBO rule. The SBO rule requires that the NRC staff complete a regulatory assessment and notify the licensees of the staff’s conclusions regarding the licensees’ response to the SBO rule. The NRC completed safety evaluations for each plant.

Extended Loss of All AC Power

The events that occurred at the Fukushima Daiichi Nuclear Power Plant site, however, highlight the possibility that extreme natural phenomena could challenge the prevention, mitigation, and emergency preparedness defense-in-depth layers that are currently in place under the NRC’s regulatory framework. The NRC’s assessment of insights from the events at Fukushima Daiichi leads the NRC staff to conclude that requirements are necessary for all licensees and applicants (both current and new reactor licensees and applicants including design certifications) to mitigate an extended loss of all ac power condition, including the loss of normal access to the ultimate heat sink resulting from beyond-design-basis external events. In the days following the Fukushima Daiichi nuclear accident in Japan, the NRC Chairman directed the NRC staff to establish a senior-level agency task force to conduct a methodical and systematic review of the NRC’s processes and regulations to determine whether the agency should make additional improvements to its regulatory system and to offer recommendations to the Commission for its policy direction. This direction was provided in a tasking memorandum (COMGBJ-11-0002), dated March 23, 2011, from the NRC Chairman to the NRC Executive Director for Operations. In response to this tasking memorandum, the NRC chartered the Near Term Task Force (NTTF).

In SECY 11 0093, the NTTF provided a number of recommendations to the Commission, including a specific proposal for new requirements for long term station blackout mitigation. The NTTF suggested enhanced station blackout mitigation strategies, within NTTF Recommendation 4.1, as follows:

Initiate rulemaking to revise 10 CFR 50.63 to require each operating and new reactor licensee to: (1) establish a minimum coping time of 8 hours for a loss of all ac power, (2) establish the equipment, procedures, and training necessary to implement an “extended loss of all ac” coping time of 72 hours for core and spent fuel pool cooling and for reactor coolant system and primary containment integrity as needed, and (3) preplan and prestage offsite resources to support uninterrupted core and spent fuel pool cooling, and reactor coolant system and containment integrity as needed, including the ability to deliver the equipment to the site in the time period allowed for extended coping, under conditions involving significant degradation of offsite transportation infrastructure associated with significant natural disasters.

In SRM-SECY-11-0124, the Commission approved the NRC staff’s proposed actions to implement without delay the NTTF recommendations as described in SECY-11-0124. The Commission approved the NRC staff’s proposed prioritization of the NTTF recommendations, including the staff’s proposals for addressing the NTTF recommendations. With regard to the portions of the SRM having relevance to this regulatory action, the Commission directed the staff to:

- Initiate a rulemaking for recommendation 4.1, Station blackout regulatory actions, as an ANPR rather than as a proposed rule.
- Designate the SBO rulemaking associated with NTTF Recommendation 4.1 as a high-priority rulemaking with a goal of completion within 24 to 30 months.
- Craft recommendations that continue to realize the strengths of a performance-based system as a guiding principle. In developing these recommendations, the Commission directed the NRC staff to consider approaches that are flexible and able to accommodate a diverse range of circumstances and conditions. The Commission noted that “in consideration of events beyond the design basis, a regulatory approach founded on performance-based requirements will foster development of the most effective and efficient, site-specific mitigation strategies, similar to how the agency approached the approval of licensee response strategies for the “loss of large area” event under its B.5.b program.”
- Monitor nuclear industry efforts underway to strengthen SBO coping times and consider whether any interim regulatory controls (e.g., commitment letters or confirmatory action letters) for coping strategies for SBO events would be appropriate while rulemaking activities are in progress.
- For NTTF Recommendations 4.2 and 5.1, provide the Commission with notation vote papers for its approval of the Orders once the NRC staff has engaged stakeholders and established the requisite technical bases and acceptance criteria.

In accordance with SRM-SECY-11-0124, the NRC staff provided SECY-12-0025, Proposed Orders and Requests for Information in Response to Lessons Learned from Japan’s March 11, 2011, Great Tohoku Earthquake and Tsunami, to the Commission on February 17, 2012, including the proposed Order to implement enhanced mitigation strategies. As directed by SRM-SECY-12-0025, the NRC staff issued Order EA-12-049, Order Modifying Licenses with Regard to Requirements for Mitigation Strategies for Beyond-Design-Basis External Events, on March 12, 2012 Order EA-12-049 imposed new requirements to implement mitigation strategies to provide additional capability to respond to beyond-design-basis external events, which can lead to an extended loss of ac power and loss of access to the ultimate heat sink. The Commission concluded that the new requirements were necessary to continue to have reasonable assurance of adequate protection of public health and safety. The Order significantly expanded the scope of the regulatory concerns addressed under NTTF Recommendation 4.2 in SECY-11-0124, as discussed below in the section entitled, Consolidation of Recommendation 4 and 7 Regulatory Activities.

The Order requires a three-phase approach for mitigating beyond-design-basis external events that lead to an extended loss of ac power and loss of normal access to the ultimate heat sink condition. The initial phase requires the use of installed equipment and resources to maintain or restore core cooling, containment, and spent fuel pool cooling. The transition phase requires provision of sufficient, portable, onsite equipment and consumables to maintain or restore these functions until they can be accomplished with resources brought from offsite. The final phase requires the capability to obtain sufficient offsite resources to sustain those functions indefinitely. The Commission concluded that the EA-12-049 requirements were necessary for ensuring continued adequate protection of public health and safety.

The NRC staff plans to issue a proposed rule amending NRC regulations to address these scenarios for both current and new reactors. The final regulatory basis for the SBOMS rulemaking, found at ML13171A061, reflects consideration of feedback from the public meeting, comments received on the

draft regulatory basis, and the ACRS interactions where it was practical to do so within the current schedule. The staff believes that the feedback on the draft rule concepts deserves careful consideration and deliberation and is considering this feedback as it develops the proposed SBOMS rule language. The Final Rule is due to the Commission on December 27, 2016.



Evolution of Onsite and Offsite Power Systems in US Nuclear Power Plants



Topics:

- **Design Requirements**
- **Operational Requirements**
- **Current Beyond Design Basis Requirements**
- **Beyond Design Basis Requirements – Fukushima Lessons Learned Action Items**



Design Requirements



General design criterion (GDC) 17, "Electric Power Systems," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," in part, requires:

"An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents."

3

Design Requirements – Cont. Defense in Depth



- Single failure
- Independence
- Redundancy
- Diversity
- Availability/Reliability
- Operating Experience

4

Design Requirements – Defense in Depth (Cont.)



- Second level undervoltage protection or Degraded grid voltage protection
- Open Phase protection
- New Reactor Designs
 - At least one offsite circuit to each redundant safety division should be supplied directly from one of the offsite power sources with no intervening nonsafety buses
 - Additional source of power to improve plant safety

5

Operational Requirements



- 10 CFR 50.36(c)(2), requires that the technical specifications (TS) include the limiting conditions for operation (LCOs), which are defined as the lowest functional capability or performance levels of equipment required for safe operation of the facility. Furthermore, the same regulations require that, when an LCO of a nuclear reactor is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the TS until the condition can be met.
- RG 1.93 - Regulatory Positions
 - The intent of each regulatory position is to implement the safest operating mode whenever the available electric power sources are less than the LCO.
 - Various levels of degradation of the electric power system in order of increasing degradation is incorporated in the TS. Whenever the TS allow unrestricted operation to be resumed, such resumption should be contingent on the verification of the integrity and capability of the restored sources.

6

Operational Requirements (Cont.)



- To Ensure that NPP is in Safe Operating Mode whenever the Available Electric Power Sources are Less than TS LCO.
Continued Power Operation Contingent on the following:
 - Reliability, Availability, and Capability of Remaining Sources
 - Required Maintenance Activities do not Further Degrade the Power System or Jeopardize Plant Safety
 - Continued Compliance With Required Actions in TS

7

Current Beyond Design Basis Requirements

- Station Blackout, Security-Related Events



- **10 CFR 50.54, Conditions of licenses- Section (hh)(2)**
- Each licensee shall develop and implement guidance and strategies intended to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities under the circumstances associated with loss of large areas of the plant due to explosions or fire
- **10CFR 50.63 Loss of all alternating current power**
- (a) *Requirements.* (1) Each light-water-cooled nuclear power plant licensed to operate must be able to withstand for a specified duration and recover from a station blackout as defined in § 50.2. The specified station blackout duration shall be based on the following factors:
 - (i) The redundancy of the onsite emergency ac power sources;
 - (ii) The reliability of the onsite emergency ac power sources;
 - (iii) The expected frequency of loss of offsite power; and
 - (iv) The probable time needed to restore offsite power.

8

Current Beyond Design Basis Requirements Station Blackout (Cont.)



- (2) The reactor core and associated coolant, control, and protection systems, including station batteries and any other necessary support systems, must provide sufficient capacity and capability to ensure that the core is cooled and appropriate containment integrity is maintained in the event of a station blackout for the specified duration.
- The capability for coping with a station blackout of specified duration shall be determined by an appropriate coping analysis. Licensees are expected to have the baseline assumptions, analyses, and related information used in their coping evaluations available for NRC review.

9

Current Beyond Design Basis Requirements Station Blackout (Cont.)



- **Reg. Guide 1.155, Station Blackout**
 - Specifies a method acceptable to the NRC staff for complying with 10CFR50.63
 - Twenty four pages of detailed guidance
 - EDG Target Reliability Levels
 - Restoration of Offsite Power
 - Ability to Cope with a Station Blackout
 - Quality Assurance Guidance for Non-Safety Systems and Equipment

10

Current Beyond Design Basis Requirements Station Blackout (Cont.)



- **NUMARC 87-00**
 - Guidelines and Methodologies for Implementing the Nuclear Management and Resources Council (NUMARC) Station Blackout Initiatives
 - Detailed Guidance, Examples, Topical Reports, and Questions & Answers
 - Endorsed by Reg. Guide 1.155 as Acceptable Guidance for Compliance to 10CFR50.63

11

Beyond Design Basis Requirements Fukushima Lessons Learned Action Items



- **Industry Response - NRC Mitigating Strategies Order (EA 12-049)**
 - Provides a diverse and flexible means to prevent fuel damage while maintaining containment function in beyond design basis external event conditions resulting in an:
 - Extended Loss of AC Power, and
 - Loss of Normal Access to the Ultimate Heat Sink
 - Objective:
 - Establish an essentially indefinite coping capability by relying upon installed equipment, onsite portable equipment, and pre-staged offsite resources

12

Beyond Design Basis Requirements Fukushima Lessons Learned Action Items (Cont.)




United States Nuclear Regulatory Commission
Protecting People and the Environment

- **FLEX employs a three phase approach:**
 - Phase 1 - Initially cope by relying on installed plant equipment,
 - Phase 2 - Transition from installed plant equipment to onsite FLEX equipment,
 - Phase 3 - Obtain additional capability and redundancy from offsite equipment until power, water, and coolant injection systems are restored or commissioned.
- **Diverse and flexible to enable deployment of the strategies for a range of initiating events and plant conditions**

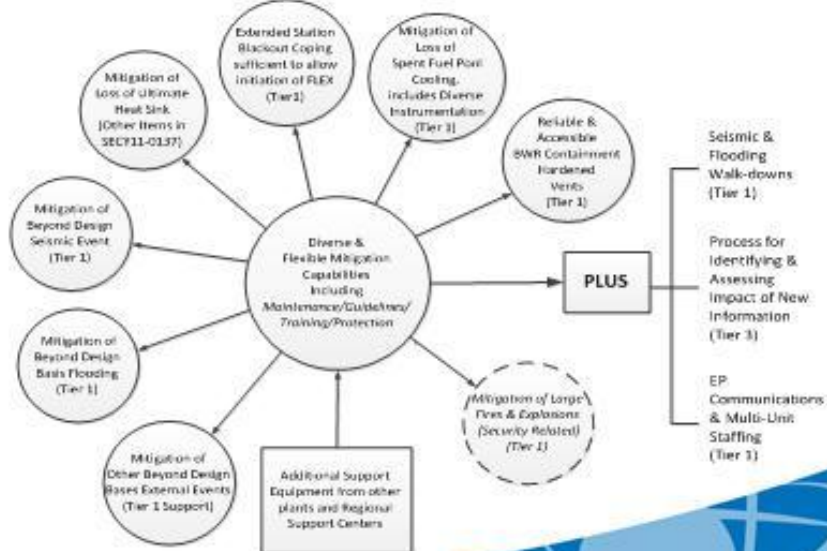



13

Beyond Design Basis Requirements Fukushima Lessons Learned Action Items (Cont.)

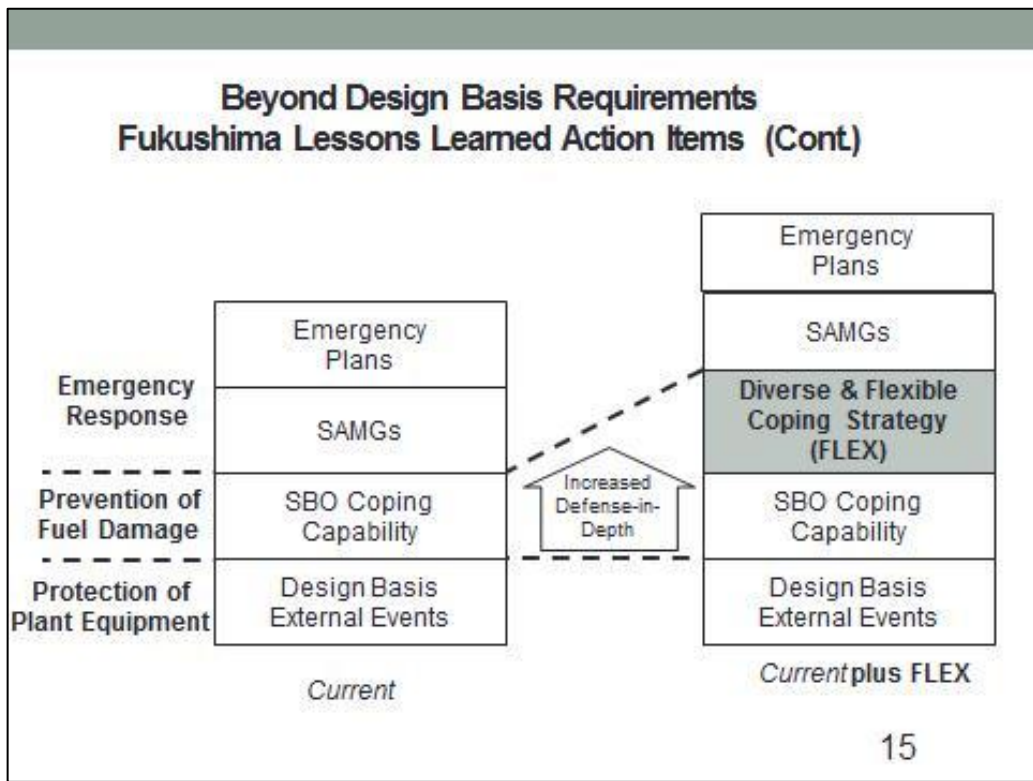


United States Nuclear Regulatory Commission
Protecting People and the Environment





14





U.S. NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment





16

SESSION TWO

"Role of Electric Power in Severe Accident Management"

Implications of Extension of Station Blackout Coping Capability on Nuclear Power Plant Safety
Andrija Volkanovski (JSI, Slovenia)

DC Batteries in NPP, Present and Future Solutions
Gery Bonduelle (ENERSYS, Sweden)

Swiss Solutions for Providing Electrical Power in Cases of Long-term Black-out of the Grid
Franz Altkind, Daniel Schmid (ENSI, Switzerland)

Strengthening the First Line of Defence: Delayed Turbine Trip at SCRAM in Westinghouse Type NPP's
Marcel van Berlo (KFD, The Netherlands)

Implications of Extension of Station Blackout Coping Capability on Nuclear Power Plant Safety

*Andrija Volkanovski
Jožef Stefan Institute, Jamova cesta 39, SI-1000 Ljubljana, Slovenia*

Abstract

The safety of the nuclear power plant depends on the availability of the continuous and reliable sources of electrical energy during all modes of operation of the plant. The station blackout corresponds to a total loss of all alternate current (AC) power as a result of complete failure of both offsite and on-site AC power sources. The electricity for the essential systems during station blackout is provided from the batteries installed in the nuclear power plant. The results of the probabilistic safety assessment show that station blackout is one of the main and frequently the dominant contributor to the core damage frequency.

Results of the analysis of the implications of the strengthening of the SBO mitigation capability on safety of the NPP will be presented. The assessment is done with state-of-art deterministic and probabilistic methods and tools with application on reference models of nuclear power plants.

The safety analysis is done on reference model of the nuclear power plant. Obtained results show large decrease of the core damage frequency with strengthening of the station blackout mitigation capability. The time extension of blackout coping capability results in the delay of the core heat up for at least the extension time interval. Availability and operation of the steam driven auxiliary feedwater system maintains core integrity up to 72 h after the successful shutdown, even in the presence of the reactor coolant pumps seal leakage. The largest weighted decrease of the core damage frequency considering the costs for the modification is obtained for the modification resulting in extension of the station blackout coping capability. The importance of the common cause failures of the emergency diesel generators for the obtained decrease of the core damage frequency and overall safety of the plant is identified in the obtained results.

1. INTRODUCTION

The main purpose of the nuclear safety is the prevention of the release of radioactive materials, ensuring that the operation of nuclear power plants (NPPs) does not contribute significantly to individual and societal health risk. The main specific issue of the nuclear safety is the need for removing the decay heat, necessary even for a reactor in shutdown.

The loss of offsite power (LOOP) initiating event occurs when all electrical power to the plant from external sources is lost. Loss of alternating current (AC) as a result of complete failure of both offsite and on-site AC power sources is referred to as a station blackout (SBO) (NRC, 1988a). The NPPs are equipped with batteries that provide electrical power for the essential safety systems for limited time known as station blackout coping time.

The results of the Probabilistic Safety Assessment (PSA) (AREVA, 2007; Bertucio and Brown, 1990) show that initiating events LOOP and SBO are the most important contributors to the core damage frequency (CDF) including the shutdown CDF (Nishio and Fujimoto, 2011). During an extended SBO functional failure would occur for nearly all instrumentation and control systems leading ultimately to the core damage. The importance of the LOOP and SBO is emphasized in latest guidelines (IAEA, 2012) considering introduction of NPP in the power system of a country.

Following accident at the Fukushima Daiichi NPP the European Council requested that a comprehensive safety and risk assessment, in light of preliminary lessons learned, be performed on all EU nuclear plants (ENSREG, 2012). The request of the Council included “stress tests” performed at national level complemented by a European peer review. The analysis within the “stress tests” has shown that in terms of safety margins, SBO is the limiting case for most of the reactor units (ENSREG, 2012).

This paper presents main results of the analysis of the implications of the modification strengthening the SBO mitigation capability on safety of the NPP (Volkanovski and Prosek, 2013). The analyzed permanent hardware modifications of the NPP power system include installation of additional emergency diesel generator and increase of the batteries capacity. The CDF is the risk measure used for the assessment of the plant safety. The CDF is obtained from the PSA model of the NPP updated and supported by the results of the deterministic safety analysis.

Description of the probabilistic and deterministic input models is given in the following sections. The main findings of the analysis are summarized and presented in the conclusions.

2. NPP MODELS

2.1 Reference deterministic model

The RELAP5 input model of the PWR nuclear power plant is used for the assessment of the nuclear power plant parameters (Prosek and Mavko, 2011; Volkanovski and Prosek, 2013). For RELAP5 calculations the latest version RELAP5/MOD3.3 Patch 4 is used. The input model includes all important components of the reactor coolant system and secondary side, reactor protection system, control systems and safety systems, model of the steam generators and auxiliary feedwater logic.

The following scenarios with or without reactor coolant pumps (RCP) seal leakage and with or without available turbine driven auxiliary feedwater system (TD AFWS) are analyzed:

- SBON – SBO without RCPs Seal LOCA and TD AFWS operational
- SBONP – SBO without RCPs Seal LOCA and TD AFWS operational and PRZ PORV stuck open after first opening
- SBOS – SBO with RCPs Seal LOCA and TD AFWS operational
- SBOS0 – SBO with RCPs Seal LOCA and TD AFWS operational for 0 hours
- SBOS4 – SBO with RCPs Seal LOCA and TD AFWS operational for 4 hours
- SBOS8 – SBO with RCPs Seal LOCA and TD AFWS operational for 8 hours

In the case scenarios with assumed reactor coolant pumps seal leakage a leakage of 1.32 l/s (Krajnc et al., 2011) is considered in the model. The only operator action assumed in the deterministic model is that the steam generator level is maintained at around 70% wide range level. Obtained results from the analyzed scenarios are presented in the following sections.

Fully operational AFW system for given time interval set for specific model is assumed in the analysis, as in the PSA model.

The time interval between the station blackout and start of the core damage is the input parameter used in the probabilistic safety analysis for the assessment of the plant risk. This time interval is assessed from the average fuel cladding temperature at the top of the core.

The typical core cooling success criteria for Westinghouse-type PWR are used (Prior et al., 1994). These criteria are defined in terms of the average fuel/clad temperature with consideration of the period of high temperature instead of the hot rod fuel/clad temperature. The core damage is assumed in the analysis if the hottest core fuel/clad node temperature in the reactor core exceeds 923K for more than 30 minutes or if temperature exceeds 1348 K.

2.2 Reference probabilistic model

The reference PSA model of the PWR nuclear power plant is developed on the basis of the Level 1 PSA model of the Surry Unit 1 NPP (Bertucio et al., 1990) modified to comply with the RELAP5 deterministic input model presented in Section 2.1.

Seven PSA models are developed from the reference PSA model (Volkanovski and Prosek, 2013) corresponding to the following NPP configurations:

- 2EDG - reference PSA model of the NPP;
- 3EDG - PSA model with added third EDG;
- 2EDGB - PSA model with increased batteries capacity;
- 3EDGB - PSA model with added third EDG and increased batteries capacity;
- 3CCF - PSA model with added third EDG and increased CCF of the EDGs;
- 3CCFB - PSA model with added third EDG, increased batteries capacity, increased CCF of the EDGs;
- 3AAC - PSA model with added third diesel generator as a alternate AC source (AAC);
- 3AACS - PSA model with added third EDG utilized as AAC and substitute diesel generator to the existing EDG during normal operation.

The reference PSA model of the NPP has two EDG. The parameters of the added third EDG are equal to the EDG parameters in the reference PSA model. The reference PSA model has batteries with a four hour capacity. The eight hour battery capacity is assumed for the PSA models with increased battery capacity with assumed equal reliability as the four hour battery.

The costs of the analyzed NPP modifications are estimated from the reported costs of the modifications in response to the station blackout rule (NRC, 2003).

The SBO event tree on Figure contains all functional events of a representative SBO event tree for Westinghouse PWRs (NRC, 2005). The station blackout is evaluated in separate event tree because of the phenomenology and special events that can occur. Those events include preservation of coolant inventory, controlled supply of feedwater to the steam generators and extension of battery life (Bertucio et al., 1990). The functional requirements for mitigation of station blackout event are the same as for other transients. Entry into this event tree presumes successful reactor scram. The anticipated transients without scram are addressed in separate event tree.

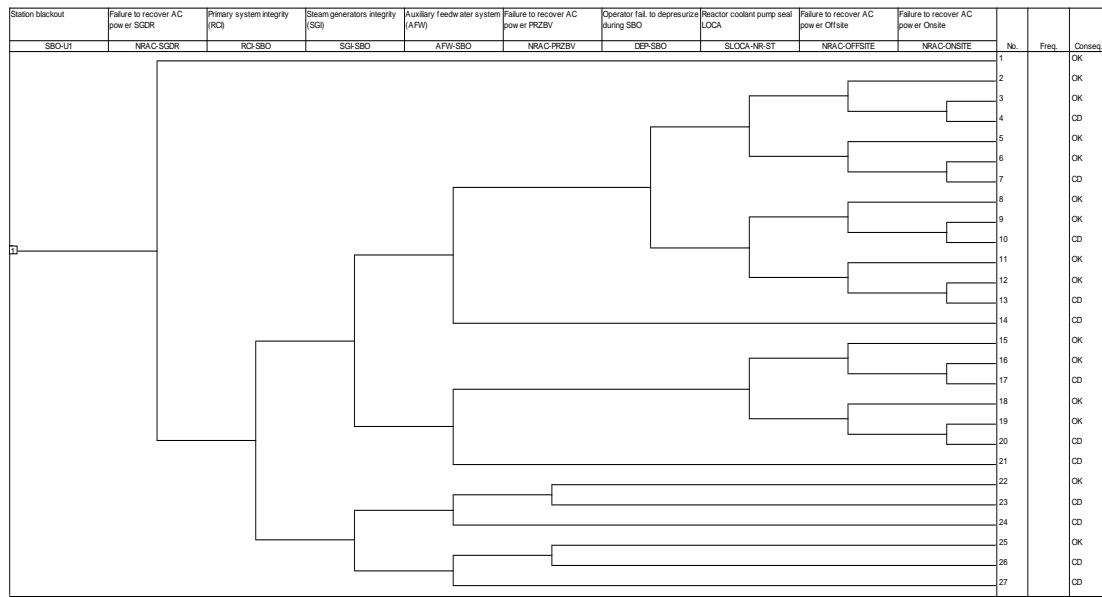


Figure 1: Station blackout event tree

Table 1 shows the basic events with probability of non-recovery of AC power in within restoration time used in reference PSA model, given in second column. The probabilities are given in third column and are obtained as probability of exceedance versus duration curve fits of the offsite power to bus recovery times in the corresponding reference (NRC, 2005). Probability of exceedance for grid related and plant centered LOOP categories (NRC, 2005) are selected as representative data for offsite and on-site power sources. The loss of offsite power initiating event frequency of LOOP=7.70E-2 events/yr equal to the value in original model (Bertucio et al., 1990) is used.

Table 1: Probability of non-recovery of AC power within given time

Basic Event	Description	Restoration time [hr]	Mean unavailability reference model
NRAC-SGDR	Steam generator dryout	0.5	8.25E-1
NRAC-PRZBV	Pressurizer PORV stuck open	1	2.81E-1
NRAC-OFFSITE(4)	AC power restoration offsite	7	6.10E-2
NRAC- OFFSITE(8)	AC power restoration	12	2.00E-2
NRAC- ONSITE(4)	AC power restoration onsite	7	1.78E-2
NRAC- ONSITE(8)	AC power restoration	12	5.85E-3

The implications of the increased CCF probability of the EDG is analyzed with increase of the CCF of all three EDG for factor of two compared to the CCF probability of the EDG in the reference PSA model (Bertucio et al., 1990) given in Table 2.

Table 2: The CCF probability of the three EDG

Basic Event	CCF probability-original	CCF probability-new
BETA-3DG	1.80E-2	3.60E-2

Figure shows that for the plant reference PSA model, with two EDG and four hour batteries capacity the CDF=1.77E-5 [1/yr] is obtained. Figure show that largest contributors to the CDF are LOCA's followed by SBO and LOOP initiating events contributing 34% of the total CDF.

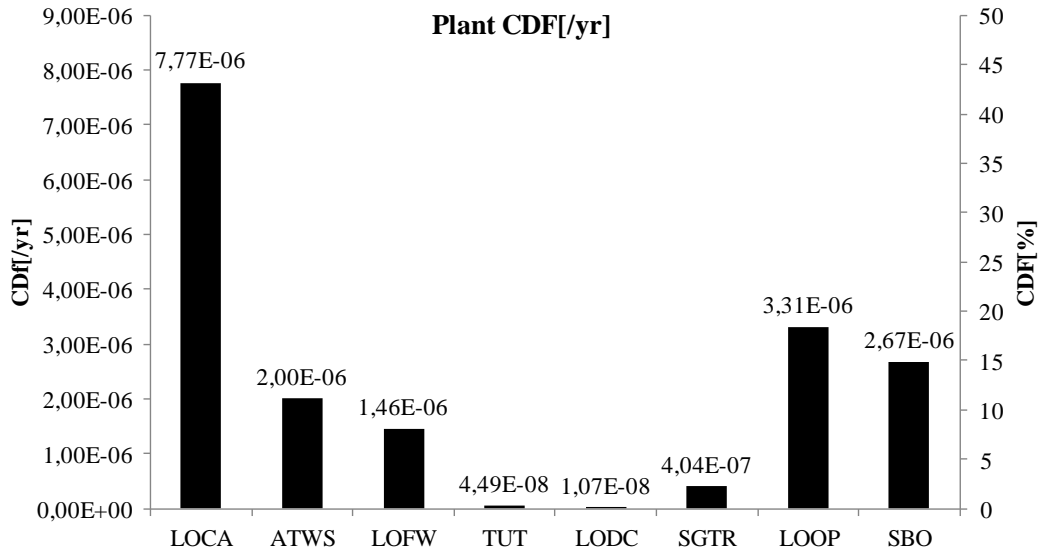


Figure 2: CDF for Internal Initiating Events

3. RELAP5 RESULTS

The results obtained from RELAP5 computer code are shown on Figure for 4 hour time window (scenarios SBONP and SBOS0), Figure for 24 hours time window (scenarios with Seal LOCA) and Figure for 72 hours time window (scenarios with TD AFW operating all the time). The main parameters characterizing the calculations are given on all three figures. These parameters are the RCS pressure, average fuel cladding temperature at the top of the core, RCS mass inventory and SG no. 1 wide range level. The RCS pressure is important in order to know, when pressurizer relief valves open. The fuel cladding temperature gives information if the core integrity is challenged. The RCS mass inventory needs to be sufficient to enable core cooling. It could be lost through RCP leaks and pressurizer relief valves. Finally, cooling through secondary side could be performed when there is sufficient water inventory (level) in the steam generators.

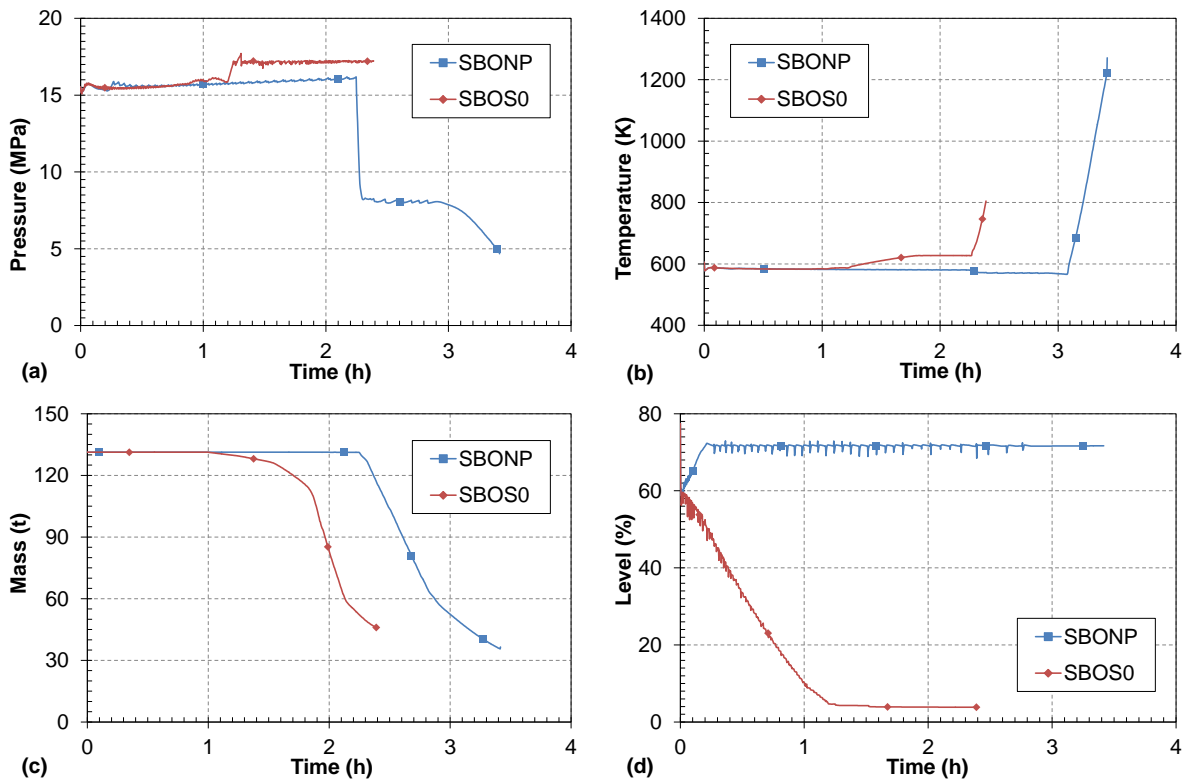


Figure 3: Main calculated parameters characterizing the calculations in 4 hours time window: (a) RCS pressure, (b) average fuel cladding temperature at the top of the core, (c) RCS mass inventory, (d) SG no. 1 level.

When TD AFWS is not functioning from the start of the SBO, as shown by the results for scenario SBOS0 on Figure, the SG wide range level drops below some minimum level in 1 hour.

As explained in Section 2 the deterministic safety analyses are complementing the PSA and are needed to obtain available time to restore AC power before the core integrity is challenged. The initial analyses are done for 4 hours and 24 hours time windows, as shown in Figure and Figure. In addition, it is also investigated the plant response having available battery power source for 72 hours time window (SBON without Seal LOCA and SBOS with Seal LOCA) with results given on Figure . The battery power is needed for instrumentation and control of plant systems including the TD AFW pump. These results are not needed for the present PSA analysis. Nevertheless, from these results one may see that further extension of battery depletion times can prolong the SBO coping times even in presence of Seal LOCA.

In case of the stuck open PRZ PORV (scenario SBONP) the results on Figure show that there are at least 2.5 hours available for restoration of AC power, isolation of the PRZ PORV by the block valve and cooling before the core integrity is challenged.

If TD AFWS is operating for 4 and 8 hours respectively, the results for scenarios SBOS4 and SBOS8 on Figure show that at least 9 and 16 hours are available for restoration of the AC power before the core damage starts. Figure(a) show that the pressurizer safety valve opening in scenario SBOS8 is 6 hours and 13 minutes after safety valve opening in the SBOS4 scenario. The safety valves opening results in large RCS inventory loss leading to core heat up in less than one hour after the valves opening. Due to RCP seal

leaks the RCS pressure, given on Figure(a) and the RCS mass inventory, as shown on Figure(c), are dropping.

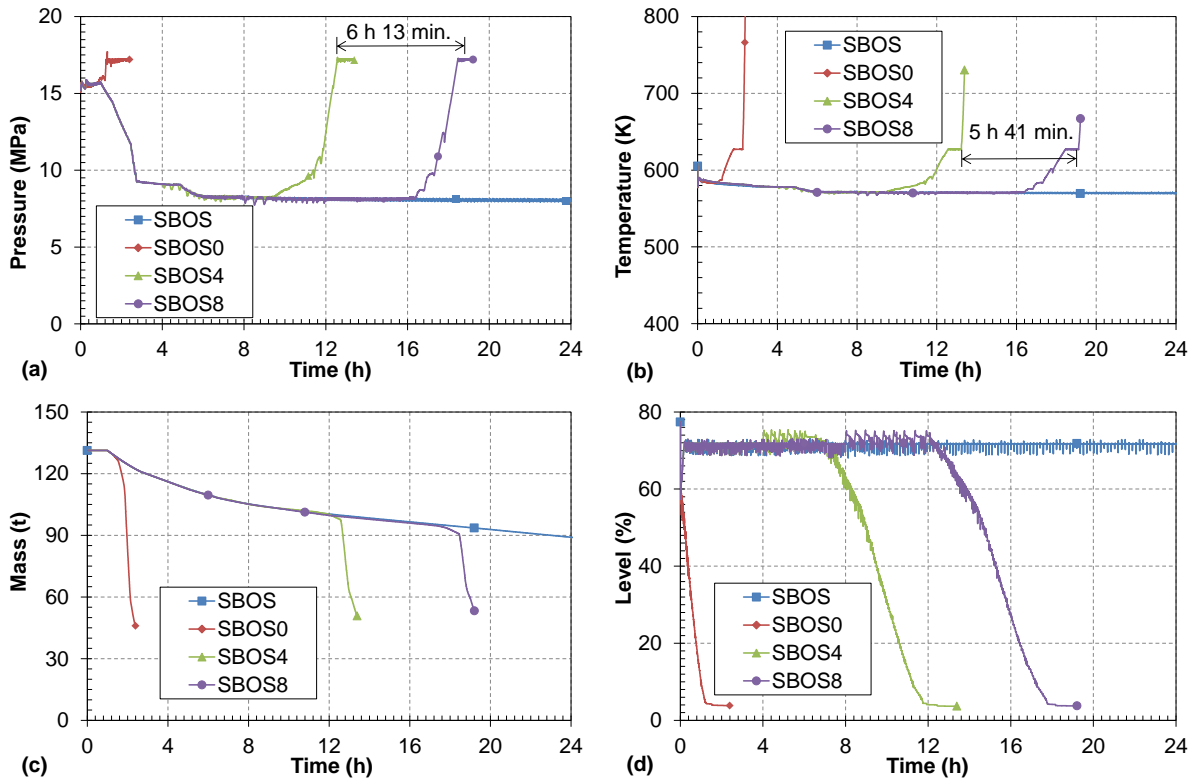


Figure 4: Main calculated parameters characterizing the calculations in 24 hours time window: (a) RCS pressure, (b) average fuel cladding temperature at the top of the core, (c) RCS mass inventory, (d) SG no. 1 level.

Results on Figure(d) for the scenario SBOS shows that the RCS mass remaining in the primary system is sufficient to cool the core for 24 hours in case of operational TD AFWS and operator is maintaining the SG level. The operators have this time window for the restoration of AC power from either on-site or offsite power sources.

Figure shows that in the cases when the TD AFWS is assumed operable all the time (scenarios SBON and SBOS) the core integrity is maintained regardless the RCPs seal leak for at least 72 hours. The RCS pressure, as shown on Figure (a), during transient is dropping to SG pressure, resulting in no RCS mass discharge through pressurizer safety valves. The RCS mass (see Figure (c)) is steadily decreasing for SBOS case due to the coolant loss through the RCP leaks, while in the case of SBON only the first day some RCS mass is released through pressurizer safety valves. Later the RCS mass remains constant. Small drop in RCS mass at the end of the analyzed period when reflux condensation started is due to the numerical error. In the first 72 hours the RCS mass is sufficient in both cases to prevent core damage as shown on Figure (b). In the SBOS scenario the remaining mass of coolant in RCS after 72 hours is about 45 t, therefore the core damage is expected in the next 12 hours. Based on this results it is concluded that the operators have at least 72 hour time window for the restoration of AC power from either on-site or offsite sources when the TD AFWS is operable.

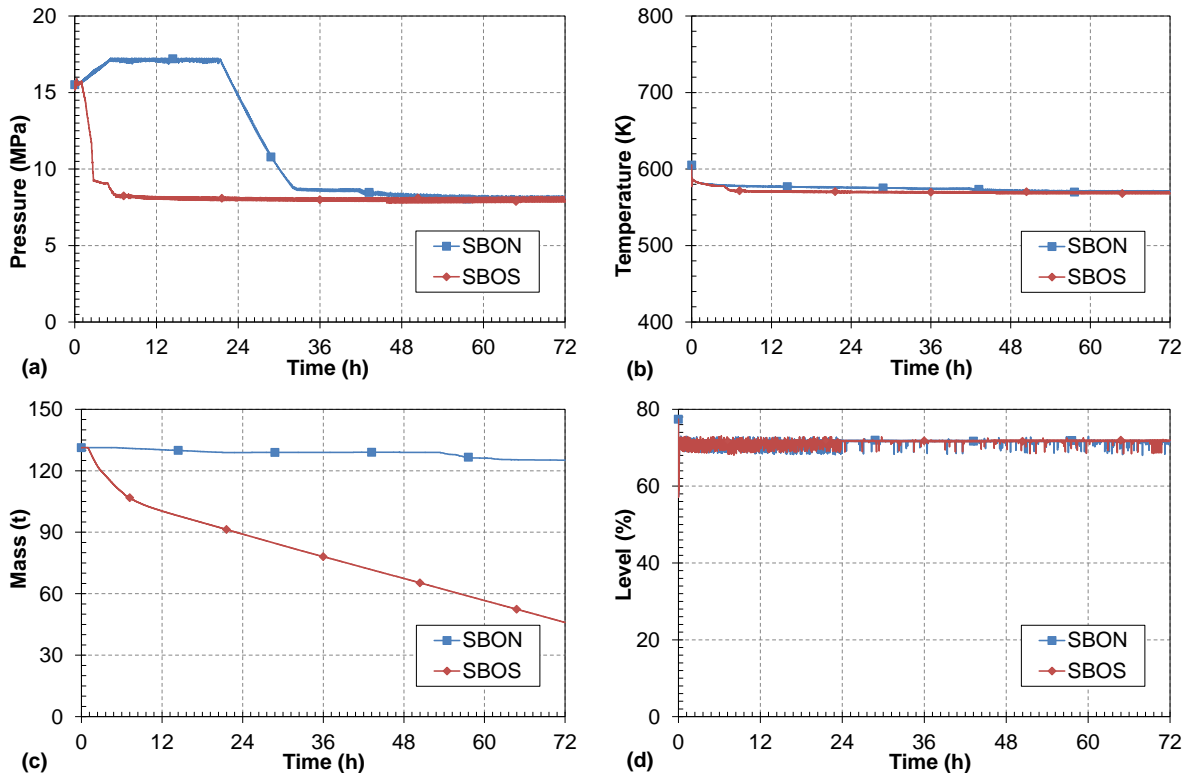


Figure 5: Main calculated parameters characterizing the SBON and SBOS calculations in 72 hours time window: (a) RCS pressure, (b) average fuel cladding temperature at the top of the core, (c) RCS mass inventory, (d) SG no. 1 level.

4. PSA RESULTS

Obtained decrease of the core damage frequency Δ CDF, given in percentiles of the CDF of the reference PSA model with two EDG, for analyzed PSA models and NPP configurations presented in Section 2.2 is given on Figure .

Figure show that largest Δ CDF is obtained for 3EDGB model with additional EDG and increased batteries capacity. Comparable Δ CDF is obtained for 3EDG model with added third EDG and 3CCFB model with increased batteries capacity, third EDG and increased CCF.

The obtained Δ CDF for model 2EDGB is almost twice smaller than the decrease in 3EDGB obtained with the installation of the third EDG.

The increase of the CCF of the EDG results in decrease of the obtained Δ CDF from the modification as shown in result for the 3CCF model given on Figure . The obtained Δ CDF for the 3CCFB is comparable to the results of 3EDGB model. Obtained result show that 3EDGB model with increased batteries capacity has smaller sensitivity to the CCF of the EDG compared to the 3CCF model. This result is expected considering the exclusion of the CCF of the batteries and EDG in the model.

Figure show that Δ CDF obtained in model 3AAC with introduction of third diesel generator as an alternate AC source is comparable to the Δ CDF of the 3CCF model. The obtained Δ CDF is increased in

the 3AACS model with the utilization of the alternate AC source as substitute of the existing EDG going under maintenance decreasing their unavailability as a result of test and maintenance.

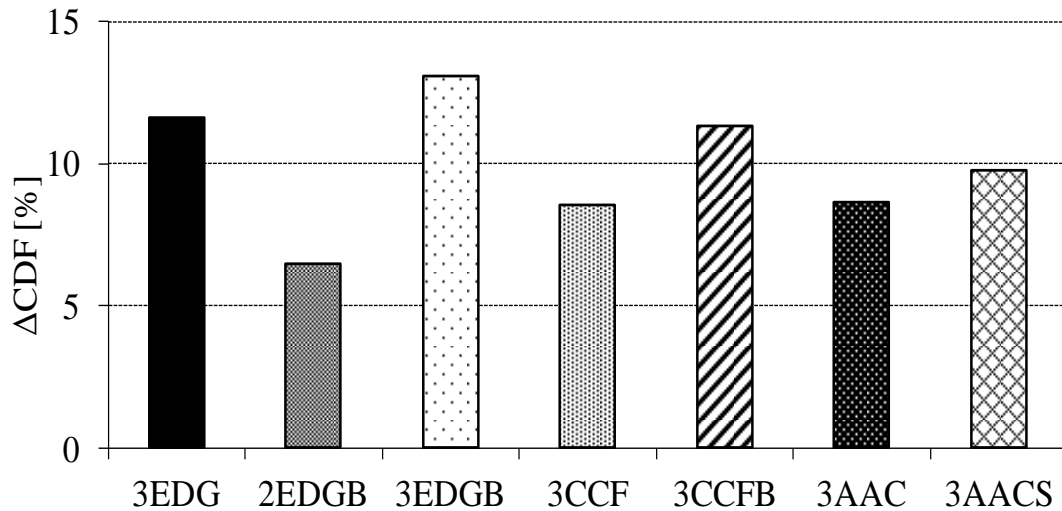


Figure 6: Decrease ΔCDF [%] compared to the CDF of reference PSA models

The obtained ΔCDF is weighted by the estimated costs of the modifications with obtained results shown on Figure . The uncertainties considering the costs of the modifications are large and they propagate on the results given on Figure .

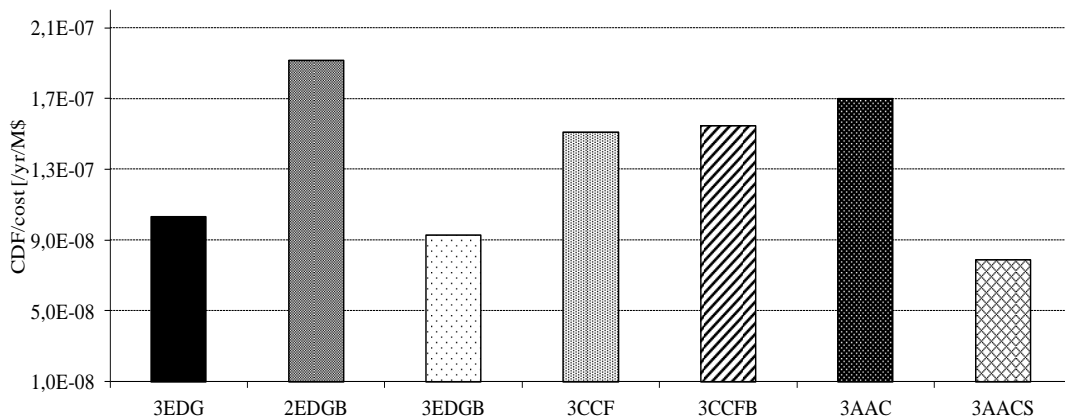


Figure 7: Weighted ΔCDF [yr/M\$] with costs of the modifications

The first 10 basic events identified with largest FV importance measure in reference PSA model are given in Table 3. The second column in Table 3 contains basic events with description given in third, unavailability in fourth column and FV importance measure given in fifth column. The last two columns contain values of Risk Decrease Factor (RDF) and Risk Increase Factor (RIF) importance measures.

Table 3 shows that basic events with largest FV importance measure in 2EDG model are basic events representing restoration of electrical power from offsite power system followed by AFW failure to start and operate.

The identified first ten basic events with largest FV importance measure in 3EDG model are given in Table 4.

Table 3: The basic events with largest FV importance measure in 2EDG model

No.	Name	Description	Nom. value	FV	RDF	RIF
1	NRAC-SGDR	Off-site power restoration	8.25E-01	1.50E-01	1.18E+00	1.03E+00
2	AFW-XHE-FO-U1SBO	Operator failure to start AFW	8.20E-02	1.23E-01	1.13E+00	2.31E+00
3	AFW-TDP-FR-2P6HR	AFW failure to run	3.00E-02	1.16E-01	1.13E+00	4.73E+00
4	R	Manual reactor scram	1.70E-01	1.13E-01	1.13E+00	1.55E+00
5	HPI-XHE-FO-FDBLD	Operator failure feed/bleed	7.10E-02	1.12E-01	1.13E+00	2.46E+00
6	NRAC-CD4	Restore off-site power	1.78E-02	9.00E-02	1.10E+00	5.97E+00
7	RECOV-T1SN-3	Operator recovery action	6.12E-01	7.44E-02	1.08E+00	1.05E+00
8	RECOV-S1---2	Operator recovery action	9.29E-01	7.35E-02	1.08E+00	1.01E+00
9	RECOV-T1N--12	Operator recovery action	3.37E-02	7.16E-02	1.08E+00	3.05E+00
10	BETA-2DG	Beta factor for 2 EDG	3.80E-02	6.60E-02	1.07E+00	2.67E+00

Table 4: The basic events with largest FV importance measure in 3EDG

No.	Name	Description	Nom.value	FV	RDF	RIF
1	AFW-XHE-FO-U1SBO	Operator failure to start AFW	8.20E-02	1.37E-01	1.15E+00	2.45E+00
2	AFW-TDP-FR-2P6HR	AFW failure to run	3.00E-02	1.28E-01	1.15E+00	5.14E+00
3	R	Manual reactor scram	1.70E-01	1.28E-01	1.15E+00	1.63E+00
4	HPI-XHE-FO-FDBLD	Operator failure feed/bleed	7.10E-02	1.27E-01	1.15E+00	2.66E+00
5	RECOV-S1---2	Operator recovery action	9.29E-01	8.32E-02	1.09E+00	1.01E+00
6	RECOV-T1N--12	Operator recovery action	3.37E-02	8.10E-02	1.09E+00	3.32E+00
7	Z	Unfavorable moderator temp.	1.40E-02	7.60E-02	1.08E+00	6.35E+00
8	PPS-XHE-FO-PORVS	Operator failure PORVs	4.40E-02	7.06E-02	1.08E+00	2.53E+00
9	RECOV-T1N--11	Operator recovery action	2.88E-02	6.98E-02	1.08E+00	3.35E+00
10	LPI-CCF-FS-SI1AB	CCF of motor driven pumps	4.50E-04	6.04E-02	1.06E+00	1.35E+02

The operator failure to start and run auxiliary feedwater system, manual reactor scram and operator failure to initiate feed and bleed cooling are identified in Table 4 as most important for NPP with three EDG. Obtained results in Table 3 and Table 4 show that selection of the permanent modification enhancing the NPP power system will affect the importance measures of basic events and future modifications in the plant.

5. CONCLUSIONS

The obtained results from deterministic safety analysis and PSA, given in Section 3 and Section 4, are in line with the latest recommendations considering the SBO mitigation capability of the NPP (NRC, 1988b).

The results of the deterministic safety analysis show that the available time for restoration of AC power to the NPP from either onsite or offsite power sources is extended for at least the batteries capacity extension time and consequential increase of the TD AFW system. The results in Section 3 show that this interval can be extended up to 72 hours after the SBO, even in the presence of Seal LOCA.

The results of the PSA given in Section 4 show that largest decrease of the CDF is obtained for model with new EDG and increase of batteries capacity. The largest weighted decrease of the CDF, considering the modification costs, is obtained for modification resulting in increase of batteries capacity. The importance of the CCF of the EDG is identified in the PSA results and need for their minimization. These results support the recommendations considering the protection of the 8-hour coping systems from all design-basis events and extended beyond-design-basis events (NRC, 1988b).

The increase of the available time for restoration of AC power is expected to decrease the stress on operators and decrease the probability of human failure events.

The TD AFW in both analyses, deterministic and probabilistic, is assumed to be operational when electrical power is available. The availability of the TD AFW after the beyond-design-basis events and especially after the combination of beyond-design-basis external events is not considered in the analysis. The assessment of the consequences of these particular or concurrent events will require both deterministic and probabilistic analysis.

These recommendations are relevant for operating and new reactors designs considering the contribution of LOOP and SBO events in overall plant risk.

Acknowledgement

This research was partly supported by the Slovenian Research Agency (research program P2-0026), partly by Krško NPP and Slovenian Nuclear Safety Administration CAMP program (project no. POG-3473) and partly by the European Atomic Energy Community's (Euratom) Seventh Framework Programme FP7/2007-2011 under Grant agreement no. 605001.

References

- AREVA, 2007. U.S. EPR Safety Analysis Report.
- Bertucio, R.C., Brown, S.R., 1990. Analysis of core damage frequency: Sequoyah, Unit 1, internal events, NUREG/CR-4550, p. Medium: X; Size: Pages: (399 p).
- Bertucio, R.C., Julius, J.A., Cramond, W.R., 1990. Analysis of core damage frequency, Surry, Unit 1 internal events appendices, NUREG/CR-4550, p. Medium: X; Size: Pages: (703 p).
- ENSREG, 2012. Stress tests performed on European nuclear power plants - Peer review report.
- IAEA, 2012. Electric grid reliability and interface with nuclear power plants, IAEA safety standards series, no. NG-T-3.8. International Atomic Energy Agency, Vienna, p. 78.
- Krajnc, B., Glaser, B., Jalovec, R., Špalj, S., 2011. MAAP Station Blackout Analyses as a Support for the NPP Krško STORE (Safety Terms of Reference) Actions, New Energy for New Europe Slovenia.

NEA/CSNI/R(2015)4

Nishio, M., Fujimoto, H., 2011. Study on Seismic PSA for a BWR in shutdown state, ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis. American Nuclear Society, Wilmington, NC.

NRC, U.S., 1988a. Station Blackout, Regulatory Guide 1.155, Washington.

NRC, U.S., 1988b. Station Blackout Rule, NRC Regulations , Title 10, Code of Federal Regulations, Washington.

NRC, U.S., 2003. Regulatory Effectiveness of the Station Blackout Rule in: Raughley, W.S. (Ed.), NUREG-1776. U.S. Nuclear Regulatory Commission, Washington.



NRC, U.S., 2005. Reevaluation of Station Blackout Risk at Nuclear Power Plants, NUREG/CR 6890, Washington.

Prior, R.P., Chaboteaux, J.P., Wolvaardt, F.P., Longton, M.T., Schene, R., 1994. Best estimate success criteria in the Krsko IPE, PSA/PRA and Severe Accidents. Nuclear Society of Slovenia, Ljubljana, Slovenia, pp. 2–12.

Prosek, A., Mavko, B., 2011. Animation model of Krsko nuclear power plant for RELAP5 calculations. Nucl Eng Des 241, 1034-1046.

Volkanovski, A., Prosek, A., 2013. Extension of station blackout coping capability and implications on nuclear safety. Nucl Eng Des 255, 16-27.

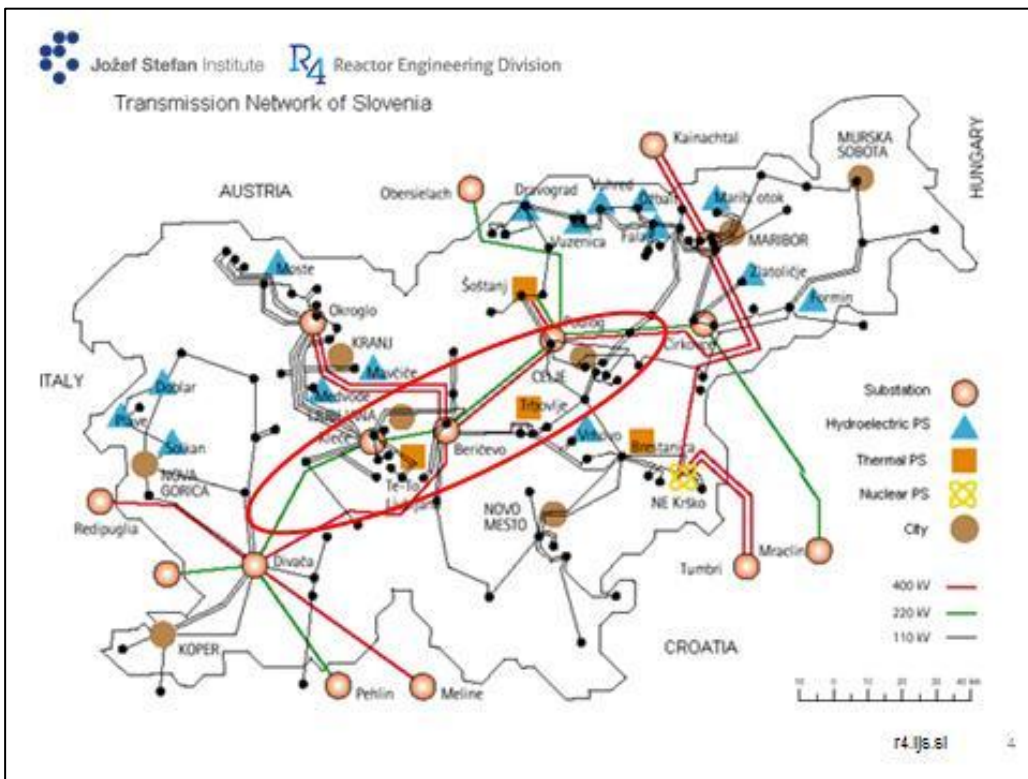


 Jožef Stefan Institute  Reactor Engineering Division

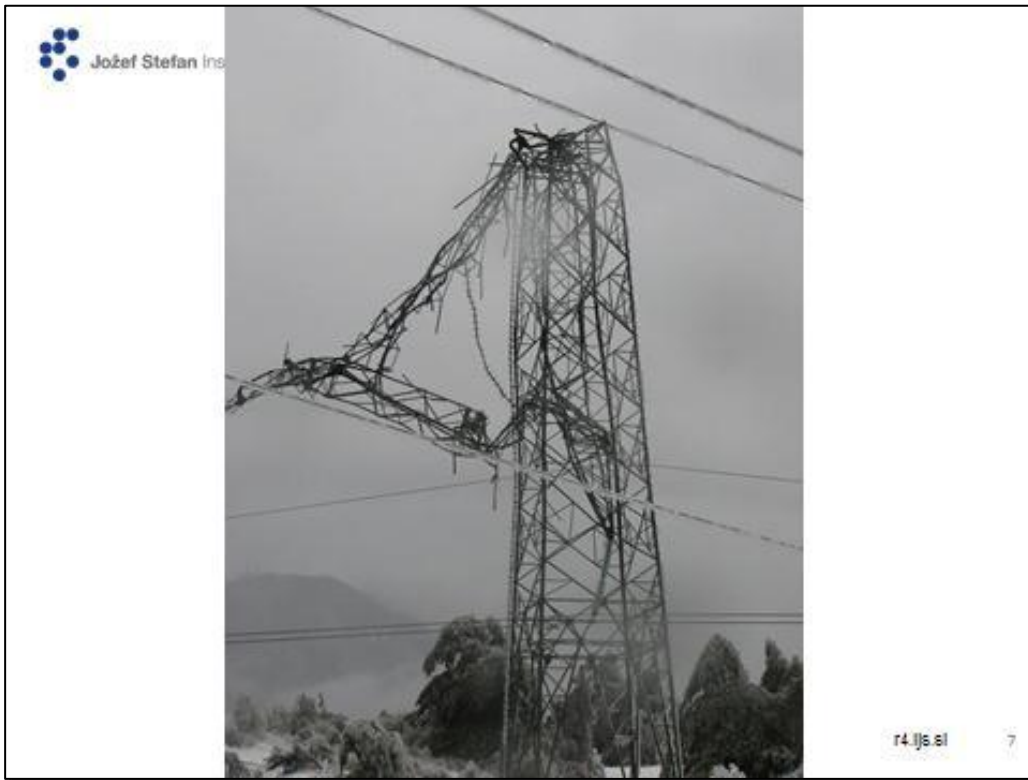
Implications of Extension of Station Blackout Cooping Capability on Nuclear Power Plant Safety

Dr. Andrija Volkanovski

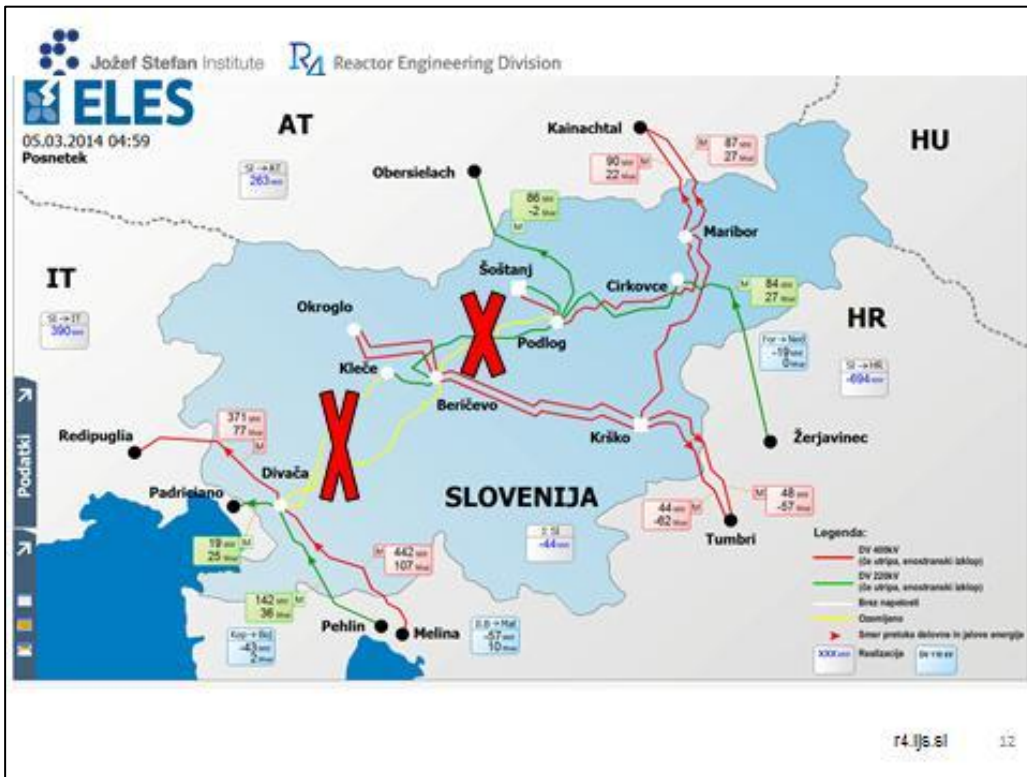
OECD/NEA, Paris, France, 1 – 4 April 2014 r4.jis.si 2











Content:

- Introduction
- NPP Models: Deterministic/PSA
- Results
- Discussion
- Research on R4 in the field

Introduction

Nuclear Engineering and Design 255 (2013) 16–27



Contents lists available at ScienceDirect

Nuclear Engineering and Design

journal homepage: www.elsevier.com/locate/nucengdes



Extension of station blackout coping capability and implications on nuclear safety

Andrija Volkanovski*, Andrej Prošek

Jožef Stefan Institute, Jamnikova cesta 39, SI-1000 Ljubljana, Slovenia

Introduction

- **SBO and LOOP dominant contributors to the plant CDF**
- **Functional failure of all I&C during extended SBO**
- **Fukushima Daiichi NPP accident**
- **“Stress tests” has shown that in terms of safety margins, SBO is the limiting case for most NPP**

Introduction



- **Implications of the strengthening of the SBO mitigation capability on safety of the NPP (new EDG/AAC, increased battery capacity and their combinations)**
- **Assessment done with state-of-art deterministic and probabilistic methods and tools**

NPP Models: Deterministic

- RELAP5/MOD3.3 Patch 4 input model of the PWR NPP
- Input model includes all important components of the NPP
- Time interval between SBO and start of the core damage is PSA input parameter used in the probabilistic safety analysis

NPP Models: Deterministic



- SBON – SBO without RCPs Seal LOCA and TD AFWS operational
- SBONP – SBO without RCPs Seal LOCA and TD AFWS operational and PRZ PORV stuck open after first opening
- SBOS – SBO with RCPs Seal LOCA and TD AFWS operational
- SBOS0 – SBO with RCPs Seal LOCA and TD AFWS operational for 0 hours
- SBOS4 – SBO with RCPs Seal LOCA and TD AFWS operational for 4 hours
- SBOS8 – SBO with RCPs Seal LOCA and TD AFWS operational for 8 hours

 Jožef Stefan Institute  Reactor Engineering Division

NPP Models: Probabilistic

- 2EDG** - reference PSA model of the NPP;
- 3EDG** - added third EDG;
- 2EDGB** - increased batteries capacity;
- 3EDGB** - added third EDG and increased batteries capacity;
- 3CCF** - added third EDG and increased CCF of EDGs;
- 3CCFB** - added third EDG, increased batteries capacity, increased CCF of the EDGs;
- 3AAC** - added third DG as a alternate AC source (AAC);
- 3AACS** - added third EDG utilized as AAC and substitute diesel generator to the existing EDG

ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs r4.ijs.si 19

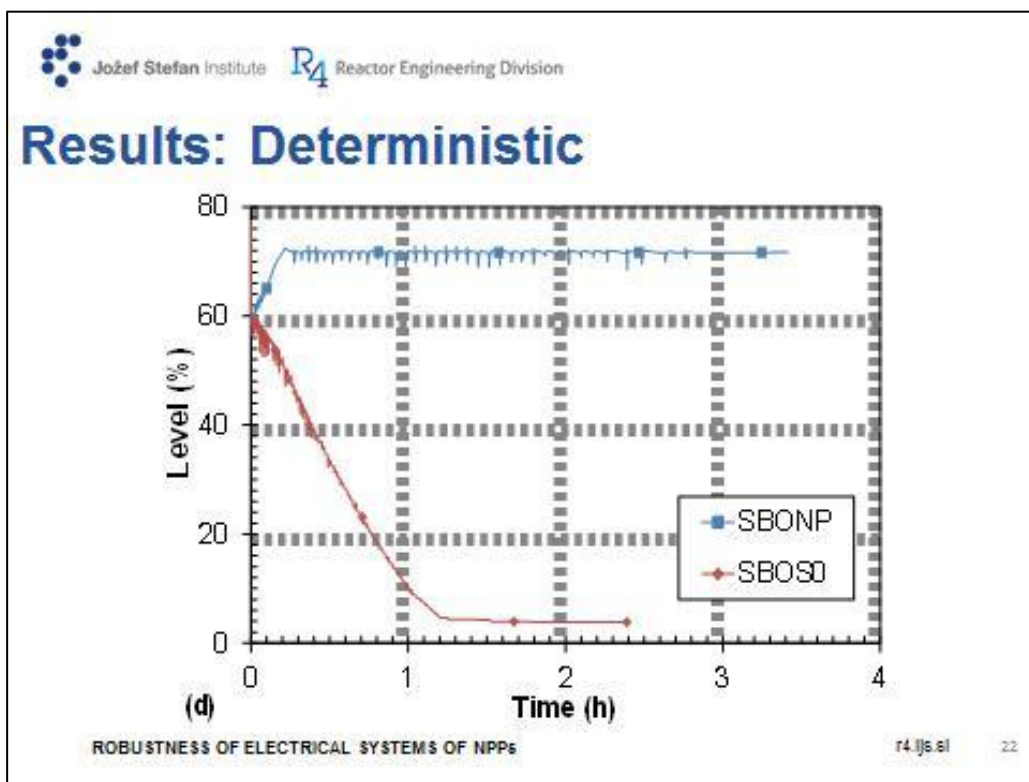
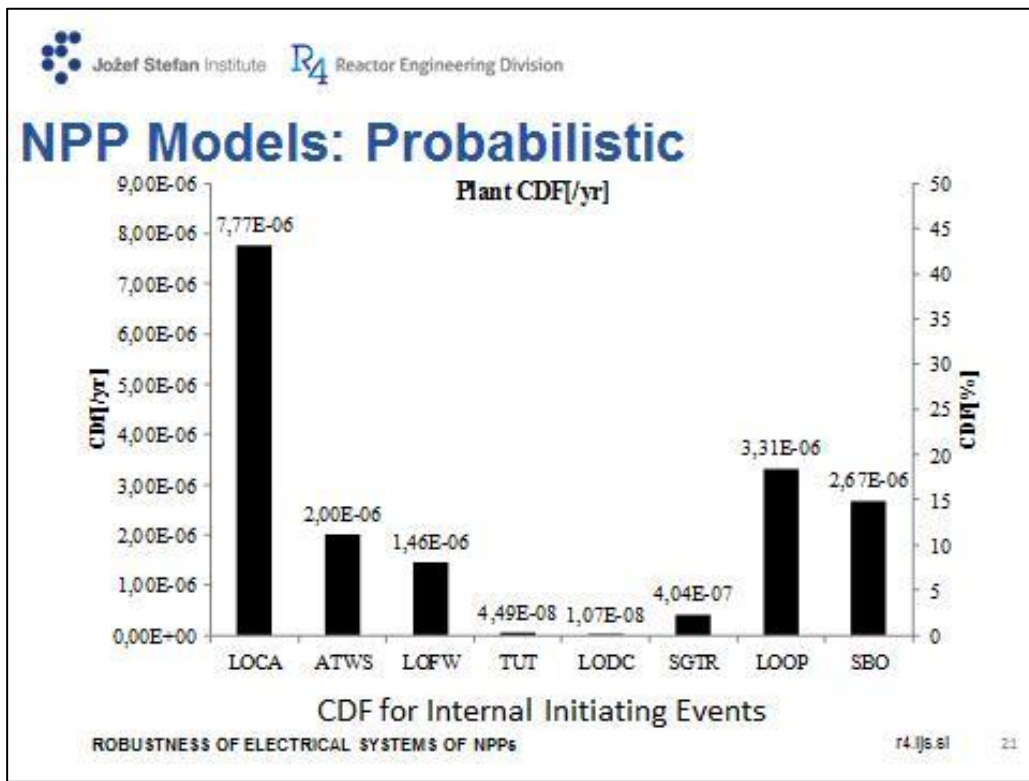
 Jožef Stefan Institute  Reactor Engineering Division

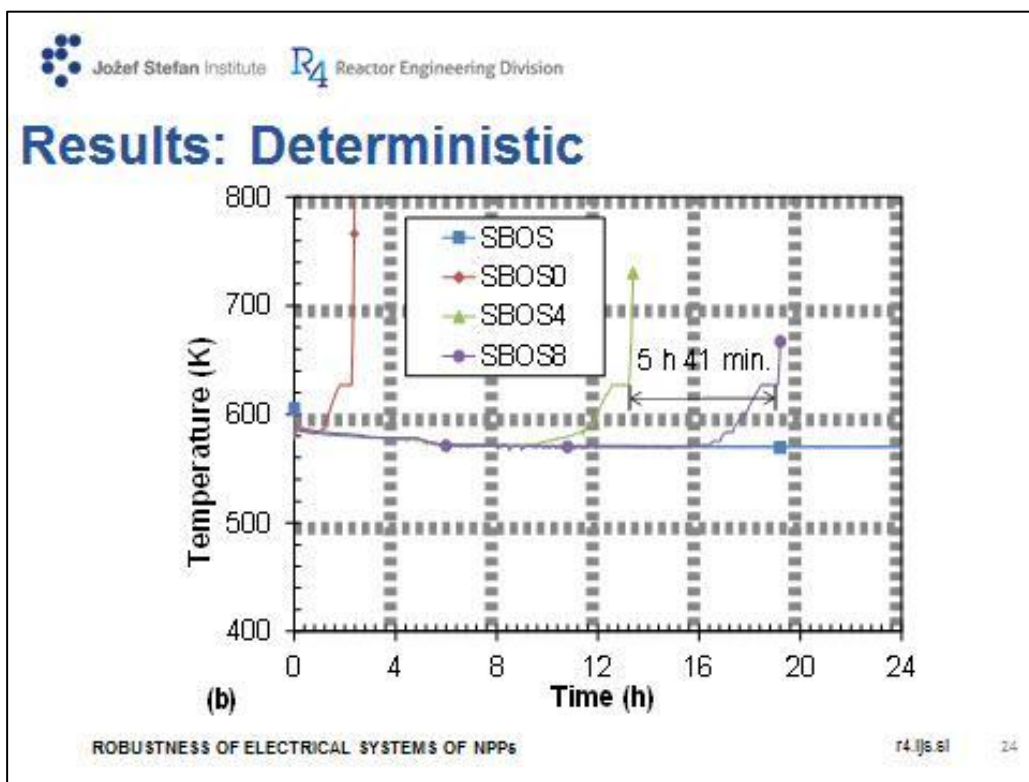
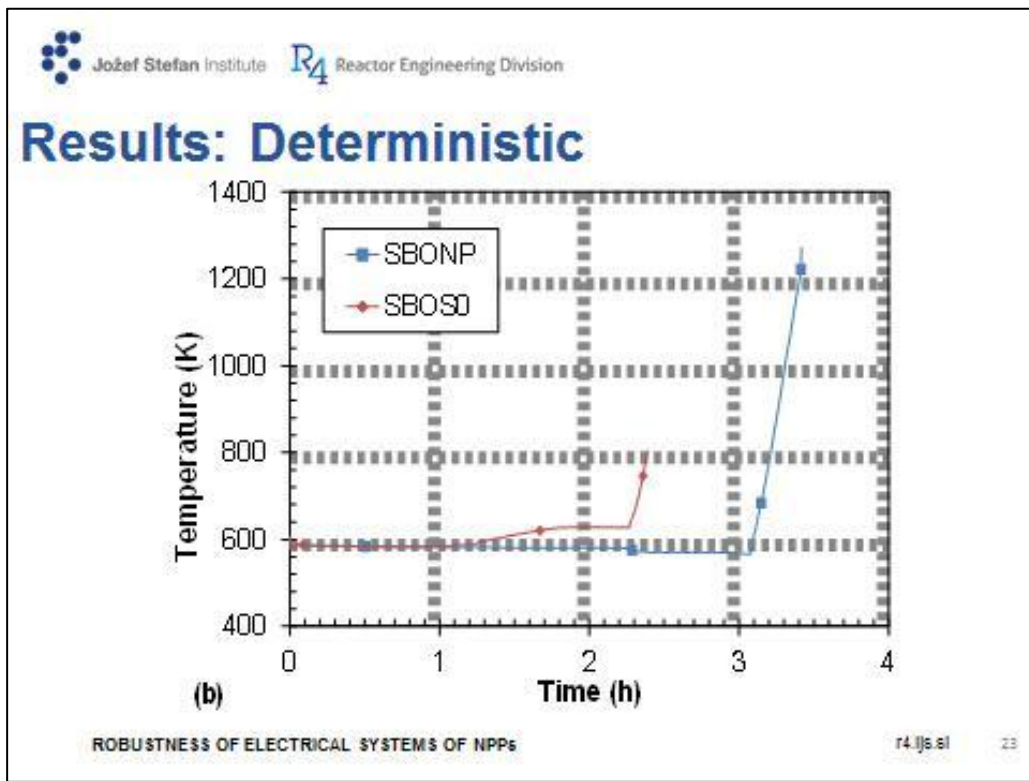
NPP Models: Probabilistic

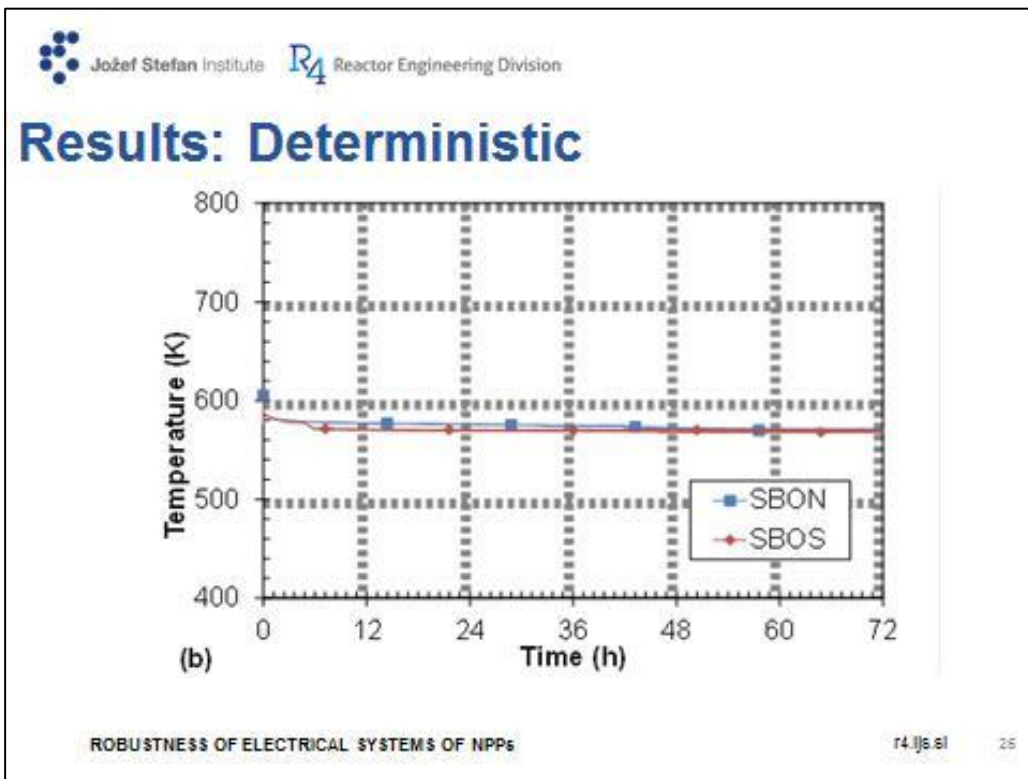
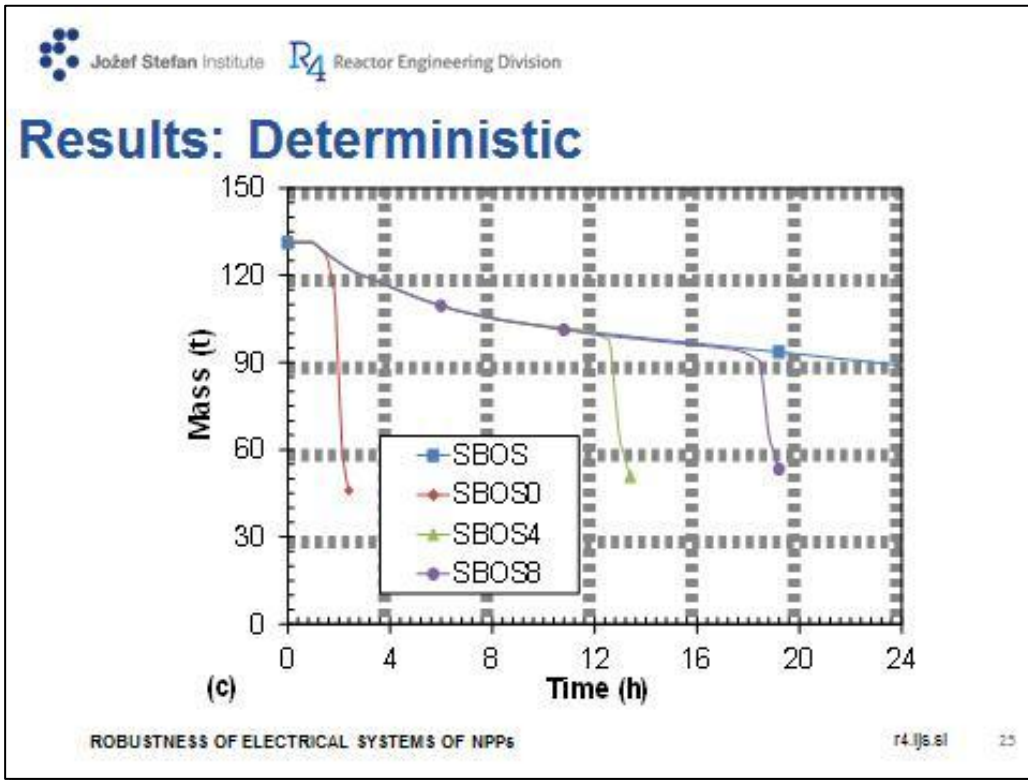
Probability of non-recovery of AC power within given time

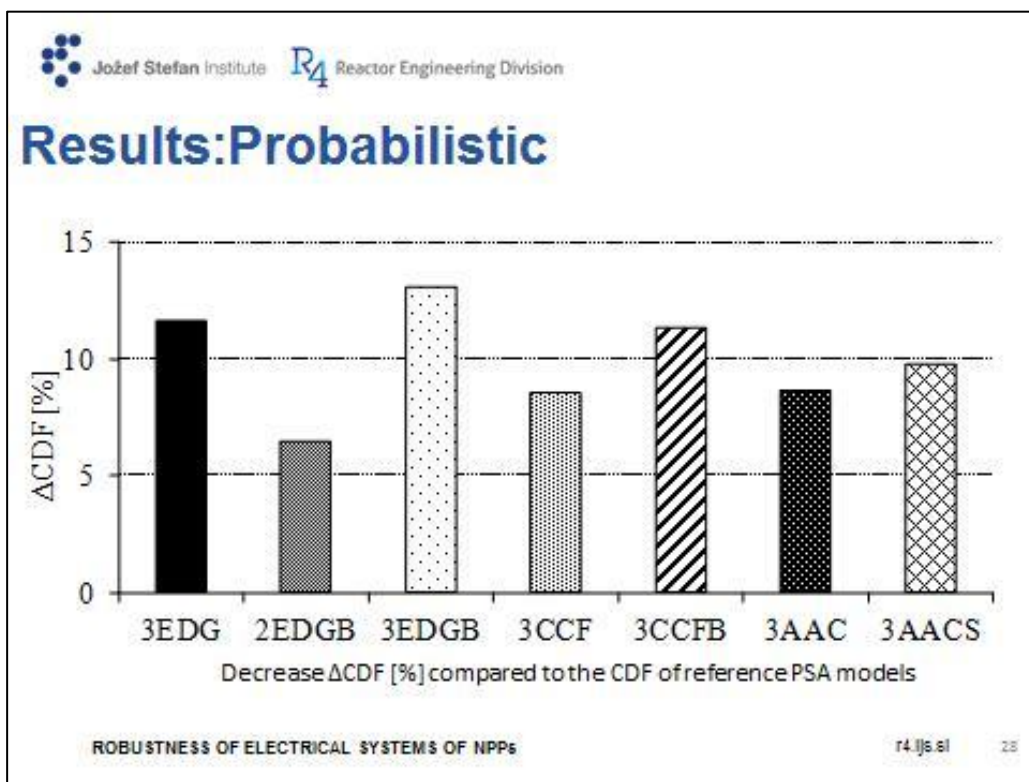
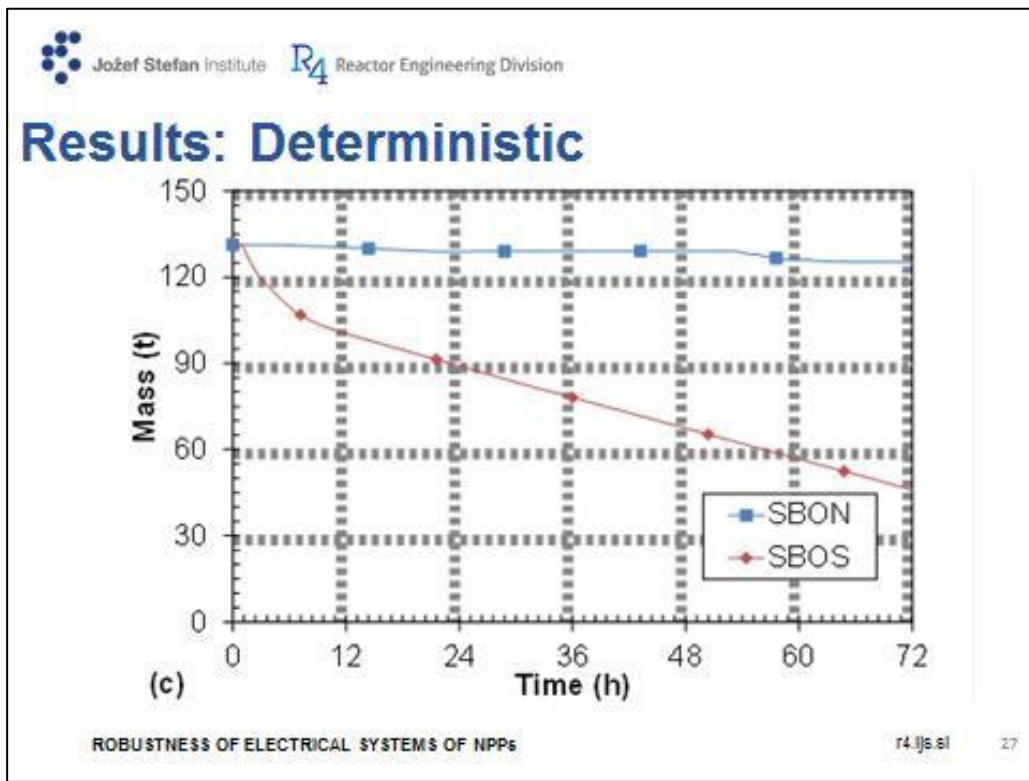
Basic Event	Description	Restoration time [hr]	Mean probability
NRAC-SGDR	Steam generator dryout	0.5 (1)	8.25E-1
NRAC-PRZBV	Pressurizer PORV stuck open	1 (2.5)	2.81E-1
NRAC-OFFSITE(4)	AC power restoration offsite	7 (9)	6.10E-2
NRAC-OFFSITE(8)	AC power restoration	12 (16)	2.00E-2
NRAC-ONSITE(4)	AC power restoration onsite	7 (9)	1.78E-2
NRAC-ONSITE(8)	AC power restoration	12 (16)	5.85E-3

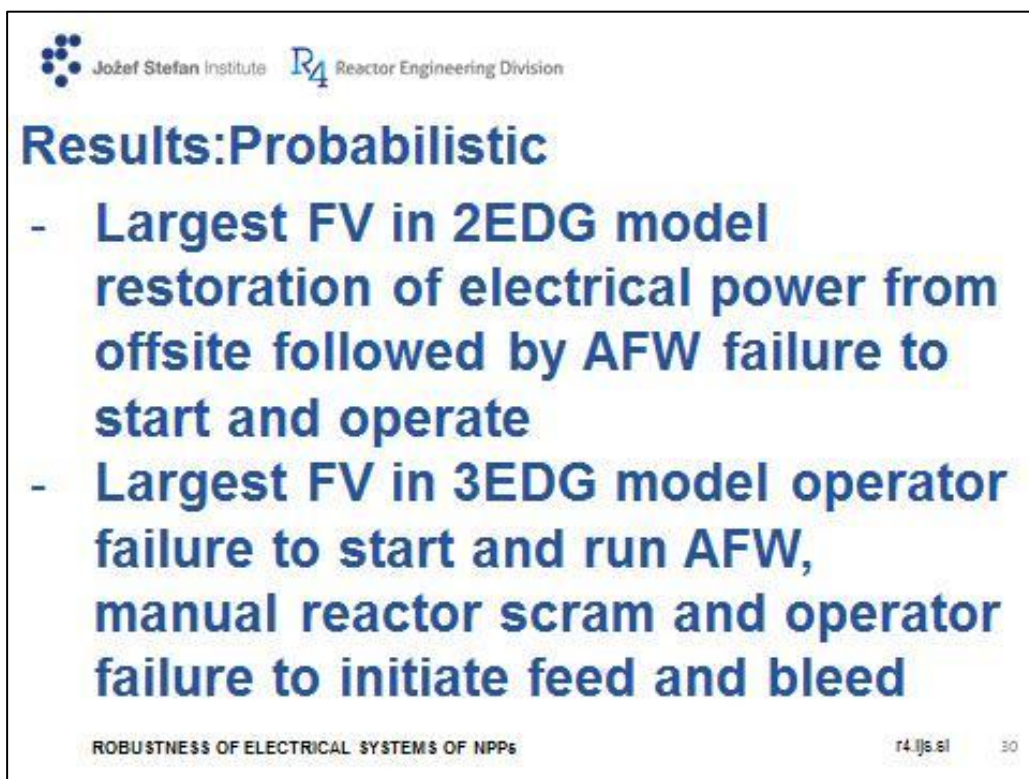
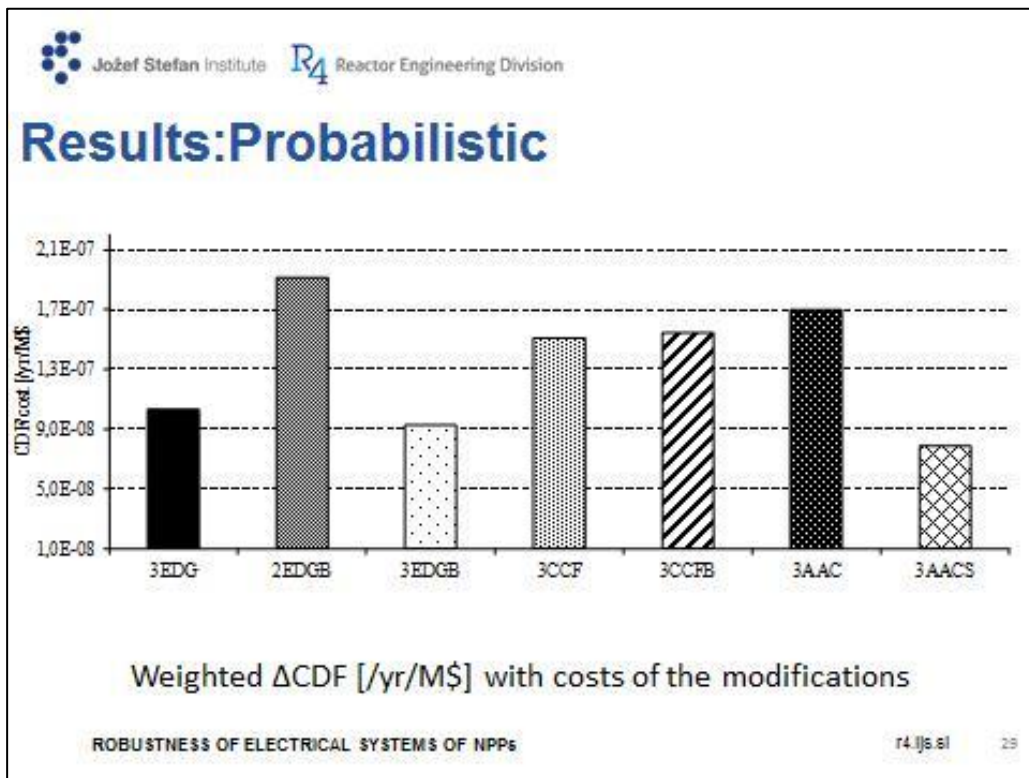
ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs r4.ijs.si 20















 Jožef Stefan Institute  Reactor Engineering Division

Conclusions



- **AC restoration time is extended for at least the batteries capacity extension time**
- **Interval can be extended up to 72 hours after the SBO, even in the presence of Seal LOCA**
- **Largest Δ CDF [%] for 3EDGB, Largest Δ CDF [/yr/M\$] for 2EDGB**

ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs r4.ijs.si 31

 Jožef Stefan Institute  Reactor Engineering Division

Reliability Engineering and System Safety 94 (2008) 1116–1127

Contents lists available at ScienceDirect

 **Reliability Engineering and System Safety** 



journal homepage: www.elsevier.com/locate/ress

Application of the fault tree analysis for assessment of power system reliability

Andrija Volkanovski*, Marko Čepin, Borut Mavko

Reactor Engineering Division, Jožef Stefan Institute, Jamova 39, 1000 Ljubljana, Slovenia

ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs r4.ijs.si 32


 Jožef Stefan Institute  Reactor Engineering Division

KT K110002 – 133.000m mesta točen

A. Volkanovski: On-site power system reliability of a nuclear power plant after the earthquake

A. Volkanovski

On-site power system reliability of a nuclear power plant after the earthquake

Emerging Issues in Nuclear Facility Safety 661

Subsynchronous resonance in nuclear power plant
Andrija Volkanovski, Andrej Prošek

Reactor Engineering Division, Jožef Stefan Institute, Jamova 39, 1000, Ljubljana, Slovenia
andrija.volkanovski@ijs.si, andrej.prosek@ijs.si



ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs r4.ijs.si 33


 Jožef Stefan Institute  Reactor Engineering Division



“Expert Opinion on Modification 599-EE-L,
 Enhancement of the Emergency Power Supply”,
 contractor: Nuclear Power Plant Krško, 2011-2012

r4.ijs.si 34

 Jožef Stefan Institute  Reactor Engineering Division

Research in the filed

- Andrija Volkanovski, Marko Čepin, Borut Mavko, **Application of the fault tree analysis for assessment of power system reliability**, Reliability Engineering & System Safety, Volume 94, Issue 6, June 2009, Pages 1116-1127, ISSN 0951-8320, <http://dx.doi.org/10.1016/j.ress.2009.01.004>.

New method for power system reliability analysis and implications LOOP frequency and NPP Safety presented

- Andrija Volkanovski, **On-site power system reliability of a nuclear power plant after the earthquake** (2013) Kerntechnik, 78 (2), pp. 99-112.

Analysis of the nuclear power plant on-site power system reliability during normal operation and after the earthquakes with given intensity



- Andrija Volkanovski, Andrej Prošek, **Subsynchronous resonance in nuclear power plant**, (2011) Transactions of the American Nuclear Society, 105, p. 661.

Analysis of subsynchronous resonance phenomena and implications on nuclear power plant safety

- Andrija Volkanovski, Marko Čepin, **Nuclear power plant on-site power system reliability** (2010) Reliability, Risk and Safety: Back to the Future, pp. 644-651.

- Andrija Volkanovski, Wolfgang Kröger, **Power grid reliability and vulnerability analysis** (2012) Advances in Safety, Reliability and Risk Management - Proceedings of the European Safety and Reliability Conference, ESREL 2011, pp. 2530-2538.

ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs r4.ijs.si 35

 Jožef Stefan Institute  Reactor Engineering Division

Implications of Extension of Station Blackout Cooping Capability on Nuclear Power Plant Safety

Dr. Andrija Volkanovski

OECD/NEA, Paris, France, 1 – 4 April 2014 r4.ijs.si 36

DC batteries in NPP, present and future solutions

Current products and technologies
Alternative battery technologies

Gery Bonduelle
March 2014



EnerSys: The Evolution

- World's largest industrial battery manufacturer with over \$2 billion in sales
- 27% share in a \$6.0 billion+ market in CY 2012 (Motive and Reserve only)
- Over 100 years of experience
- 30 manufacturing facilities in the Americas, EMEA and Asia
- 10,000 customers in 100 countries
- 8,800 employees globally



EnerSys: Our Global Marketplace



31 manufacturing facilities in the U.S., Europe and Asia and global distribution with world headquarters in Reading, Pa.



Lead Acid Battery Technologies



Battery Technologies

Terminology:

- Cycle life : Number of cycle with discharge and recharge
- Calendar life : Life expectancy on float, without any cycle
- DOD : Energy discharged during one cycle (in %)
- SOC : Ratio between Energy discharged and nominal capacity (in %)
- Capacity : Energy stored in the battery (in Ah or Wh)
- Self discharge : Capacity loss during rest period (in %)
- Charge efficiency : Ratio between Ah of charge and Ah of discharge (in %)
- Specific Energy : Energy per mass unit (Ah/kg or Wh/kg)
- Energy Density : Energy per volume unit (Ah/L or Wh/L)
- Specific Power : Power per mass unit (W/kg)
- Power density : Power per volume unit (W/L)



Theory - Basic Terminology

- Cell
 - An assembly of electrodes and electrolyte which constitutes the basic unit of a battery
- Battery
 - Electrochemical power source
 - Receives, stores, and delivers electrical energy
 - Includes one or more cells
- String
 - Series connection of batteries of a required total cell quantity and capacity



EnerSys OPzS Flooded Tubular plate



- 200Ah to 3000Ah
- In NPP:
- EDF France
- Forsmark Sweden
- Fortum Finland
- ...



EnerSys Vb Flooded Flat plate



- 275Ah to 2400Ah
- In NPP:
- Armenia
- Temelin, Czech Republik
- Paks, Hungary
- Ignalina, Lithuania
- Many in Russia and Ukraine



EnerSys GN Flat plate



- 1140Ah to 3600Ah
- In NPP:
 - USA
 - China
- Certified to IEEE standard



3 ranges and 3 technologies, why ?

- Products were designed by different companies that are now together as 1
- They all have in common
 - Proven in the application since >30 years
 - Flooded mature technology
 - High control QA
 - Certified to customer NPP specifications
 - Safest design



Conventional Flooded Lead Acid Battery

Pros:

- Extremely robust design, proven since many years
- Safe design, no known field issue
- Reliable
- Easy to maintain
- Easy to control and detect potential issue

- >95% recyclable
- Well established sales & service networks limiting non-productive downtime
- Low cost/KWh @ \$150/KWh



Conventional Lead Acid Battery

Cons

- Watering required on flooded batteries
- Need large floor space in some RP applications
- Self discharge can damage battery when not used
- Capacity reduction in low temperature applications



Conventional Lead Acid Battery

Availability

- Predominant industrial battery technology used for over 100 years.
- Many alloys variations for performance vs. life tradeoffs
- Very mature industry with well established manufacturing, distribution, service, and recycling options available



Conventional Lead Acid Battery

- Reliability
 - Most reliable solution to date, proven by field data
- Life prediction, monitoring
 - A few measurement give a good indication of state of charge and health
 - Monitoring temperature and voltage is often sufficient



Conventional Lead Acid Battery

- Safety
 - Hydrogen generation
 - Behavior well understood and documented
 - Ventilation requirements are known and in place
 - No intrinsic product safety issue:
 - Internal short, or overcharge, or undercharge,
 - Will not result in a safety hazard
- Safety post seismic choc
 - Should there is an extreme seismic shock
 - Container breaks, corrosive electrolyte goes into retention area below the battery. Do not pose a flammability hazard.
 - Battery even empty from electrolyte can provide 20% of its initial energy

x16



Other Energy Storage options:

- ⑩ Valve Regulated Lead Acid Battery
- ⑩ Lithium Ion (Li Ion) Battery
- ⑩ Ni based (Nickel Cadmium and Nickel Zinc)



Valve Regulated Lead Acid Battery

- Based on the same electrochemical process found in standard lead acid battery technologies, but electrolyte held in an absorbed glass mat (AGM) between the plates, or in form of Gel
- VRLA AGM utilizes thinner plates and in greater quantities allowing for a more efficient chemical reaction and higher energy densities than standard lead acid batteries



VRLA AGM Flat plate




- 40Ah to 3000Ah
- No water addition
- up to 15 year design life (ambient temp)
- NPP application in Sweden



VRLA: OPzV Gel Tubular plate

- 200Ah to 3000Ah
- No water addition
- 20 year design life (ambient temp)
- One or two NPP application




Flooded - AGM - GEL

Conventional cell: Shows a 'SEPARATOR' between a 'POSITIVE PLATE' and a 'NEGATIVE PLATE'. It is filled with 'Liquid electrolyte'. Gases O_2 and H_2 are shown rising from the plates.

AGM cell: Shows a 'POSITIVE PLATE' and 'NEGATIVE PLATE' separated by a 'MICROPOROUS SEPARATOR'. An 'Electrolyte absorptive glass mat' is positioned between the plates. Oxygen (O_2) is shown recombining within the cell.

Gel cell: Shows a 'POSITIVE PLATE' and 'NEGATIVE PLATE' separated by a 'MICROPOROUS SEPARATOR'. The electrolyte is in a 'Gelled electrolyte' state.



VRLA Battery

Pros

- No watering required, less maintenance
- Higher energy density than conventional flooded lead acid batteries

- Higher efficiency density than conventional flooded lead acid batteries
- Can be stacked to increase stored energy in a given room

- Low cost/KWh @ \$200 to \$300/KWh
- >95% recyclable, and retain some value at end of life



VRLA Battery

Cons

- Lower operating life than conventional flooded lead acid batteries
- Less possibilities to check for issues
 - No acid density check
 - No visual check

- Water recombination process can imply some variation in actual voltages lead to misinterpretation of state of health
- More sensitive to ambient temperature
- Require more controlled charging conditions



VRLA Battery

Availability

- Technology employed in Telecom and UPS industry for the past 20 years
- Manufacturing advancements allowing for development of larger cells and improved consistency



VRLA Battery

• Reliability

- Product can be reliable, but shorter actual field life need to be understood and considered
- Product more sensitive to environment conditions (charging voltage adjustment to temperature...)

• Life prediction, monitoring

- Difficult to anticipate failure
- Monitoring temperature and voltage is not always sufficient
- Alternative measurement using ohmic resistance/impedance/conductance add information, but in a very high integrity application is not sufficient



VRLA Battery

- Safety
 - In the early 80's when this technology was introduced, there were a few cases of thermal runaway. Under overcharge higher voltage than specified the battery can overheat. Stopping the charge stops the reaction.
 - With modern chargers/rectifiers those issues are very rare.
 - Monitoring of individual voltage and alert would prevent any safety hazard
- Safety post seismic test
 - Container breakage will not cause corrosive electrolyte leaks, the battery will retain most of its energy
 - An internal short would lead to self discharge of the cell and inability for the cell to provide its energy. Not a safety hazard



Li Ion Battery

Pros

- Estimated 2000 to 10,000 cycles before replacement
- No gas emissions, clean-air working environment
- No maintenance required
- Lighter and smaller (2x to 3x) may help
 - Extended runtime possible
- Very high charge rate acceptance
- Less self discharge issues, long shelf life
- No partial charge damage
- Nearly same performance at 2,4,6,8 Hour rate



Li Ion Battery

Cons

- High cost/KWh: >750 \$
- Actual life in the application not proven, only projections
- Redundant safety design considerations required to prevent thermal venting conditions and a sophisticated electronic management system (no deep discharge / no overcharge), the BMS
- Shipping restrictions as a "Class 9 Miscellaneous Hazardous Material"



Li-Ion Battery

Availability

- Several Li-Ion different technologies, which one will be chosen ?
- Some products available but many many development on-going
- Government subsidized prototype projects for industrial batteries
- Cost projections show drastic reductions as well as increased availability of manufacturing capability
- No standard on our markets at the moment



Li-Ion Battery

- Reliability
 - Multiple technologies available since a short period of time, so no data available
 - Mandatory electronic supervising system add complexity and reduce overall reliability compared to standard lead acid product
- Life prediction, monitoring
 - Embedded electronic system include a life prediction algorithm



Li-Ion Battery

- Safety
 - Issues with this technology have been publicized heavily in the recent years
 - One key internal component is flammable: the electrolyte which is an organic solvent
 - Under specific conditions, if a short is created between the electrodes, the solvent can ignite.
 - Overcharge can lead to a fire or explosions
 - Electronic systems are monitoring constantly all cells to avoid overcharge, and containment have been designed to avoid propagating fire or overpressures into dangerous areas
- Safety post seismic choc
 - Breakage of container or housing can lead to electrolyte leaks, and flammable vapors
 - Risk of creating an internal short, which can lead to a fire hazard

x30



Ni based

- Pros

- Good energy density NiZn > NiCd, 2x better than Pb
- Service life, no corrosion
- NiCd with outstanding deep discharge robustness, (delivered & stored in discharged state)
- NiCd low temperature performance even in charge
- NiCd life in high temperature
- NiZn maintenance free
- NiZn High current performance



EnerSys
Powerful Solutions

Ni based

- Cons

- Cost: 450\$/kWh for NiCd
- Environmental, recycling for NiCd
- Flooded NiCd require maintenance
- Derating in float applications
- Limitations at very high temperatures (above 50C)

EnerSys
Powerful Solutions

Ni based

Availability

- NiCd for aircraft, rail, RP, Solar, ME Oil and Gas industry
- NiCd is used in NPP in some countries
- NiMH for HEV, consumer cells
- NiZn in extensive development state, field test to be started in rail and UPS



Ni Cd

- Reliability
 - Proven reliability in the application
- Life prediction, monitoring
 - A few measurement give a good indication of state of charge and health
 - Monitoring temperature and voltage is often sufficient



Ni Cd

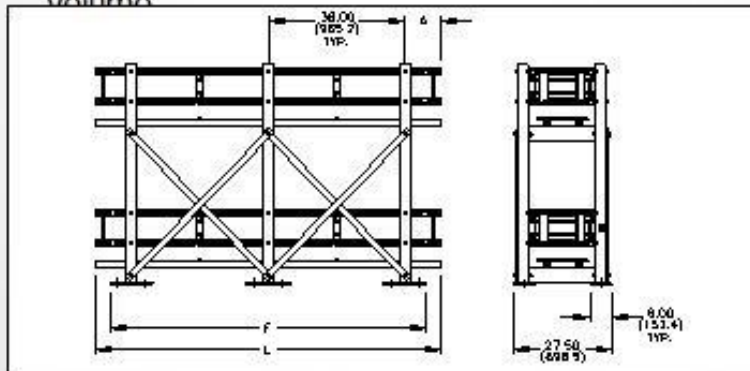
- Safety
 - Hydrogen generation
 - Behavior well understood and documented
 - Ventilation requirements are known and in place
 - No intrinsic product safety issue:
 - Internal short, or overcharge, or undercharge,
 - Will not result in a safety hazard
- Safety post seismic choc
 - Should there is an extreme seismic shock
 - Container breaks, corrosive electrolyte goes into retention area below the battery. Do not pose a flammability hazard.

x35



Opportunity for increased runtime

- Continue with proven conventional flooded technology
- But conventional technologies utilize a large floor space
- Development of 2 step or 2 tier design to optimize volume



Conclusion

- EnerSys is serving Nuclear Power Plants since decades with several battery technologies
- Most of those technologies have in common to use conventional flooded lead acid technologies
 - High reliability proven, robustness
 - Ease of problem prediction
 - Safest design
- Is the ideal choice to maintain current reliability and safety
- Increasing runtime can be made by designing alternative racking system



**Swiss Solutions for Providing Electrical Power in Cases of
Long-Term Black-Out of the Grid**

Altkind, Franz

ENSI, Switzerland

Schmid, Daniel

ENSI, Switzerland

Abstract

A better understanding of nuclear power plant electrical system robustness and defence-in-depth may be derived from comparing design and operating practices in member countries. In pursuing this goal, the current paper will focus on Switzerland. It will present in general the protective measures implemented in the Swiss nuclear power plants to ensure power supply, which comply with the "Defence-in-depth" principle by means of several layers of protection. In particular it will present the measures taken in case of a total station blackout.

The different layers supplying electricity may be summed up as follows. The first layer consists of the external main grid, which the plant generators feed into. The second layer is the auxiliary power supply when the power plant is in island mode in case of a failure of the main grid. A third layer is provided by the external reserve grid in case of both a failure of the external main grid and of the auxiliary power supply in island mode. As a fourth layer there exists an emergency electrical power supply. This is supplied either from an emergency diesel generator or a direct feed from a hydroelectric power plant. In the fifth layer, the special emergency electrical power supply from bunkered emergency diesel generators power the special emergency safety system and is activated upon the loss of all external feeds. A sixth layer consists of accident management equipment.

Since the Fukushima event, the sixth layer has been reinforced and a seventh layer with off-site accident management equipment has been newly added. The Swiss nuclear safety regulator has analysed the accident^{1,2}. It reviewed the Swiss plants' protection against earthquakes as well as flooding and demanded increased precautionary measures from the Swiss operators in the hypothetical case of a total station blackout, when all the first five layers of supply would fail. In the immediate, a centralized storage with severe accident management equipment was jointly set up by the operators. This equipment would be transported to the plant site by land or air. In a second step, each operator installed additional severe accident management diesel generators in each plant and prepared the necessary cabling and switch gear. Particular attention was dedicated to establish procedures so that the hooking and operation of the accident management equipment could be directly performed by shift personnel.

¹. <http://www.ensi.ch/de/2011/10/31/lessons-fukushima-11032011/>

². <http://www.ensi.ch/de/2013/03/01/aktionsplan-fukushima-2013/>

The presentation shall show both current practices and recent design changes of safety-related electrical systems in nuclear power plants in Switzerland.

Introduction

The current paper is a contribution from the Swiss perspective to the workshop on “Robustness of Electrical Systems of NPPs in Light of the Fukushima Daiichi Accident”. It will present in general the protective measures implemented in the Swiss nuclear power plants to ensure the house load supply, which comply with the "Defence-in-depth" principle and comprise several layers of protection. In particular the paper will present the measures taken in the case of a total station blackout. The Swiss participation in the workshop also aims to improve the safety review process of nuclear power plant electrical systems by learning from best practices in member countries and by promoting and cooperation among member countries to improve safety, as intended by the NEA.

The five Swiss nuclear power reactors come from different original manufacturers. Two of them – the Mühleberg NPP in operation since 1972 at 390 MW electrical power and the Leibstadt NPP in operation since 1984 at 1245 MW electrical power - are boiling water reactors from General Electric. A further plant - the Gösigen NPP in operation since 1979 at 1060 MW electrical power - is a Kraftwerksunion pressurized water reactor and the remaining two – NPP Beznau I & II in operation since 1969 and 1971 respectively at 380 MW electrical power each – are Westinghouse pressurized water reactors. Therefore the overall design as well as the electrical design is different among the plants.

Nevertheless, with the backfitting already implemented in the less recent plants, the electrical design principle remains the same for all NPPs. It can be structured into five designbase layers and two extended additional layers. Each of them will be explained further.

1. Layer one

Layer one consists of the external main grid, which the plant generators feed into. This is the high tension grid node available at the NPP location. The two newer NPPs are connected to the 380 kilovolt grid, whereas the less recent three are connected to the 220 kilovolt grid. Although this interface is mainly for energy delivery from the plant, it can be used to supply the plant in case of a problem with the production and/or the dedicated plant turbine/generator group.

2. Layer two

In case of a problem with the main grid – caused by an external event anywhere affecting the high tension grid – the block circuit breaker opens. Then the second layer has to take over supplying the plant. The second layer consists of the plants own turbine/generator group. In such a situation, the generator control system performs a cutback of the power to approximately 5-7%, forcing also the reactor into a reduced power range. This is the so-called ‘Island Mode’, where the plant runs for its own power supply. This is not an emergency mode and therefore no automatic diesel start is necessary. When the ‘Island Mode’ is reached the situation needs to be analysed by the operator to decide whether the reactor has to be shut down or whether the main grid is about to reset, a situation which might arise in the case of a grid problem which originated in the nearby switchyard and is easily resolved. In the latter case, an immediate synchronisation and power generation to the grid is possible (within limitations posed by the load gradients of the reactor and generator).

3. Layer three

If the island mode also fails, then the external reserve grid acts as a third supply layer. For one NPP it is the 220 kilovolt grid, whereas for the others it is the 50 kilovolt grid. In case the main grid is adversely affected, this lower tension, more regional grid interface may still be operable and function as a reserve supply. However such an interface feeds the emergency bus bars only, letting the plant perform a shutdown, triggered for instance by the turbine/generator control system.

4. Layer four

If the external reserve supply also fails, the plant goes into emergency electrical power supply mode. This is either an emergency diesel generator supply or a direct feed from a nearby hydroelectric power plant, equipped with water resistors to adjust for load and frequency in such a way that only the house load is available for the nuclear plant. The hydroelectric power plants have the advantage of being available continuously, whereas the diesel generators have to be first started up (approximately 10 seconds for power production). While the two newer NPPs have emergency diesel generators, the Mühleberg NPP has this hydroelectric supply. At the Beznau double block NPP, construction is under way for new emergency diesels located in new buildings to replace the hydroelectric plant emergency supply in 2014 for block 1 and 2015 for block 2. This project was required by and is under the supervision of the Swiss regulator (Swiss Federal Nuclear Safety Inspectorate, ENSI).

5. Layer five

Under the assumption of an extreme external hazard, the power plants have in a fifth supply layer the special emergency electrical power supply from bunkered diesel generators to power the special emergency safety systems. The two newer power plants were designed with such bunkered systems, whereas the three less recent blocks were retrofitted with them. The bunkered diesels are held in such a condition to start immediately and automatically, upon the loss of the external reserve grid interface. The bunkered diesels feed in order of priority, their assigned safety systems, lighting, ventilation, battery chargers and instrumentation. The bunkered diesels are class 1E diesel generators.

In the Swiss plants, besides the AC power, the provision of DC power is also implemented redundantly. This means that there are redundant battery groups for the safety trains and additional independent and redundant battery groups for the special emergency safety systems. The battery groups for electrical loads important to safety in an emergency have been analysed with respect to the battery discharge time and their locations in the buildings. The results showed that battery capacity is sufficient until accident management power supply for recharging the batteries is available.

The five layers of AC supply are implemented according to the particular incident, following design principles along the Swiss nuclear guidelines. The different modes of supply are tested periodically and the corresponding procedures are trained by the operating staff.

6. Effect of the Fukushima accident

After the reactor accident in Japan, a review process was initiated in Switzerland. As a direct consequence of the Fukushima accident, the Swiss Federal Nuclear Safety Inspectorate issued formal orders, by which the operators of the Swiss NPPs were required both to implement immediate measures and also to conduct additional reassessments. The immediate measures comprise improvements for the spent fuel pools but also the establishment of an external emergency storage facility for the Swiss NPPs. The additional reassessments focused on the design of the Swiss NPPs against earthquakes, external flooding and a combination. Investigation of the coolant supply on the basis of insights gained from the accident in Japan was also requested.

From the electrical point of view, the accident in Fukushima corresponds to the scenario of a total station blackout. The establishment of one external emergency storage facility aims to cope with just such a situation. The storage facility is hosted in a seismically robust, bunkered building situated on a non-floodable high ground and it is located at a distance between 20 to 70 Km from the Swiss NPPs.

7. Reinforced Layer six

In a second step, the operators installed additional severe accident management diesel generators at the plants and prepared the necessary cabling and switch gear interfaces. Procedures and training were established in such a way that hooking and operation of the accident management equipment can be performed by shift personnel. The aggregates are placed in containers on the roof of classified buildings (protected against flooding and earth quake) or on ground partly moveable and will be tested periodically to fulfil the supply to the foreseen safety systems. The original emergency connection points for electricity were revised and additional connection points were installed. The connecting cables are equipped with connectors and marked by colours on both sides for easy identification and installation.

The Swiss Federal Nuclear Safety Inspectorate conducted topical inspections on all the NPPs to gain an insight into the preparedness of the power plants for a long-lasting loss of electrical supply. The power plant operators previously had to document with a concept and detailed information how they would cope with such a situation. Assuming an initial full-power situation, two scenarios were investigated.

In the first scenario, the losses of the main and reserve external grid as well as the breakdown of the island mode and all emergency diesel generators were assumed. In other words failure of supply from all first four layers was assumed. In this case the special emergency diesel generators had to provide electrical supply for reactor shutdown, cooling and monitoring using the reactor accident instrumentation. The Swiss regulatory framework demands an automatic emergency control without any manual intervention (for the first 10h) and a longer-term controlled situation, including manual interventions, over at least seven days.

In the second scenario, the special emergency diesel generators in addition to the first four layers also were assumed to fail – a so called total station blackout – and the situation would have to be handled by severe accident management guidelines. Only battery-powered supplies were available, whereby the batteries must be sufficient until any accident management power supply could be connected. The regulations require that the situation must be governed with on-site means for three days and after that with using offsite means, up to seven days.

The NPPs were asked to present their prepared accident management procedures to identify and manage the given scenarios. The procedures had to specify also time-critical actions and any interdependence. The consumption balance of safety equipment, instrumentation, lighting, communication and the availability of sufficient personnel had to be demonstrated.

In case of severe accident management, the operators had to explain how they would transport mobile equipment, how they would refuel equipment, connect the equipment together technically and also prove that the tasks could be carried out by the shift-personnel. How the equipment is stored in a robust manner safe from seismic and flooding and where corresponding documentation is kept, also had to be explained. For open items, a clear time-schedule had to be given. The relevant locations were visited during the inspections.

8. New Layer seven

The central storage facility was requested by the Swiss Federal Nuclear Safety Inspectorate as an immediate measure and it was implemented only three months after the accident in Fukushima. The Swiss NPPs operators organized a common operating crew for the storage facility and submitted the operating

concept to the Swiss Federal Nuclear Safety Inspectorate. The Inspectorate reviewed this concept and inspected the storage facility. Pumps, diesel units, hoses, fuel, cabling as well as food and documentation are stored in a way to be easily accessible and transportable to the plant by truck or helicopter. The storage facility was fully set up in time and first training exercises proved the feasibility of the concept. The examination confirmed their readiness in practice for use. The safe and secure underground buildings are well maintained with industrial loading ramps for transportation by land or air. Though there was no practical doubt about the robustness of the storage facility against earthquake, it was however submitted to examination of the corresponding standards by a third-party expertise.

In a training exercise, the transportation of a heavy generator by truck and a heavy pump by helicopter was demonstrated. The transportation was carried out by the Swiss army and the coordination with the ground personnel was drilled. Some improvements were identified and are being taken care of. Such training is scheduled to be repeated periodically.

9. Conclusion

Although the electrical systems of Swiss NPPs are built according the Defence-in-depth principle and are capable to withstand the defined design accidents, with the measures adopted on the Swiss NPPs two additional layers of electrical supply were reinforced or introduced. They consist in a sixth layer with the on-site accident management diesel generators and a seventh layer with the means of the off-site storage facility.

The implementation of these precautionary measures to cope with a long-lasting total station blackout was verified by the Swiss Federal Nuclear Safety Inspectorate. The inspections in all Swiss NPPs have shown that strategies to prevent core damages were revised since the Fukushima accident and measures in case of total station blackouts are in place.

ROBustness of ElECTrical SYStems

of Swiss NPPs

NEA OECD | CSNI International Workshop Paris, 1st-4th of April 2014

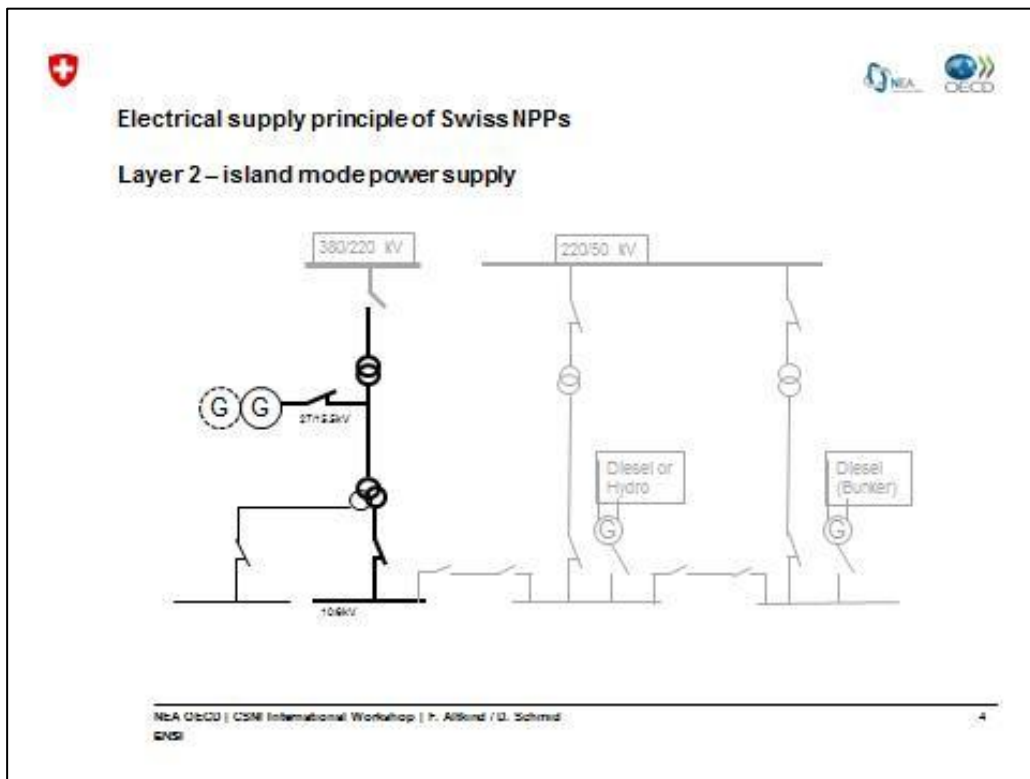
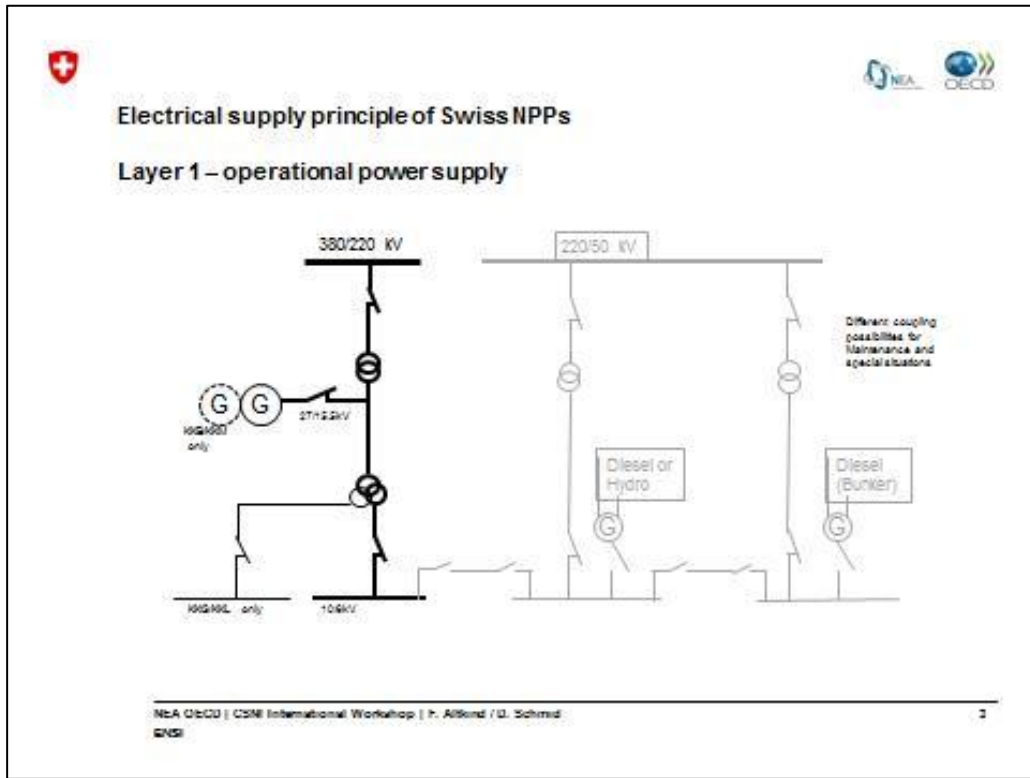
F. Altkind / D. Schmid

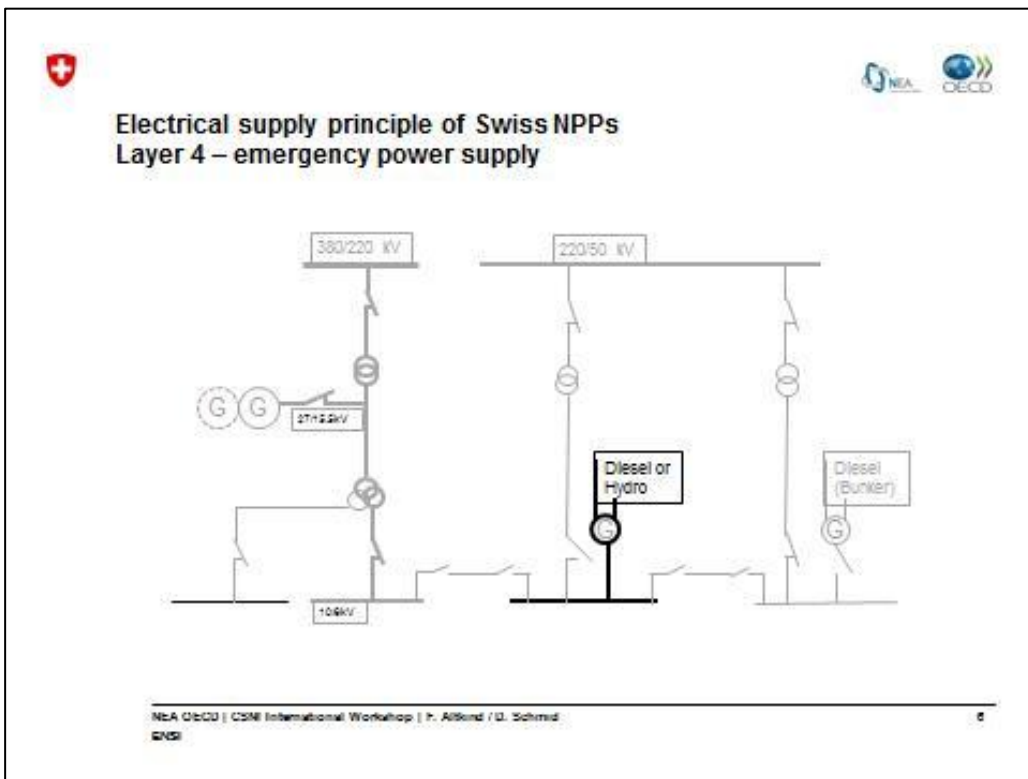
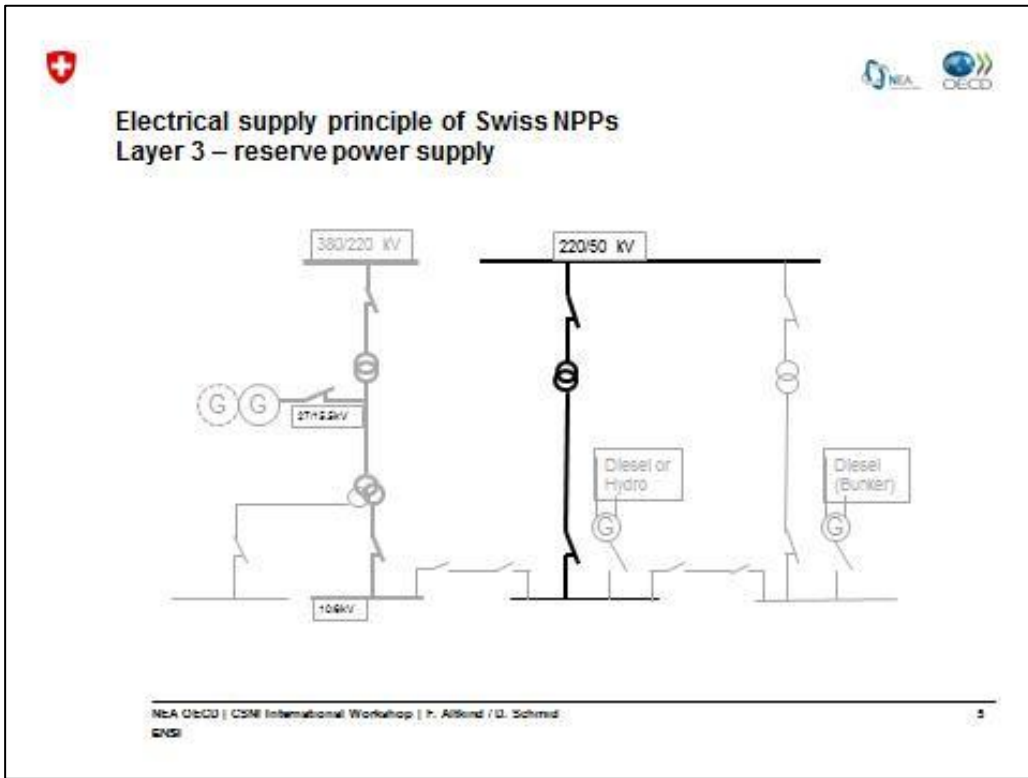
ENSI

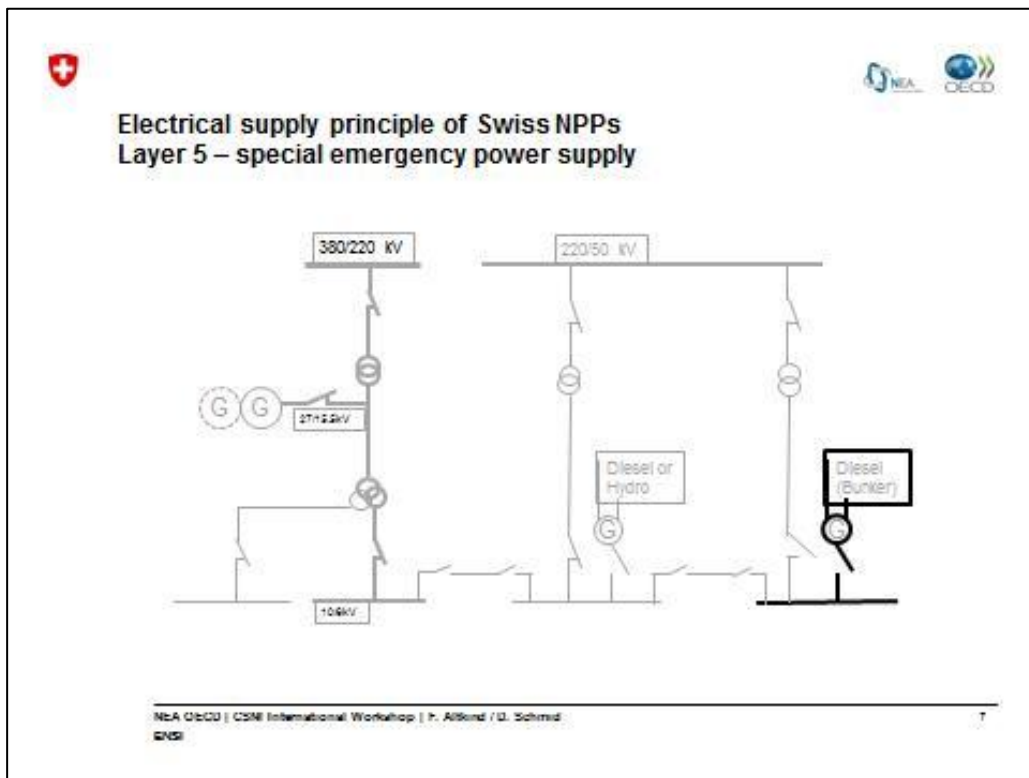


Overview of Swiss NPPs











Impact of Fukushima

As a measure directly triggered by Fukushima, the Swiss Nuclear Authority required one centralised electrical supply material depot useable in case of an unlikely but extreme hazard in a NPP.

In addition, the operators added procedures and equipment which are available on-site in prepared condition to be used in such a case.

NEA OECD | CSNI International Workshop | P. Allford / G. Schmid
ENSI



Assumptions on loss of power supply

Investigation for a long-lasting loss of power supply by the Nuclear Regulatory Authority (ENSI)

Case 1: No Emergency Diesel/Hydro available
=> Supply with special (bunkered) emergency diesel generators





Case 2: No special emergency Diesel available
=> Supply with SAMG generators

NEA OECD | CSNI International Workshop | P. Allford / G. Schmid
ENSI

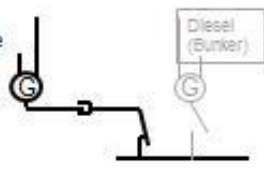



Electrical SAMG equipment in case of a total station-blackout

Layer 6 and 7 power supply

Diesel-Module available and prepared on-site (Layer 6)



Or

From storage facility (Layer 7)

NEA OECD | CSNI International Workshop | P. Allford / G. Schmid
ENSI






External (electrical) supply storage facility (Layer 7)

- Located at approx. 50km from all Swiss NPPs
- Operational since 1 June 2011
- Transport by helicopter < 2000 kg
- Bunkered army depot
 - Diesel generators incl. fuel
 - Pumps and hoses
 - Cables
 - Boric acid
 - Radioprotection equipment
 - Documentation / tools / food










NEA/OECD | CSNI International Workshop | P. Allford / G. Schmid
ENSI

11



Conclusion / Summary

After the Fukushima event, the electrical design has been revised and found to be as required by existing regulations.

Nevertheless, to deal with the case of a total station-blackout, additional equipment has been allocated, allowing the supply of electricity to the NPP on a well-prepared ad hoc basis.

NEA/OECD | CSNI International Workshop | P. Allford / G. Schmid
ENSI

12



***Thank you for your
attention***

for more information please visit:



**www.ensi.ch
www.ifsni.ch**

**Strengthening the First Line of Defence:
Delayed Turbine Trip at SCRAM in Westinghouse type NPP's**

Ir. M.A.J. (Marcel) van Berlo

KFD (Authority for Nuclear Safety and Security ANVS),

Ministry of Infrastructure and Environment,

The Netherlands

Abstract

The availability of Information, Control and Power (ICP) is not treated as a Critical Safety Function (CSF). After the Forsmark (2006) and Fukushima (2011) incidents there is reason to add ICP as a separate CSF. Adding ICP as a separate CSF would possibly lead to procedural adaptations, or even design changes, for Nuclear Power Plants.

As an example, this paper focusses on the transitions immediately after a SCRAM. At a SCRAM in many nuclear power plants the turbine is tripped immediately to prevent the extraction of too much heat from the reactor. However this requires a large and fast transition for the entire secondary system. The rescheduled priorities could lead to the wish NOT to trip the turbine before load has been reduced and alternative power has been secured.

This paper discusses a “soft landing” for the turbine by keeping it running after the SCRAM. Turbine control can follow reactor power by controlling the pressure of the available residual steam from the steam generator. With a proper control design this enables a flexible and precise control of primary temperatures without any fast switching in the secondary system during the first ½ to 3 minutes. In this period reactor load and turbine power are smoothly lowered to minimum levels during of which automatic preparatory measures can be triggered. The normal transitions can be initiated in a staged form to provide a soft landing for the entire secondary and electrical system.

Introduction

In the Westinghouse concept for nuclear installations there is a direct coupling between a SCRAM of the reactor and the immediate trip of the steam turbine. The turbine load controller tries to keep constant power output to the grid. At a SCRAM the drop in available power from the core results in further opening of the turbine inlet valves. This will amplify the pressure drop and extract more heat from the primary water. At a SCRAM this must be prevented in order to prevent re-criticality. This is the background for the immediate trip of the turbine at a SCRAM. However this turbine trip is a major transient for the entire secondary system:

1. the turbine
2. the turbine bypass system
3. the condensate and feedwater loop
4. the steamgenerators
5. the grid
6. the supply electrical power to the in-house load

This paper discusses this transient and the consequences for safe handling of the period immediately after the SCRAM. An alternative control strategy is proposed in which the turbine tip is separated from the SCRAM. This leads to a “soft landing” for the turbine avoiding most of the transients in the electrical- and condensate system. More over the ½ - 3 minutes that are gained will allow for starting of the Emergency Diesel Generators (EDG) as a running backup before power is switched. Even a staged transfer of internal load to either grid connection or EDG-power is possible while the turbine is still running at reduced power.

Background

In the wake of the 1979 Three Mile Island incident Westinghouse developed a procedural approach to improve nuclear safety with the goal to Prevent Radiation Release. This Emergency Operating Procedures (EOP, 1979) and Emergency Response Guideline's (ERG's) aimed at protecting the three barriers by fulfilling the requirements for the Critical Safety Functions (CSF).

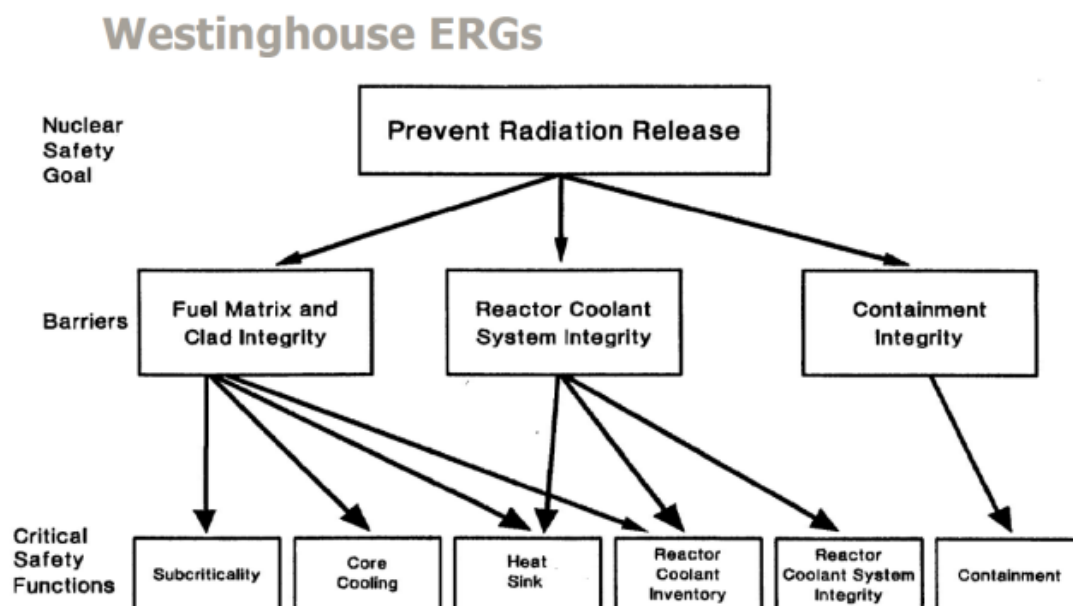


Figure 1. Critical Safety Factors as basis for Emergency Response Guidelines.

This well-developed approach is used for many nuclear installations in the world. A seventh CSF considered is the availability of utilities. At the Three Miles Island incident the problems were not directly related to the availability of Information, Control and Power (ICP), but much to the interpretation of the information. This explains the development of the six CSF's in the 80's. The provision of power is a high

priority in the Emergency Response Guidelines, but not as a CSF with its own priority. As Forsmark 2006 and Fukushima 2011 have shown ICP should probably be treated as a separate CSF. This would lead to a more systematic evaluation of:

- **Information:** information is the crucial resource for all processes that do not rely on passive or inherent mechanisms. Even for passive and inherent mechanisms information can be vital for evaluation of the situation. Much of the information is provided by process-instrumentation. Power requirements are generally relatively low (e.g. 1-100 W/instrument) which makes batteries a secure source of power for many hours. Use of large batteries for many combined information points and data handling creates a weakness in itself. In all cases an immediate loss of all information should be avoided. Batteries should be scheduled for a graceful degradation instead.
- **Control:** to make information useful options to execute actions are needed. For control-actions (e.g. by operating valves) the power requirements are somewhat higher (e.g. 0,1-10 kW/actuator), but the use is mostly intermittent with a low duty cycle (e.g. 1 min per hr), so that this can still be provided by batteries. In the classification of components options do (manual) actions over a (very) long time after a blackout should be considered.
- **Power:** is needed for active systems like pumps, fans, cranes etc.. The consumption is often too high for batteries and in practice Emergency Diesel Generators (EDG) are needed for providing emergency backup power. Grid and turbine are only sources capable of providing enough power to provide all functions of the first and second line of defence.

Figure 3.4.2-1: Robust power supply

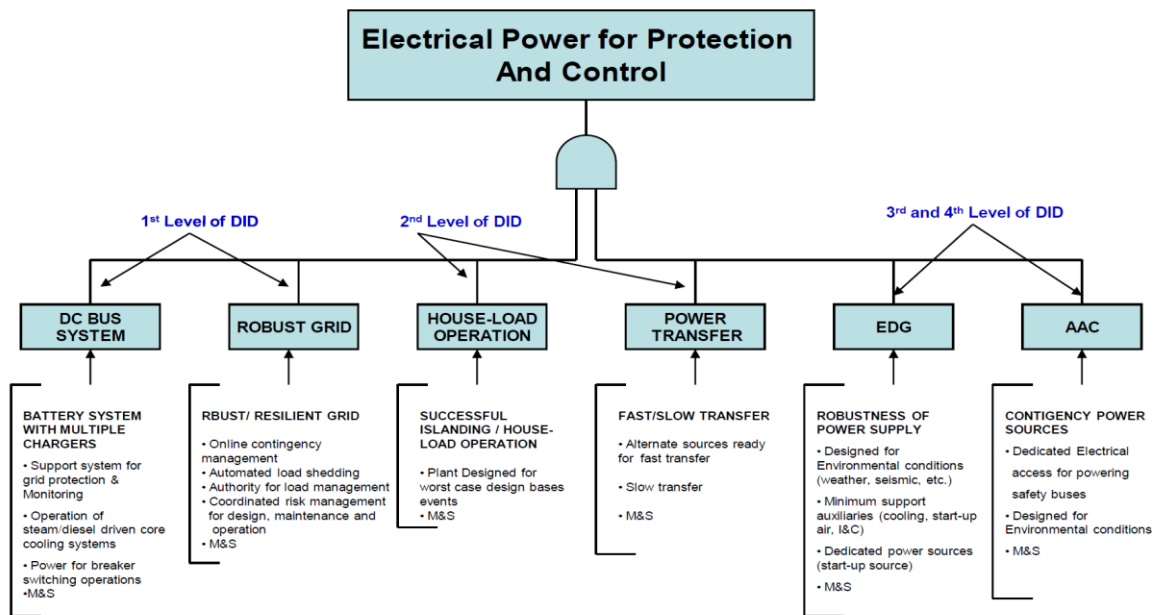


Figure 2. Levels of Defence in Depth for Power supply (NEA 2009, Didelsys p.68)

Adding ICP as a separate CSF would possibly lead to procedural adaptations, or even design changes, for Nuclear Power Plants. As an example in this paper we focus on the transitions immediately after a

SCRAM. The rescheduled priorities could lead to the wish NOT to trip the turbine before alternative power is secured.

Problem definition

In the Westinghouse concept for nuclear installations a SCRAM of the reactor is immediately tripping the steam turbine. A turbine trip, however, is a drastic action with profound impact for the entire installation (NEA, 2009-nov-9). It involves an immediate disconnection of the generator from the grid. The local grid can be influenced very much by the disconnection of the generator switch.

Depending on the configuration (machine-transformer, generator switch and startup-transformer) fast-transfer switching may be needed to provide in-house load. The voltage, frequency and phase variations caused by the switching are a risk of losing the grid connection or of triggering subsequent failures. In this case the second line of defence is lost as a direct consequence of giving up the first line of defence. Then there is a direct reliance on the EDG's. The limited power available from the EDG's has direct impact on the options to support the CSF's. Also the water-steam cycle is disrupted by tripping the turbine. This could disturb feed-water supply to the steam generators.

The reason for the immediate trip of the turbine at a SCRAM is a consequence of the chosen control structure in which the turbine is leading the power demand. The core is following the power demand by keeping temperatures of the primary coolant stable. However at a SCRAM the drop in available power from the core, and thus of the live steam pressure, will result in further opening of the turbine inlet valves. This way the turbine load controller amplifies the pressure drop and, via the steam generators, lowers the temperature of the primary coolant. At a SCRAM this must be prevented in order to prevent a renewed criticality. Therefore, normally, an immediate turbine trip is triggered at a SCRAM. As an alternative a concept for a smooth transition after a SCRAM is worked out below.

Consequences of a turbine trip

In the defence in depth concept the running turbine is effectively the major component of the first line of defence:

- It closes the water-steam cycle: because of its continuous operation it is an always tested and reliable heat sink.
- The turbine-generator: Generates power in parallel to the grid both stabilising and contributing to the reliability of power availability.

The problem with the turbine trip at a scram is that both functions are given up instantaneously and many components need to respond at the same time:

- Closure of turbine inlet valves and at the same time opening of turbine bypass valves and opening of the valves for water injection for steam cooling.
- Drastic load increase and temperature transient for main condenser.
- Disconnection of generator switch at full generator load (or of main switch and fast transfer to start transformer).

Due to the large power available at the moment of the trip the transients are maximal both on the steam-side and on the electrical side of the turbine-generator system.

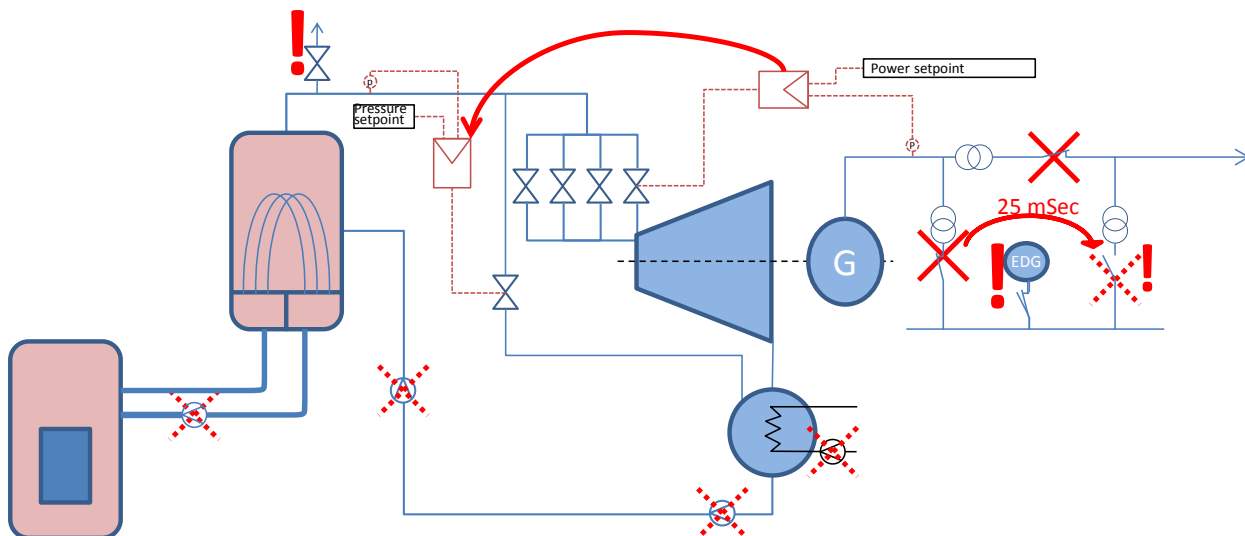


Figure 3. Function loss at failed transfer of electrical supply after turbine trip.

The trip of the generator generates large transients on the power lines it is a critical transition for the grid because full load is switched off unscheduled and must be compensated in seconds. The grid voltage, frequency and phase are disturbed and this can hamper local grid availability. Consequently reconnecting the alternative feed (start-up transformer) is having a significant chance of failure, inducing (partial) loss of electrical supply for the in-house-load. The internal configuration of the supply of the in-house-load (e.g. generator switch or start-up transformers) can cause different behaviour. See the evaluation report of the Forsmark incident by the DIDEISYS taskgroup (NEA, 2009-nov-9, p. 61)¹ for background on switching the power. As an example the scheme of Figure 1 indicates a failed transfer of the in-house-load from turbine-generator to grid supply. Then there is immediate reliance on the EDG's. Due to the limited power of these EDG's all main pumps are non-available with EDG-power. This way a turbine trip generates directly major additional consequences in the primary system.

The main components in the first line of the defence in the defence in depth are the running turbine and closed water-steam-cycle. The turbine-generator also is the first line of defence for the power supply. The problem with the turbine trip at a scram is that both functions are given up instantaneously with high transients due to the large power available at that moment. The many components that have to act under full load in a time critical transition are a risk of failure. Such failure could immediately hamper the second line of defence. Therefore it is proposed to operate as long as possible with the turbine-generator in its normal configuration.

Concept

Instead of tripping it, the turbine of a NPP could be used for handling the transition to a low power stage after a SCRAM. It requires that the turbine is kept online in a way that controls the requirements for the primary loop. The turbine inlet valves can be used for a smooth transition. Therefore the control of the turbine inlet valves should be switched from normal control of the generator power output to the control of the live steam pressure.

¹. NEA. (2009-nov-9). *Defence in Depth of Electrical Systems and Grid Interaction, Final DIDEISYS Task Group Report*. Nuclear Energy Agency, Committee On The Safety Of Nuclear Installations. OECD.

Live steam pressure is maintained following the same the time dependent pressure-setpoint as with the controller of the bypass valves. The amplification of the live steam pressure drop will be avoided. A feedforward steering will use the maximum available closing speed of the turbine inlet valves till the appropriate pressure and live steam quantity are reached. For the steam generators pressure variations could even be smaller because of the avoidance of timing problems normally caused by the transition from turbine inlet valves to turbine bypass valves. As a consequence the bypass valves will not be needed in the first time after the SCRAM and transients from the switch-over will be avoided.

This modification only involves adaptation of the turbine control system. The control behaviour of the turbine inlet valves can be designed the same way as the turbine bypass valves. It results in significant strengthening of the first line of defence by keeping the turbine running on the nuclear decay-heat for about ½ to 3 minutes after the SCRAM. This could improve the robustness of the plant for other failures immediately after the SCRAM.

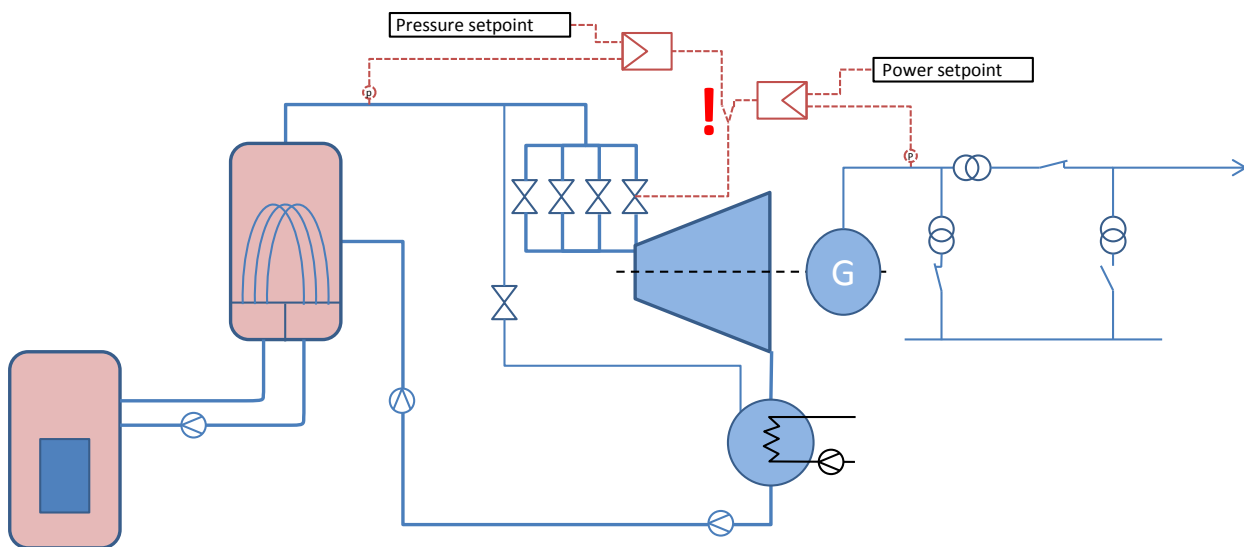


Figure 4. Switching of turbine control at SCRAM

With the proposed change the information flow will be reversed after the SCRAM: The nuclear decay heat decreases with a curve in time. The turbine inlet valves will follow the decreasing steam production by controlled throttling to keep the steam pressure stable. The turbine output power will be following the nuclear decay heat. It will be reduced to 4% of nominal power in about half a minute and will then decrease to 3,5% after a minute and to 3% after about 3 minutes². This can continue till the turbine Reverse-Power-Protection triggers and the turbine is switched off. At this time, the transient on the secondary water-steam-cycle and the electrical system is one or two orders of magnitude smaller.

Power supply is uninterrupted during this first minute. This means that all large pumps (Primary Coolant Pumps, cooling water pumps, condensate pumps and feedwater pumps) remain operative for the removal of large quantities of residual heat from the plant. The grid is stabilised by the running generator

². Garland, 1998, Decay heat estimates

and time is available to do necessary switching of components in a staged way. And because the secondary water-steam-cycle remains intact during this first minute the inventory of water in the steam generator and deaerator tank is preserved. In the time gained actions can be triggered to prepare a soft landing of the process. By continued use of the entire normal secondary loop during the first minute transition the chances of a Failure-on-Demand (FOD) will be decreased.

In the first half a minute action can be triggered to prepare a “soft landing” of the process. First of all operators get alerted before the mass of alarms from all secondary processes get triggered. The Emergency Diesel Generators (EDG’s) can be started in order to have them as running-standby. Even synchronisation of an EDG could be possible.

Consequences of delaying the turbine trip

Running the turbine deliberately after a SCRAM is a deviation from the Westinghouse approach used up to now. But it can be realised with relative little effort. It mainly involves switching the controller of the turbine inlet valves from normal control on generator power to control on the live steam pressure. The dynamics of the turbine inlet valves should be validated and compared to those of the turbine bypass valves. These parameters should be used for a control design that will guarantee optimum performance with regard to the influences on the primary loop. A PID-controller would probably be a simple and sufficient base for the design of the controller. A feed-forward signal could send the turbine inlet valves to a predefined position in anticipation of the required steam flow and pressure after the SCRAM.

The turbine will have to run for ½ to 3 minutes with a steam flow of 5-3%, which is below the normal minimum for the turbine. But as the steam flow is small and the time is short the erosion effect of wet steam on the turbine blades will be negligible. Generally turbine suppliers allow this low load operation for a limited number of hours per year. It is a load comparable to the load for island operation of the plant.

Possibly a number of other controllers of components in the secondary loop need to be validated for this transient. Performance can be improved by adding a feed-forward signal that triggers on the SCRAM command. In principle all these actions are less drastic with a delayed turbine trip than with an immediate turbine trip.

In a situation without a generator switch (NEA, 2009-nov-9, p. 61)³ the transfer of inhouse-load from turbine to grid connection can be done while the turbine is still connected to the grid. Then the turbine-grid connection is much more stable than when doing the transfer just at the moment of disconnecting the generator. This greatly improves the chance on a correct fast-transfer. This is a major contribution to the safety by keeping the first line of defence for power supply intact. Then it is possible to transfer in-house load in separately (per redundancy) to the grid. If one of these fails the EDG is already running and supply is restored with much less interruption. The soft running down power of the turbine-generator, instead of the instant trip at full load, is also favourable for the grid operator.

Conclusion

A relative simple addition to the turbine control can keep the turbine online for ½ to 3 minutes after a SCRAM. The turbine load controller can be switched to control of the live steam pressure with the turbine

³. NEA. (2009-nov-9). Defence in Depth of Electrical Systems and Grid Interaction, Final DIDELSYS Task Group Report. Nuclear Energy Agency, Committee On The Safety Of Nuclear Installations. OECD.

inlet valves. The turbine will then follow the decreasing production of decay-heat. This enables control of the life steam pressure without a transition to the turbine bypass valves.

The running generator stabilises the grid and power is gradually decreasing till the power reaches a minimum of only a few percent of nominal load. Only then the turbine is tripped. Transients in as well the secondary water-steam-cycle as the grid are one or two orders of magnitude smaller. This can be handled by the first line of defence and reduces risk of also losing the second line of defence.

During the time of pressure control preparations for a soft landing can be initiated. EDG's can be started and in-house-load can be fast-transferred to grid connection while the generator is still coupled to the grid. Staged switching of all components reduces chances on failure. For plant operators as well as the grid operator a smoother transfer is favourable.

 Ministry of Infrastructure and the Environment




Soft landing after SCRAM








Strengthening the first line of defence; Delayed trip of the turbine

Ir. M.A.J.(Marcel) van Berlo
KFD / Authority Nuclear Safety and Radiation Protection
The Netherlands

ROBELSYS
Robustness of Electrical Systems
Lessons Learned Fukushima
Paris, April 1-4, 2014


 **KFD: Authority Nuclear Safety and Radiation Protection**

The KFD Department of Nuclear and Radiological Safety, Security and Safeguards in the Netherlands monitors nuclear facilities, storage and transport of nuclear material and non-proliferation (preventing proliferation) of nuclear materials and technology.



In the Netherlands:

- 1 NPP
- 2 Research reactors
- Fuel processing
- Waste storage
- Isotope production

 2

Ministry of Infrastructure and the Environment 1 April 2014




The Netherlands – NPP Borssele

- The Netherlands have **one commercial nuclear power plant** in operation:
- **NPP Borssele**
 - IRS plant code: NL-2
 - PWR, 510 Mwe
 - Start of operation 1973
 - LTE envisaged until 2033



3 Ministry of Infrastructure and the Environment 1 April 2014



Critical Safety Functions Westinghouse ERGs

Nuclear Safety Goal

Prevent Radiation Release

↓

Barriers

Fuel Matrix and Clad Integrity

Reactor Coolant System Integrity

Containment Integrity

↓

Critical Safety Functions

Subcriticality

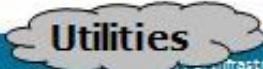
Core Cooling

Heat Sink

Reactor Coolant Inventory

Reactor Coolant System Integrity

Containment



4 Ministry of Infrastructure and the Environment 1 April 2014

Critical Safety Functions

Three Mile Island is the origin of CSF's.
Based on problem with interpretation of information

Forsmark and Fukushima have shown problems with:

- **P**ower
- **C**ontrol
- **I**nformation

5 Ministry of Infrastructure and the Environment 1 April 2014

Critical Safety Functions

Electrical and Control systems are used to mitigate Other risks.

Electrical systems are interconnected

Needed: **Additional Separate CSF for ICP.**

6 Ministry of Infrastructure and the Environment 1 April 2014



Power, Information and Control

Information, **C**ontrol and **P**ower should be assigned a separate **Critical Safety Function (CSF)**


Information is crucial for assessment of the situation, even if there is no problem.
Limited power is needed per instrument (e.g. 10-100 Watt/instrument)

Control is crucial for having options to react on situations.
Power use is limited to short intervals (e.g. 1000 Watt/valve for 1 minute per hour)

Power for small components.
10-500 kW/motor, could be continuous

Robustness = Graceful Degradation path

7 Ministry of Infrastructure and the Environment 1 April 2014



Soft landing after Scram

At the NPP Borssele (NL) turbine load control on fixed electrical output that will continue to extract maximum energy out of the reactor at a **SCRAM**.

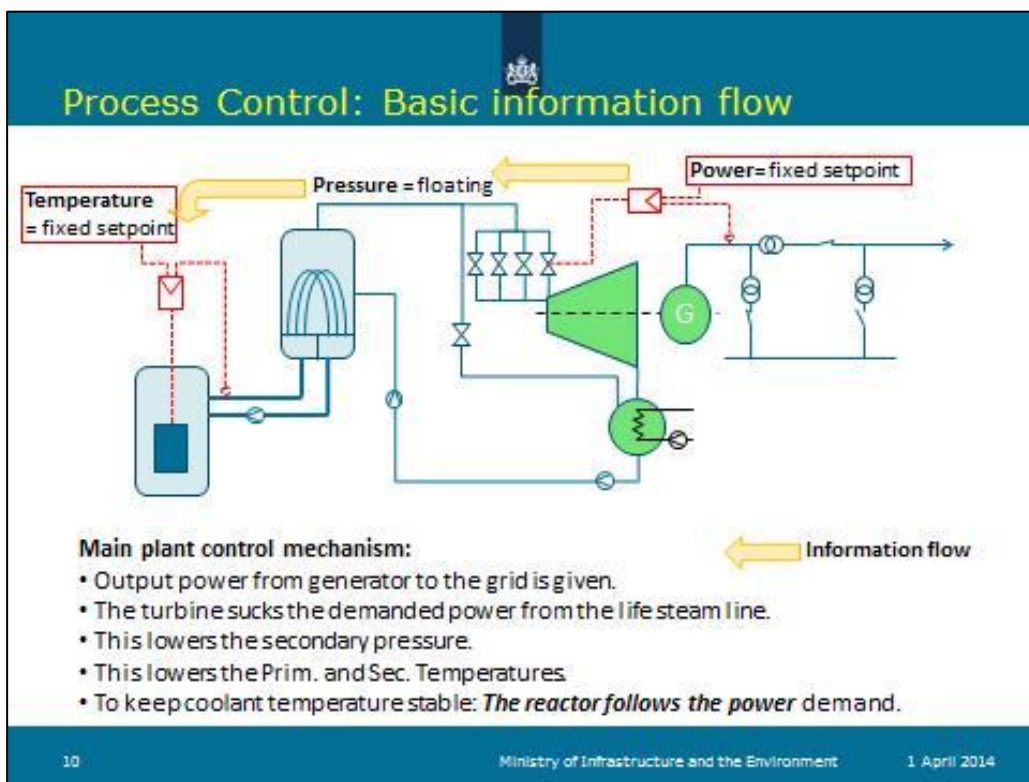
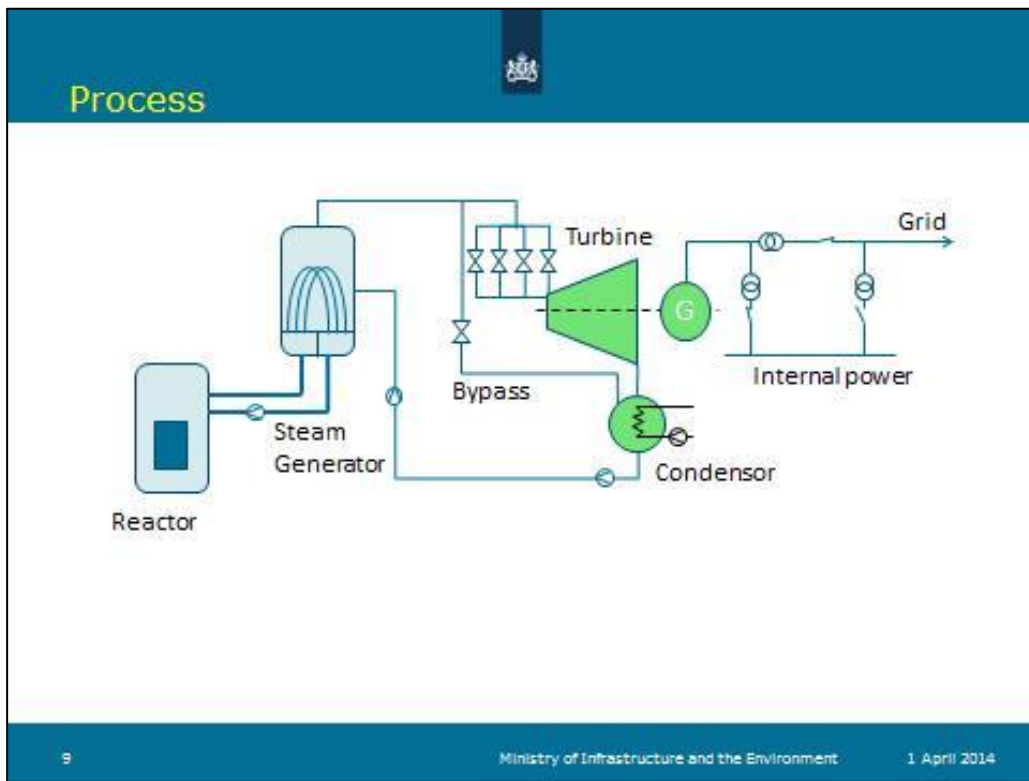
Therefore a SCRAM is automatically inducing an **immediate turbine trip**. This is a major transient in the entire secondary and electrical system. This has also major secondary implications for the primary system and the availability of utilities.

The philosophy should be to keep the turbine running as long as possible.

The transition can be postponed for one to several minutes when power levels are much lower. Therefore grid implications are smoothed out which reduces the risk of Losing Of Offsite Power (LOOP). In the mean time switching of components can be staged and chances of component failure or Station BlackOut (SBO) can be significantly reduced.

Following sheets explain this strengthening of the first line of defence.

8 Ministry of Infrastructure and the Environment 1 April 2014



Conventional transfer at SCRAM

BANG – BANG transfer

Full power trip

• Electrical power switch off:	515 MW _e	~10mSec (half a period)
• Reconnect startup transformers:	25 MW _e	<25 mSec
• Steam flow cutt off:	375 kg/sec	in 2sec
• Steam bypass opening + water injection		in 2 sec

Transfer is initiated before SCRAM is evaluated !

April 2014

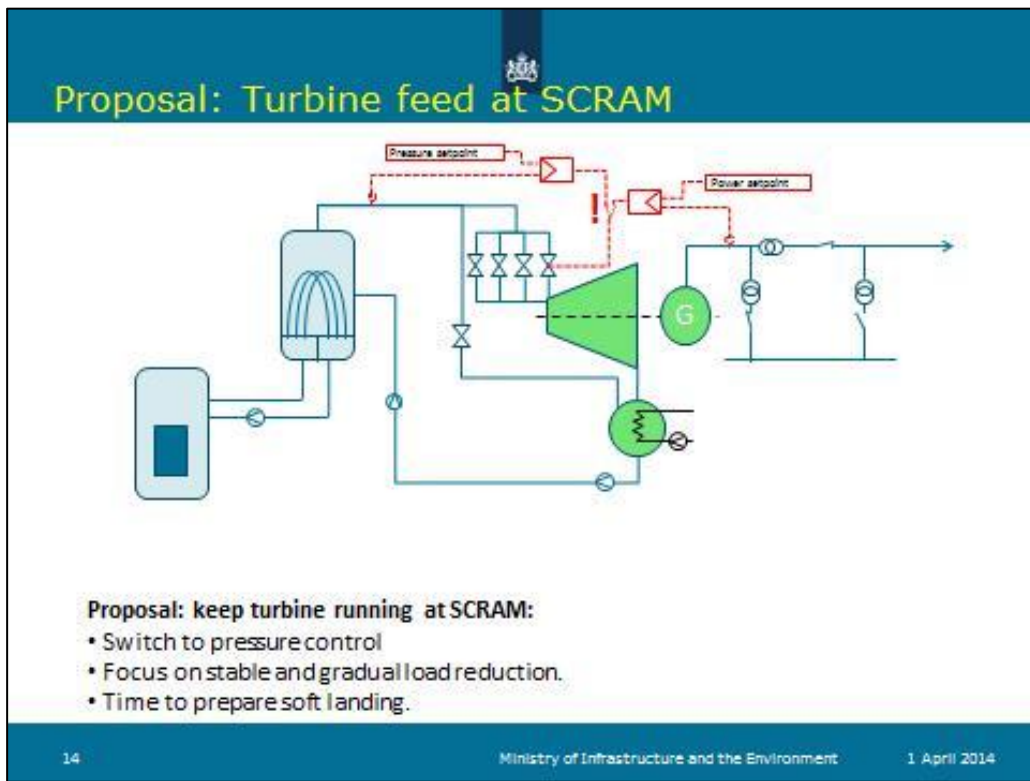
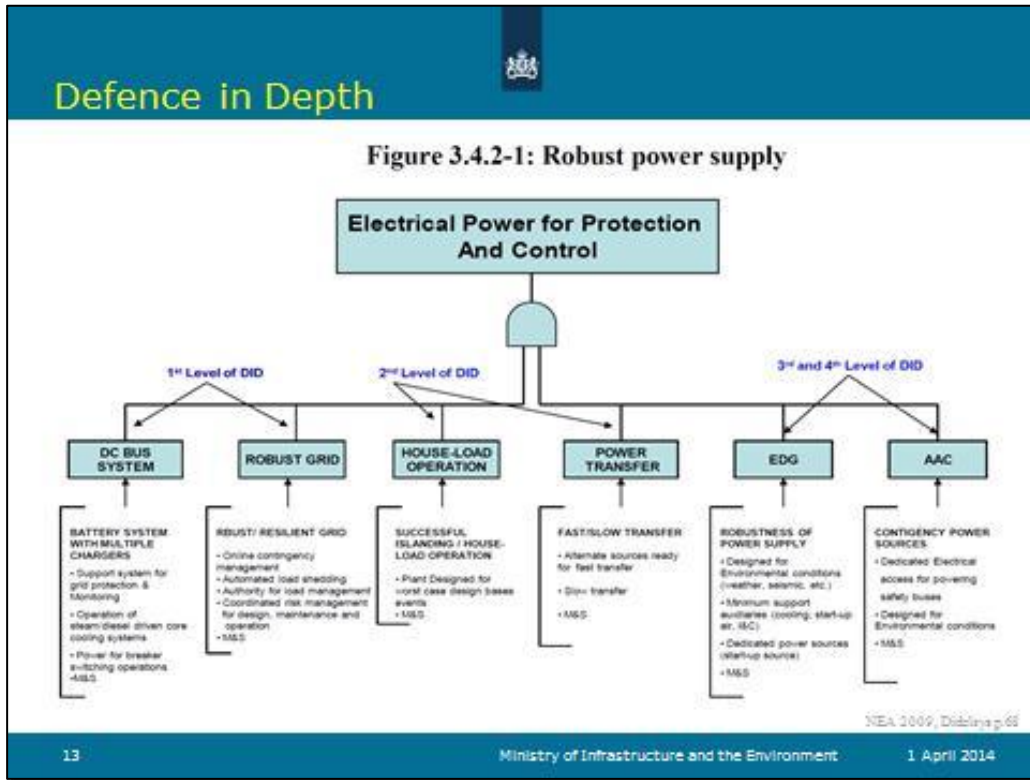
Failed transfer after SCRAM

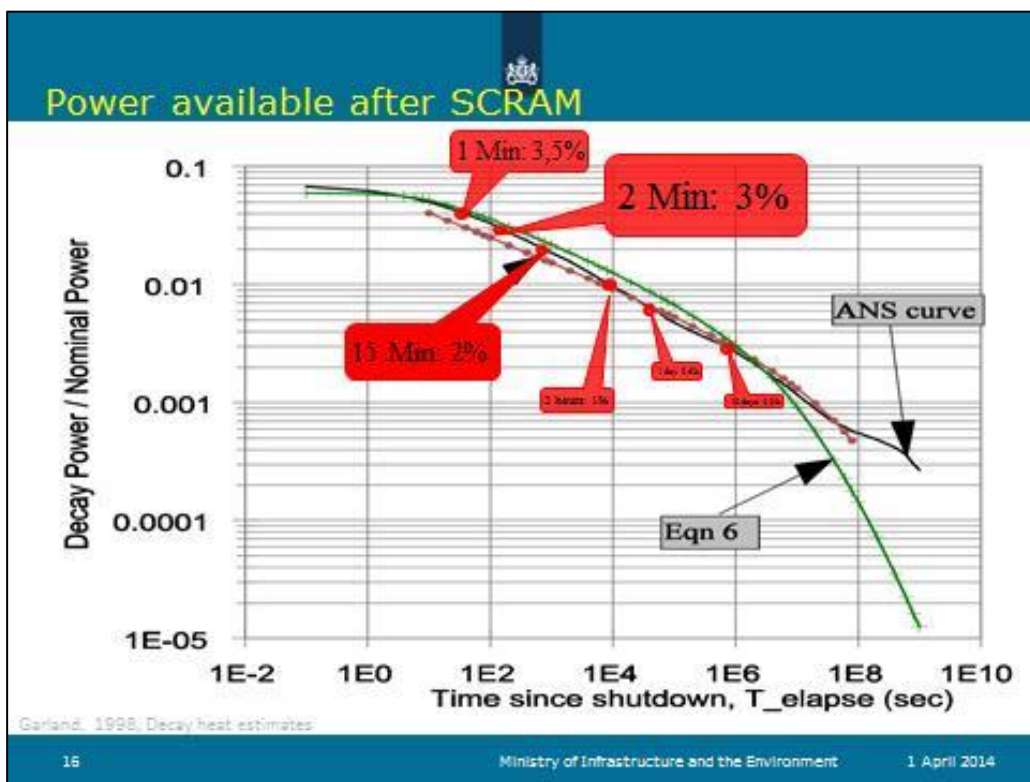
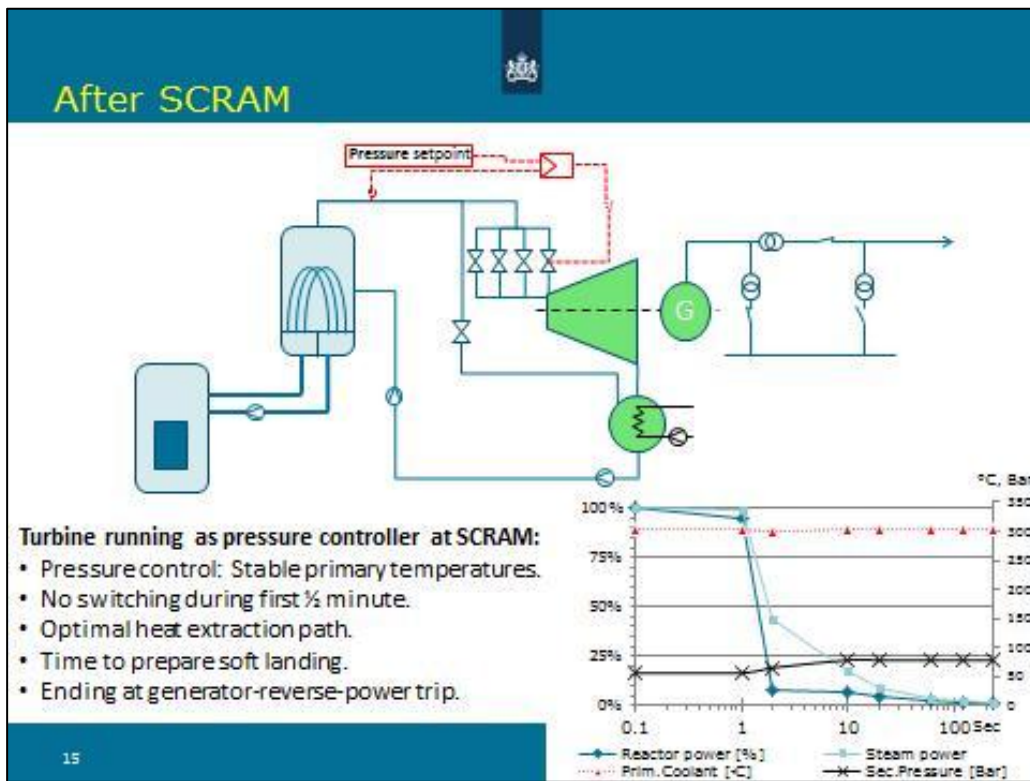
If transfers fails:

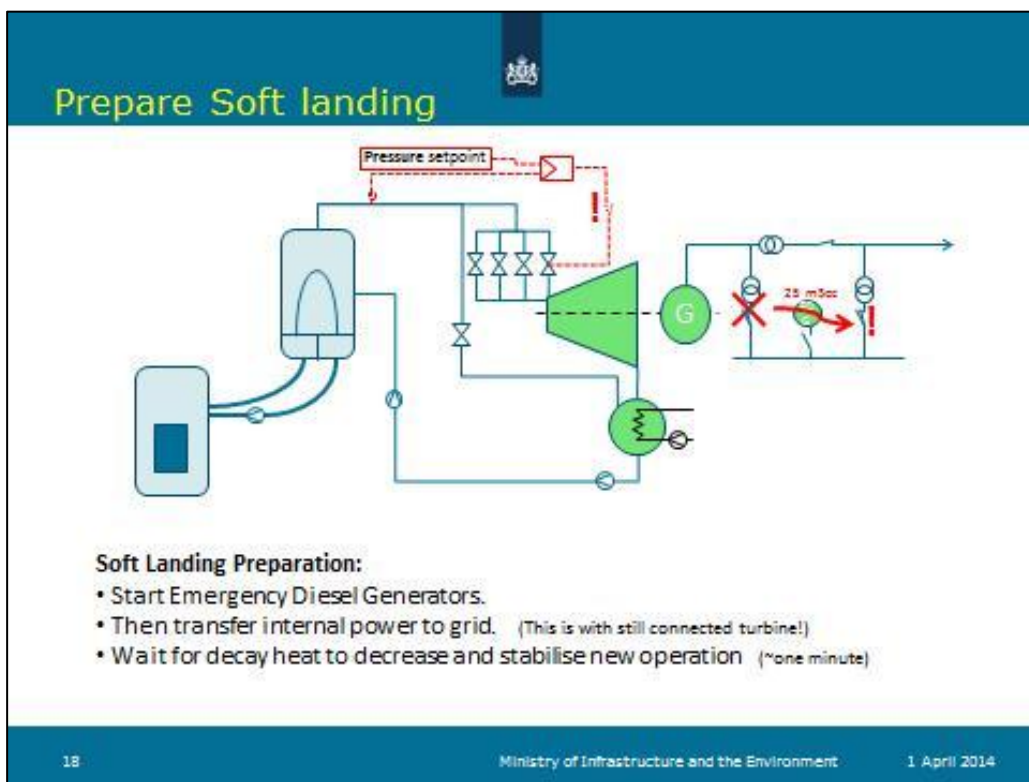
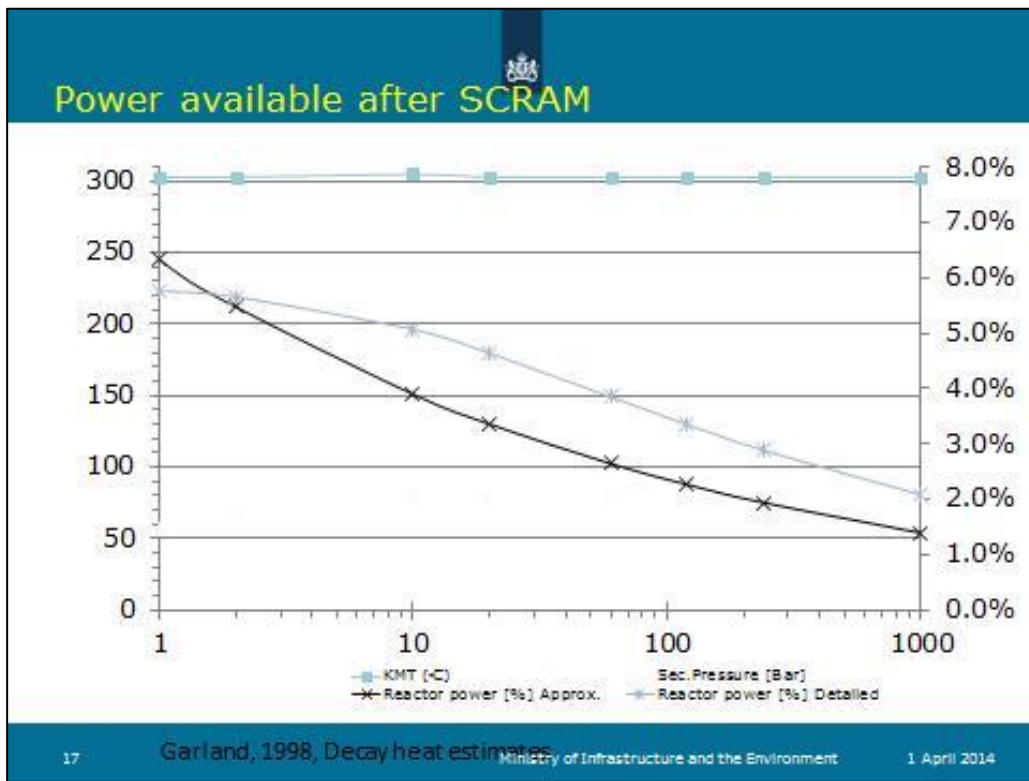
- Loss of all high-power pumps
- Loss off water steam cycle
- Full dependency on diesel engines, only available for selected emergency equipment

This is a SINGLE "failure", impairing primary and secondary system

1 April 2014







Transfer to bypass operation (~2 minutes)

Soft Landing Procedure:

- Open bypass valve.
- At Reverse Power from Generator protection disconnect generator (at low power condition).

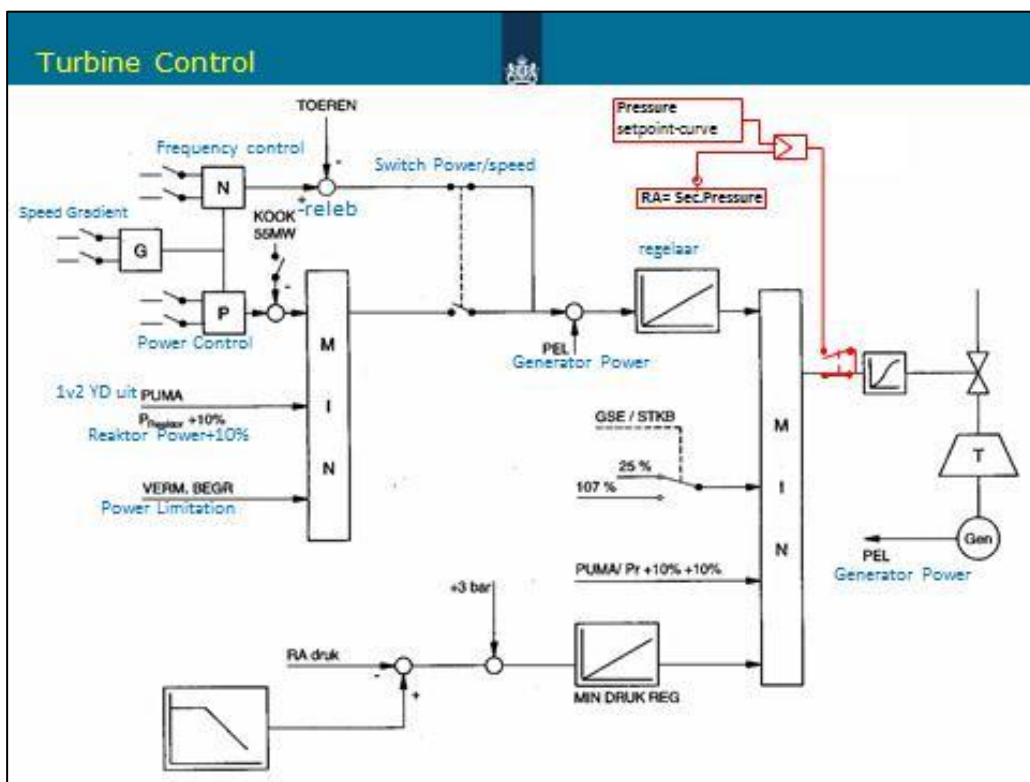
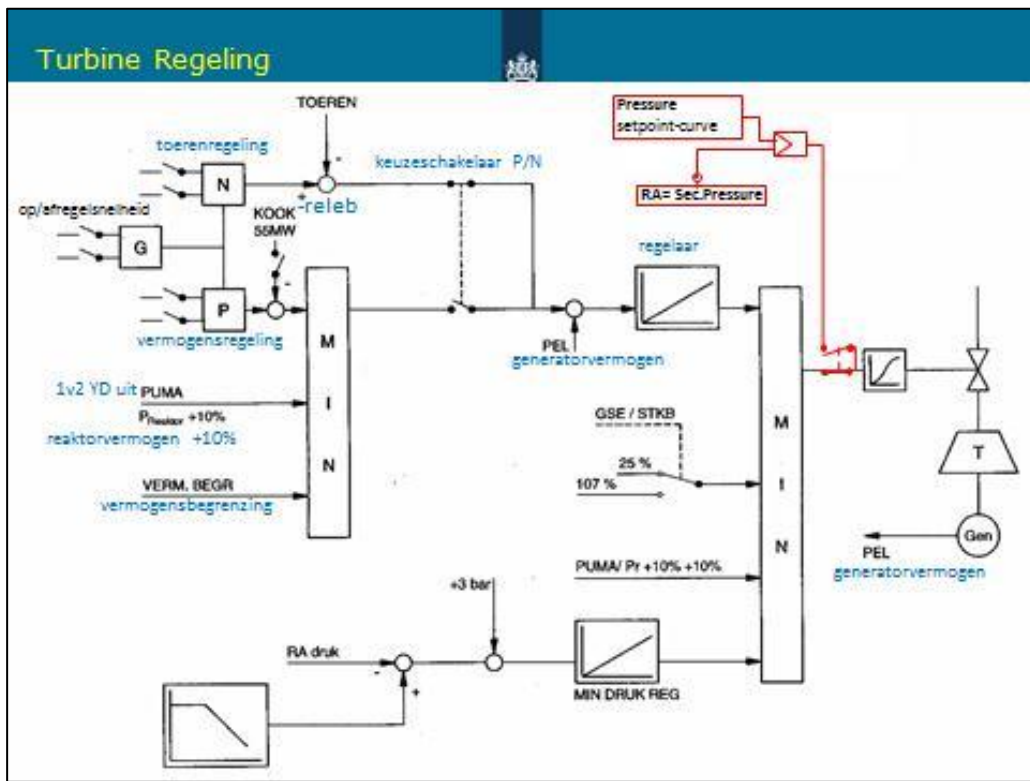
19 Ministry of Infrastructure and the Environment 1 April 2014

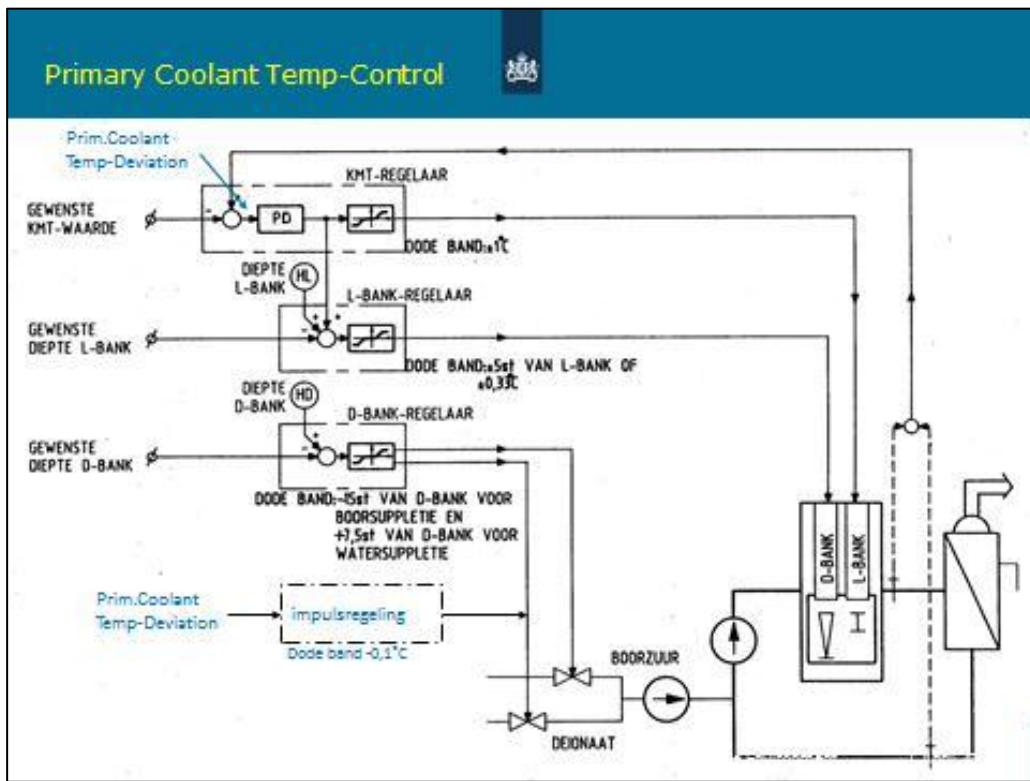
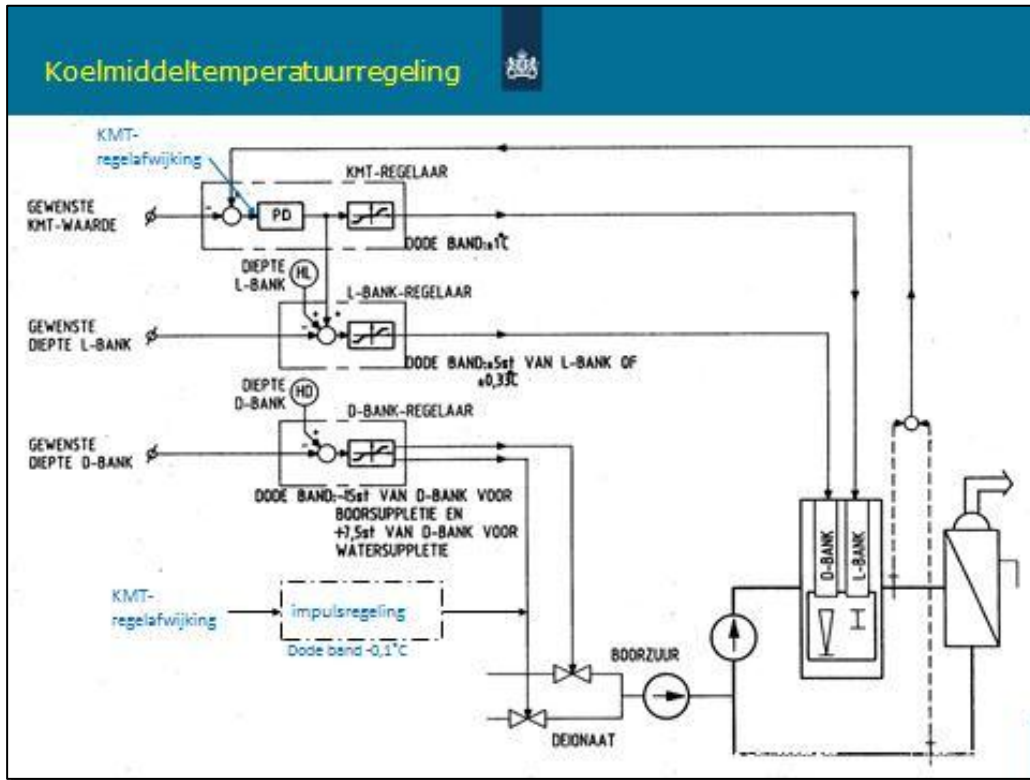
Soft landing options: Master-Slave control

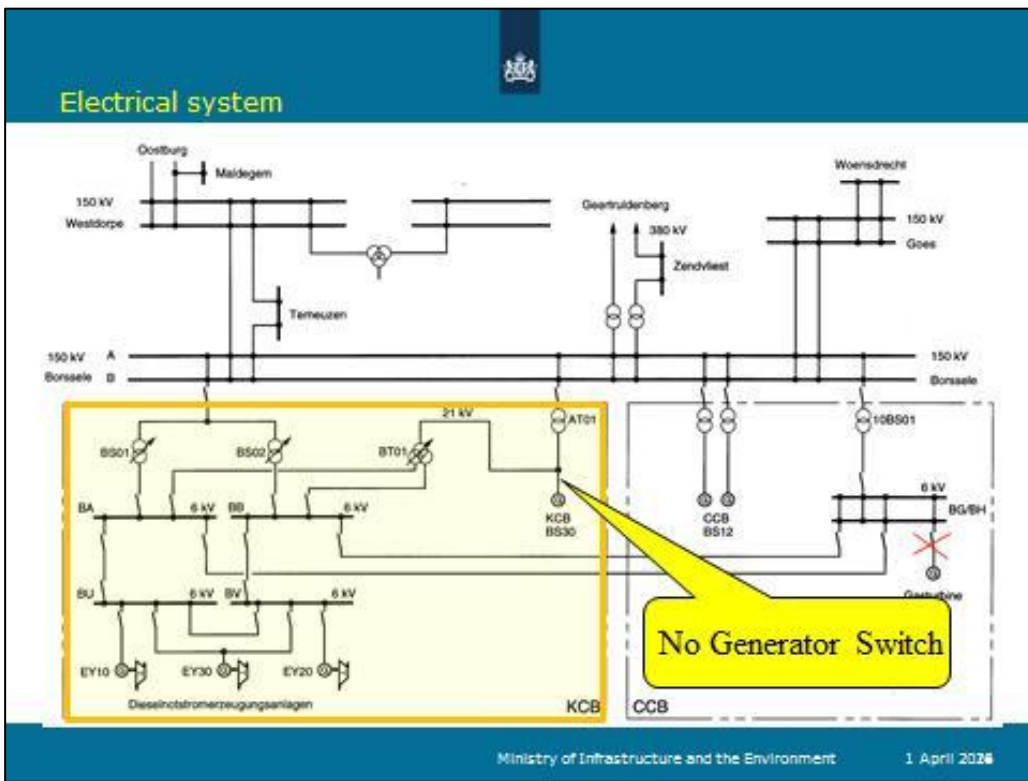
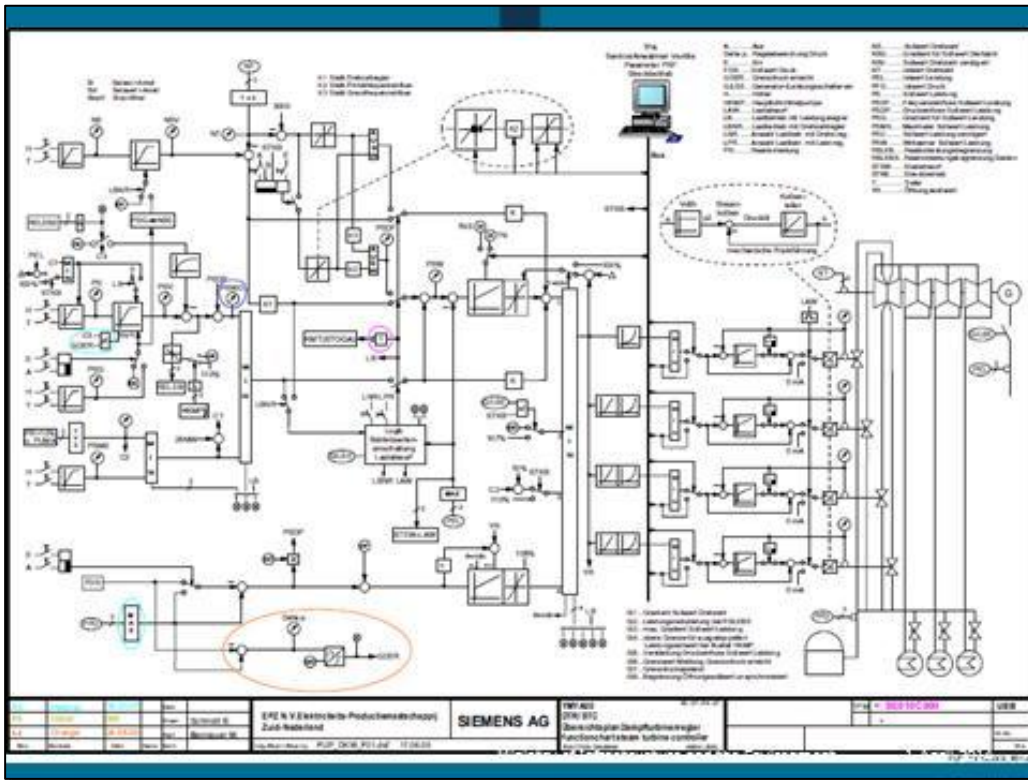
Options to consider:


1. Staged transfer of redundancies from turbine to grid.
2. Master-Slave control of primary coolant temperature.

20 Ministry of Infrastructure and the Environment 1 April 2014









Conclusion after Fukushima

Power, **I**nformation and **C**ontrol should be assigned a separate **Critical Safety Function (CSF)**


The turbine is first line of defence:
At a Scram the philosophy should be to keep the turbine running as long as possible.

Transients in the entire secondary and electrical system can be reduced significantly.

The risk of Losing Of Offsite Power (LOOP) can be reduced.

Requires only a simple additional pressure-controller

27Ministry of Infrastructure and the Environment1 April 2014



Perspective

Any reliance on outside world is a risk in itself.

Long term autarky autonomous operation of key electrical systems on decay heat

Primary loop in medium hot standby (e.g. 200°C, 40bar)
 Secondary micro-turbine (e.g. 200°C, 10 bar, <1 MW)

Air cooled condenser.
 Minimum equipment involved
 No EDG.

28Ministry of Infrastructure and the Environment1 April 2014

SESSION THREE

"Requirements for Robustness of Onsite Electric Power Systems"

Electrical Systems Design Applications on Japanese PWR Plants in Light of the Fukushima Daiichi Accident

Tsutomu Nomoto (MHI, Japan)

Effects of Common Cause Failure on Electrical Systems

Kevin Pepper (ONR, UK)

A Survey of the Hazards to Electrical Power Systems

Gary Johnson (Independent Consultant, USA)

Modernization of Unit 2 at Oskarshamn NPP – Main Objectives, Experience from Design, Separation of Operational and Nuclear Safety Equipment – Lessons Learned

Salah Kanaan (E.ON/OKG, Sweden)

RCC-E A Design Code for I&C and Electrical Systems

Jean-Michel Haure (EDF, France)

Overall Strategy and Architecture for Post-Fukushima-Mitigation and Mitigation on Other Events in the Electrical Systems

Waldemar Geissler (AREVA, Germany)

Comparison Between Different Power Sources for Emergency Power Supply at Nuclear Power Plants

Magnus Lenasson (Solvina AB/Sweden)

Advancing Ruggedness of Nuclear Stations by Expanding Defence in Depth in Critical Areas

Thomas Koshy (IAEA)

Electrical systems design applications on Japanese PWR plants in light of the Fukushima Daiichi Accident

Tsutomu Nomoto

MHI, Japan

Abstract

After the Fukushima Daiichi nuclear power plant (1F-NPP) accident (i.e. Station Blackout), several design enhancements have been incorporated or are under considering to Mitsubishi PWR plants' design of not only operational plants' design but also new plants' design.

Especially, there are several important enhancements in the area of the electrical system design. In this presentation, design enhancements related to following electrical systems/equipment are introduced;

- Offsite Power System
- Emergency Power Source
- Safety-related Battery
- Alternative AC Power Supply Systems

In addition, relevant design requirements/conditions which are or will be considered in Mitsubishi PWR plants are introduced.

1. Introduction of the Japanese PWR Plants

Currently, Japan has total 24 PWR plants and the electric output per unit is 340-579MWe for 2-loop plants, 826-912MWe for 3-loop plants, and 1160-1180MWe for 4-loop plants. Each PWR plant location is shown in Figure 1. The figure also shows its position and distance from the epicenter of the earthquake which triggered the 1F-NPP accident. The figure shows that all the PWR plants are located away from the epicenter of the earthquake and fortunately they suffered little damage caused by tsunami.

As of April 2014, all the nuclear power plants in Japan including PWR and BWR are not in operation and a safety review are being performed to restart operations.

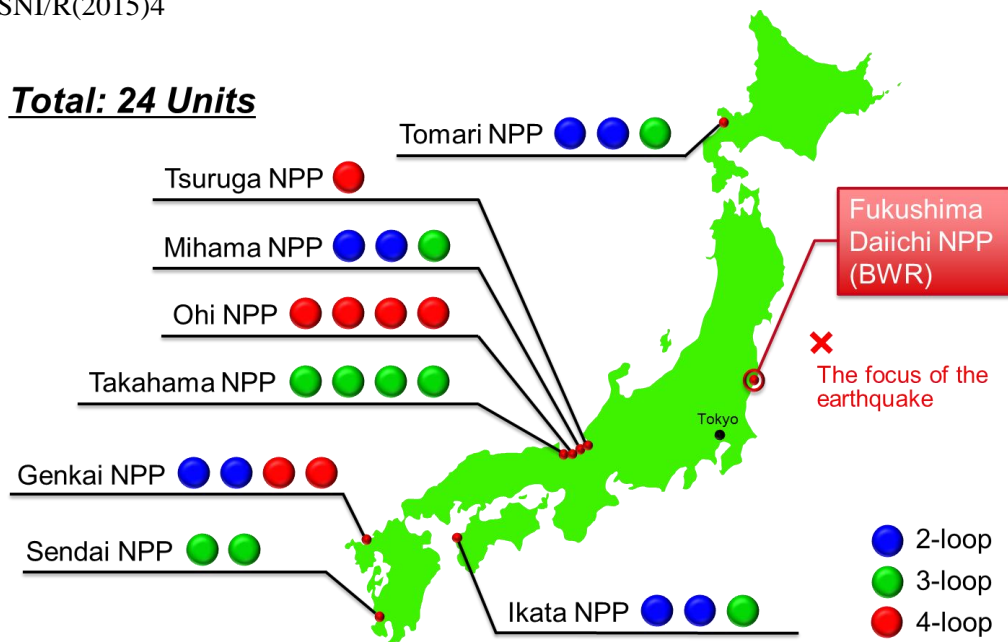


Figure 1. Site Location of the Japanese PWR Plants

2. Changes in the Japanese Regulatory Requirements Before and After the 1F-NPP Accident

Before the 1F-NPP accident, the nuclear power plants in Japan were designed in accordance with the following guideline:

- Review Guide for Safety Design of Light Water Nuclear Power Reactor Facilities

This guideline required design consideration for SBO events as well as design requirements for Design Basis Condition (DBC). However, the SBO duration assumed in the guideline was very short compared to that of the 1F-NPP accident.

Since the 1F-NPP accident, the regulatory requirements had been reviewed in light of the lessons learned from the accident, and the following new regulatory standards went into effect on July 8, 2013:

- Regulation on the Technical Standards for Commercial Nuclear Power Reactors and Associated Facilities

In the new regulatory standards, the design requirements for DBC have been enhanced, and in addition, those for Design Extension Condition (DEC) have been enhanced and added. Especially, in consideration of the fact that the 1F-NPP accident had evolved into severe accident due to the extended SBO, the new regulatory standards have included several important enhancements to electrical design. The main design requirements/conditions are as follows:

- Improvement of reliability of the Offsite Power System
- Increase of the safety-related battery discharge duration
- Increase of the fuel tank capacity for the emergency power source
- Installation of alternative power supply system
- Enhancement of the protective capability against Extreme External Hazard
- Enhancement of the protective capability against terrorism/airplane crash

The safety review based on the new regulatory standards is currently being performed for the nuclear power plants in Japan. To enhance safety of the electrical system of the Mitsubishi PWR plants, some of the above requirements have been incorporated to their electrical design and some are under consideration. Section 3 below shows in detail the improved design principles and typical examples of how they are incorporated in the actual design.

3. Design Improvement on the Electrical Power Systems

3.1 Offsite Power System

The regulatory requirements before the 1F-NPP accident required that the offsite power system be designed to connect to a power grid via two or more transmission lines, but independency of each transmission line was not considered.

The regulatory requirements after the 1F-NPP accident require that two or more transmission lines be independent from each other. This design can prevent loss of all the transmission lines even if one of the substations or switchyards fails. Also, the new regulatory requirements consider increase of a seismic capacity for equipment/structures associated with the offsite power system to the extent possible, although the offsite power system is non-safety classified. These design improvements enhance reliability of the offsite power system.

3.2 Emergency Power Source

Before the 1F-NPP accident, emergency power sources had enough fuel stored onsite to supply power to required loads for two to seven days. This capacity was determined for each plant by considering the time needed to transport fuel from offsite for replenishment.

The regulatory requirements after the 1F-NPP accident assume that duration of loss of offsite power is at least seven days. Therefore, any plants need to store fuel for emergency power sources onsite, which is sufficient to operate for seven days. This enhances the functionality of emergency power sources.

3.3 Safety-related Battery

Before the 1F-NPP accident, there were no national guidelines which stated safety-related battery capacity. Therefore, safety-related battery capacity was designed to be two hours based on the American standard “Supplementary Criteria for Electrical Power Systems for Nuclear Power Plants.” However, assuming SBO events like the 1F-NPP accident, it is necessary to increase battery capacity to cope with the events using only dc power supply until restoration of ac power.

In light of the above lessons learned, the regulatory requirements after the 1F-NPP accident clearly state the safety-related battery capacity as follows:

- Batteries should supply electric power for 8 hours without switching off the loads. After 8 hours, the system should supply electric power for subsequent 16 hours (i.e. 24 hours in total) with switching off the loads not required for safety purpose.

Based on this requirement, it is necessary to increase the safety-related battery capacity so as to supply power to required loads for 24 hours. The increase of battery capacity can be done by replacing with larger capacity battery or providing additional batteries.

3.4 Alternative Power Supply Systems/Equipment

The regulatory requirements before the 1F-NPP accident did not require installation of back-up ac power supply, i.e. alternative AC (AAC) power supply system, onsite, because early restoration of offsite power or emergency power sources were expected. However, considering the case of the Extreme External Hazard which was experienced during the 1F-NPP accident, it is necessary to assume that the offsite power and emergency power sources cannot be restored for a prolonged time.

In light of the above lessons learned, the new regulatory standards require installation of alternative power supply systems/equipment as follows:

- Deployment of transportable alternative power supply systems/equipment (e.g. power supply vehicle and batteries)
- Installation of alternate current power supply system as a permanently-installed alternative power supply system

In addition, the new regulatory standards require that alternative power supply systems/equipment be independent and spatially separated from the DBC management system. These arrangements including the diversification mentioned in the later section ensure that ac power supply is available even in the event of SBO.

3.5 Loss of Normal Access to the UHS (LUHS)

All the PWR plants in Japan apply diesel generators (DGs) for emergency power sources. This type of engine needs cooling water to operate, i.e. UHS needs to maintain its function to operate the diesel engine. In this case, assuming that LUHS occurs due to external events, such as tsunami, all the emergency power sources will fail. Therefore, it is necessary to install power sources which do not rely on UHS, e.g. gas turbine generator (GTG) and air-cooled DG, in addition to emergency power sources. Applying this type of power source for AAC can provide diversity between AAC and EPS (water-cooled), increasing the reliability of the power supply systems.

3.6 Connection with Transportable AAC

As described in Section 3.4, Mitsubishi PWR plants are planning to install transportable AAC as alternative power supply equipment. This power source normally stands by in the area onsite where safety is ensured. In the event of SBO, it is moved near the building and connected manually to the connecting port provided on the outward wall of the building. Providing multiple connecting ports in different places prevent failure of connection due to common cause failure.

3.7 Extreme External Hazard

Before the 1F-NPP accident, plant design considered the effect of postulated natural phenomena, such as earthquake, tsunami, flood, and freeze. However, in the 1F-NPP accident, external hazards, i.e.

earthquake and tsunami, exceeding the design basis hit the plant and made the protection equipment incapable. Taking into account the lessons learned from this experience, protection against the Extreme External Hazard needs to be enhanced.

Specifically, the following protection measures can be considered:

- ✓ For protection against tsunami/flooding
 - Raising the height of the flood barrier
 - Provision of adequate water seals to openings of the building
 - Extension of the inlet/outlet duct of DG to locate the opening to a higher level
- ✓ For protection against tornado
 - Install a missile protection nets

3.8 Terrorism/Airplane Crash

Although the 1F-NPP accident was caused by natural phenomena, the new regulatory standards enhance the requirements for protection against not only natural external hazards but man-induced external hazards, e.g. terrorism and airplane crash.

Specifically, it is required that an independent facility be built outside the Reactor Building, which is equipped with necessary equipment/systems, to cope with loss of safety function in the Reactor Building due to terrorism or airplane crash. “Necessary equipment/systems” refer to those to prevent damage to the containment vessel, e.g. pumps, power and water sources, and monitoring and control systems.


ROBELSYS Workshop

**Electrical System's Design
Applications on Japanese PWR Plants
in light of the Fukushima Daiichi Accident**

1 - 4 April 2014


MITSUBISHI HEAVY INDUSTRIES, LTD.

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved.



MITSUBISHI
HEAVY INDUSTRIES, LTD.
Our Technologies. Your Tomorrow.

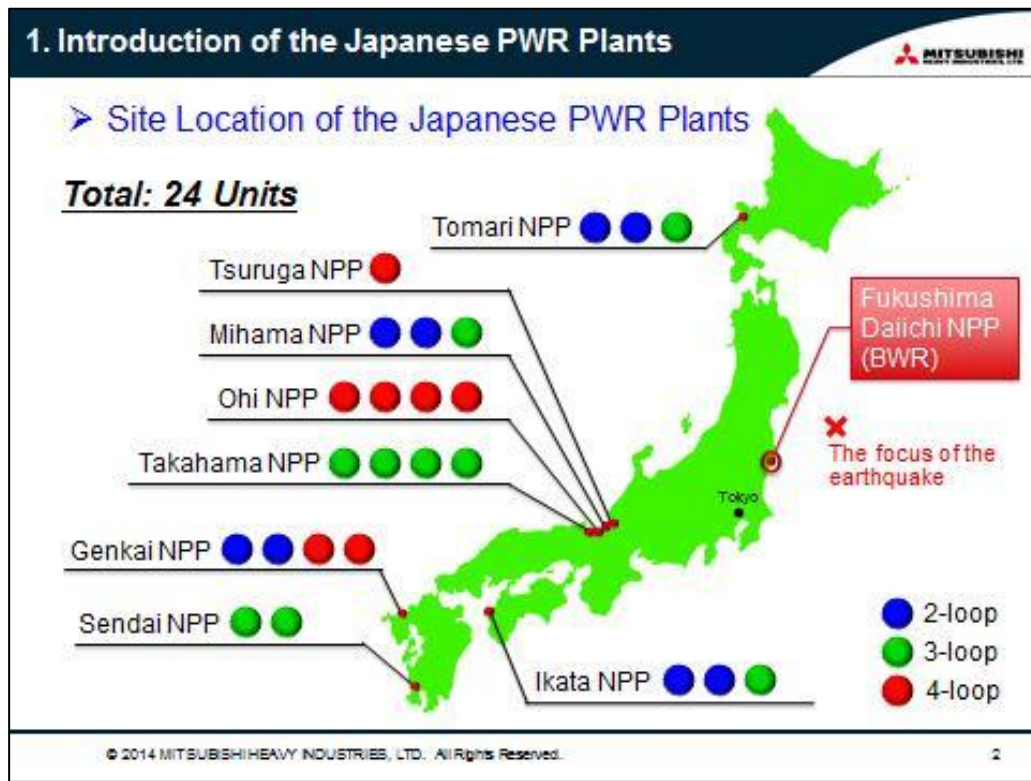
CONTENTS



1. Introduction of the Japanese PWR Plants
2. Changes in the Japanese Regulatory Requirements Before and After the Fukushima Daiichi Accident
3. Design Improvement on the Electrical Power Systems
 - 3.1 Offsite Power System
 - 3.2 Emergency Power Source
 - 3.3 Safety-related Battery
 - 3.4 Alternative Power Supply Systems/Equipment
 - 3.5 Loss of Normal Access to the UHS (LUHS)
 - 3.6 Connection with Transportable AAC
 - 3.7 Extreme External Hazard
 - 3.8 Terrorism/Airplane Crash
4. Conclusion

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved.

1



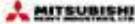
2. Changes in the Japanese Regulatory Requirements Before and After the Fukushima Accident

➤ Main Requirements for Electrical Design

Before Fukushima Daiichi Accident	After Fukushima Daiichi Accident
<p>➤ Regulation; "Review Guide for Safety Design of Light Water Nuclear Power Reactor Facilities"</p> <p>➤ Main Requirements;</p> <ul style="list-style-type: none"> ✓ Installation of emergency power supply systems ✓ Ensuring the redundancy and independency for emergency power supply systems ✓ Consideration of a short-term Station Blackout (SBO) for electrical design 	<p>➤ New Regulation; "Regulation on the Technical Standards for Commercial Nuclear Power Reactors and Associated Facilities"</p> <p>➤ Main Requirements;</p> <ul style="list-style-type: none"> ✓ Improvement of reliability of the Offsite Power System ✓ Increase of the safety-related battery discharge duration ✓ Increase of the fuel tank capacity for the emergency power source ✓ Installation of alternative power supply systems ✓ Enhancement of the protective capability against Extreme External Hazard ✓ Enhancement of the protective capability against terrorism

© 2013 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved. 3

Details about the Regulatory Requirements



➤ Before Fukushima Daiichi Accident

Review Guide for Safety Design of Light Water Nuclear Power Reactor Facilities

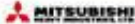
Guideline 27. Design Considerations against Loss of Power
 The nuclear reactor facilities shall be so designed that safe shutdown and proper cooling of the reactor after shutting down can be ensured in case of a short-term total AC power loss.

Guideline 48. Electrical Systems
 (1) The electrical systems shall be designed to allow the structures, systems and components with safety functions of especially high importance to be fed by either of off-site power and emergency on-site power when they need electric power to fulfill their safety functions.
 (2) The off-site power system shall be connected to the electric power system with two or more power transmission lines.
 (3) The emergency on-site power system shall incorporate redundancy or diversity and independence and have enough capacity and capability to accomplish the following properly even with an assumption of a single failure of its components.
 1) Shutting down and cooling the reactor without the acceptable fuel design limits and design conditions for the reactor coolant pressure boundary being exceeded in case of anticipated operational occurrences.
 2) Cooling the reactor core and ensuring the integrity of the reactor containment and safety functions of other necessary systems and components in case of an accident, such as loss of reactor coolant.
 (4) The electrical systems associated with safety functions of high importance shall be designed such that their important portions can be tested and inspected on a periodical basis.

© 2013 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved.

4

Details about the Regulatory Requirements



➤ After Fukushima Daiichi Accident

Regulation on the Technical Standards for Commercial Nuclear Power Reactors and Associated Facilities

Interpretation of the Regulation on the Technical Standards for Commercial Nuclear Power Reactors and Associated Facilities


Article 72 (Electric power supply system)
 A nuclear power reactor facility shall be provided with the necessary systems/equipment to ensure electric power required for preventing significant damages to the reactor core, failure of reactor containment, significant damages to fuel assemblies in the spent fuel pool and significant damages to the fuel assemblies in the reactor in shutdown state (hereinafter referred to as "fuel assemblies within shutdown reactor"), when a serious accident occurs due to loss of power supply for systems/equipment to cope with design basis accidents.

Article 72 (Electric power supply system)
 1. The "necessary systems/equipment to ensure electric power required" in the Clause 1 mean the systems/equipment provided for the purpose of the following measures or any other measures with same or better effectiveness:
 a. Installation of alternative power supply systems/equipment
 i. Deployment of transportable alternative power supply systems/equipment (e.g. power supply vehicle and batteries)
 ii. Installation of alternate current power supply system as a permanently-installed alternative power supply system
 iii. The above systems/equipment should be independent of and spatially separated from the systems/equipment to cope with design basis accidents.
 b. The permanently-installed direct current power supply system with batteries should supply electric power for 8 hours without switching off the loads. "Without switching off the loads" does not include the cases where the loads can be easily switched off in the reactor control room or adjacent rooms such as electric rooms. After 8 hours, the system should supply electric power for subsequent 16 hours (i.e. 24 hours in total) with switching off the loads not required for safety purpose.
 c. Such transportable direct current power supply system/equipment should be provided that can supply electric power (direct current) for 24 hours to the systems/equipment required for the response to serious accidents.
 d. In the case of multiple unit plants, necessary cables should be laid in advance to allow electric power interchange among the units by manual connection.
 e. Loss of functions of station electric equipment (e.g. motor control centers (MCCs), power centers (PICs) and metal clad switchgears (MCSs)) due to common causes should be avoided by, for example, providing alternative station electric equipment, and at least one train should maintain its function and allow access of personnel.

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved.

5

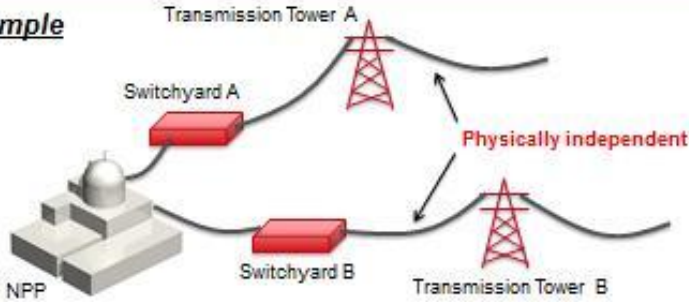
3. Design Improvement on the Electrical Power Systems



3.1 Offsite Power System


Before Fukushima Daiichi Accident	After Fukushima Daiichi Accident
<ul style="list-style-type: none"> ✓ Connection to a power grid via two or more power transmission lines 	<ul style="list-style-type: none"> ✓ Connection to a power grid via two or more independent power transmission lines ✓ Increase a seismic capacity of equipment/structures associated with offsite power system

Typical example



© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved. 6

3. Design Improvement on the Electrical Power Systems (Continued)

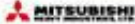


3.2 Emergency Power Source

Before Fukushima Daiichi Accident	After Fukushima Daiichi Accident
<ul style="list-style-type: none"> ✓ Capacity of fuel tank : 2 to 7 days (Determined for each plant by considering the time needed to transport the fuel from outside the plant for replenishment.) 	<ul style="list-style-type: none"> ✓ Capacity of fuel tank : at least 7 days

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved. 7

3. Design Improvement on the Electrical Power Systems (Continued)



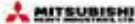
3.3 Safety-related Battery

Before Fukushima Daiichi Accident	After Fukushima Daiichi Accident
✓ Discharge Duration : 2 hours	✓ Discharge Duration : 8 hours (without load shedding) Subsequent 16 hours (with load shedding)

Typical example

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved. 8

3. Design Improvement on the Electrical Power Systems (Continued)



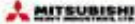
3.4 Alternative Power Supply Systems/Equipment

Before Fukushima Daiichi Accident	After Fukushima Daiichi Accident
✓ N/A	✓ Installation of Permanent AAC ✓ Deployment of transportable AAC (e.g. power supply vehicle)

Typical example

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved. 9

3. Design Improvement on the Electrical Power Systems (Continued)



3.5 Loss of Normal Access to the UHS (LUHS)

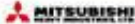
Before Fukushima Daiichi Accident	After Fukushima Daiichi Accident
✓ N/A	✓ Installation of power sources which do not rely on UHS

Install power sources which do not rely on UHS (e.g. gas turbine generator, air-cooled diesel generator) so that they can supply power to the required loads even if LUHS occurs due to external events such as tsunami.

Applying this type of power source for AAC can provide diversity between AAC and EPS (water-cooled), increasing the reliability of the power supply systems.

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved. 10


3. Design Improvement on the Electrical Power Systems (Continued)



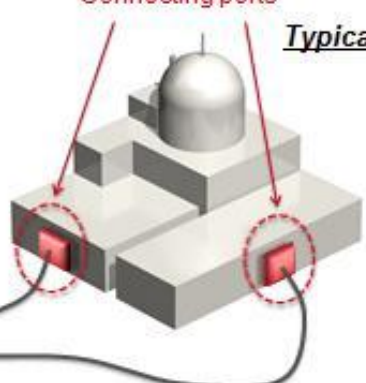
3.6 Connection with Transportable AAC

Before Fukushima Daiichi Accident	After Fukushima Daiichi Accident
✓ N/A	<ul style="list-style-type: none"> ✓ Providing multiple connecting ports ✓ Installation of each connecting port in a different place

Provide connecting ports in different places to prevent failure to connect with the transportable AAC due to common cause failure.



Transportable AAC



Connecting ports

Typical example

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved. 11

3. Design Improvement on the Electrical Power Systems (Continued)

3.7 Extreme External Hazard

Before Fukushima Daiichi Accident	After Fukushima Daiichi Accident
<ul style="list-style-type: none"> ✓ Plant Design to ensure that safety is not impaired by assumed natural phenomena(*). <p>(*) earthquake, tsunami, flood, freeze, etc.</p>	<ul style="list-style-type: none"> ✓ Enhancement of the protective capability against Extreme External Hazard

Typical example

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved. 12

3. Design Improvement on the Electrical Power Systems (Continued)

3.8 Terrorism/Airplane Crash

Before Fukushima Daiichi Accident	After Fukushima Daiichi Accident
<ul style="list-style-type: none"> ✓ Protection of the safety function in the Reactor Building 	<ul style="list-style-type: none"> ✓ Establishment of an independent facility outside the Reactor Building dedicated to coping with loss of entire safety function in Reactor Building ✓ Provision of equipment necessary to prevent damage to the containment vessel

Typical example

© 2014 MITSUBISHI HEAVY INDUSTRIES, LTD. All Rights Reserved. 13

4. Conclusion



- ✓ Since the Fukushima Daiichi accident, the regulatory requirements had been reviewed in light of the lessons learned from the accident.
- ✓ The new regulatory standards have included several important enhancements to electrical design.
 - Improvement of reliability of the Offsite Power System
 - Increase of the safety-related battery discharge duration
 - Increase of the fuel tank capacity for emergency power source
 - Installation of AAC system
 - Enhancement of the external hazards protection
 - Enhancement of the man-induced external hazard protection
- ✓ To enhance safety of the electrical system of the Japanese PWR plants, some of the above requirements have been incorporated to their electrical design and some are under consideration.

Effects of Common Cause Failure on Electrical Systems

Eur Ing Kevin Pepper B.Eng (Hons) C.Eng MIET

Electrical Inspector, Office for Nuclear Regulation, United Kingdom

Abstract

The essential electrical systems of reactor designs have developed progressively with an increased focus on the use of redundant, segregated and independent safety system equipment ‘trains’. In this arrangement, essential safety functions associated with safe shutdown and cooling of the reactor are replicated on near identical electrical systems with each of the trains of safety system equipment supported by a fully rated standby generator.

Development in designs has seen the number of trains increased to enable maintenance to be undertaken with reactors at power, improving the economics of the units whilst maintaining nuclear safety.

This paper provides a background to common cause failure and provides examples where supporting guidance and international experience is available. It also highlights the regulatory guidance available to UK licensees.

Recent examples of common cause failures on plant in the UK are presented together with an issue identified during the recent Generic Design Assessment review of new reactor designs within the UK. It was identified that one design was claiming a very low probability of failure associated with the loss of a single break and no-break voltage level, orders of magnitude below the target figure within ONR’s Safety Assessment Principles. On closer scrutiny it was established that a significant safety function provided from identical low voltage switchboards would be lost in the event of a common cause failure affecting these boards.

The paper will explain the action that has been taken by the requesting party to improve the resilience of the design and how this impacts on the ONR reliability targets for reactor designs within the UK.

1. Introduction

The events at Fukushima Daiichi in March 2011 are classic examples of Common Cause Failure. Seismic and flooding events have long been recognised as a significant risk to electrical systems used to support safe shutdown and post-trip cooling of nuclear power plants. On this occasion, the effect was the inability to provide electrical power from either any of the off-site supplies or the on-site generators. This paper will remind the reader of what constitutes common cause failure and why it is more encompassing than the more widely used term common mode failure. It will provide background on the information that is available to support UK licensees and describe some recent events in the UK which have challenged the resilience of the common cause failure arrangements.

2. Guidance

The International Atomic Energy Agency (IAEA) provides the following useful definition of Common Cause Failure (CCF)¹:

Failure of two or more structures, systems or components due to a single specific event or cause. For example, a design deficiency, a manufacturing deficiency, operation and maintenance errors, a natural phenomenon, a man-induced event, saturation of signals, or an unintended cascading effect from any other operation or failure within the plant or a change in ambient conditions.

Common mode failure is defined by the IAEA as:

Failure of two or more structures, systems or components in the same manner or mode due to a single event or cause. i.e. common mode failure is a type of common cause failure in which the structures, systems or components fail in the same way.

Requirement 24 of IAEA Specific Safety Requirement SSR-2/1² states that the “design of equipment shall take due account of the potential for common cause failures”. There are also numerous guidelines for the analysis of CCF for probabilistic safety assessment³ and protecting digital I&C systems⁴. This definition highlights that common mode failure is in effect considered to be a subset of common cause failure that considers the failing occurring through the same mechanism.

In the UK, the Office for Nuclear Regulation (ONR) provides guidance within a section of its Safety Assessment Principles⁵ (SAPs) entitled “Design for Reliability”. This section gives expectations on the level of robustness that we expect for systems, considering both common cause failure and the single failure criterion, providing specific principles that are expected to be targetted. The section states:

The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of common cause failure. Examples of diversity are different operating conditions, different working principles or different design teams, different sizes of equipment, different manufacturers, different

1. “IAEA Safety Glossary”, IAEA, 2007

2. “Safety of Nuclear Power Plants: Design”, Specific Safety Requirement SSR-2/1, IAEA, 2012

3. “Procedures for conducting common cause failure analysis in probabilistic safety assessment”, IAEA-TECDOC-648, IAEA, 1992

4. “Protecting against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants”, NP-T-1.5, IAEA, 2009

5. “Safety Assessment Principles for Nuclear Facilities”, Office for Nuclear Regulation, 2006 Revision 1

components, and types of equipment that use different physical methods. The design should also be tolerant of random failure occurring anywhere within the safety systems provided to secure each safety function.

One specific principle, EDR.3, states:

Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.

In the supporting paragraphs, it advises that CCF claims should be substantiated, with claims for CCF no better than one failure per 100 000 demands, or equivalence for a continuously acting system. This figure is based on a judgement by ONR of the best limit that could reasonably be supported for a simple system using currently available data and methods of analysis. It is indicated that a worse figure may need to be used, of say 1 per 10 000 or 1 per 1000, according to the complexity and novelty of the system, the nature of threat and the capability of the equipment. It also concedes that the continuing accumulation of good data and advances in analysis could lead, in exceptional circumstances, to a situation where a strong case could be made by the duty holder for better figures. In final advice, the SAPs indicate that where required reliabilities cannot be achieved due to CCF considerations, the required safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.

3. International Activity

In terms of the statistics and high level event causes of CCF, there are a number of useful sources to add a world context to CCF. Below are just some examples. The Organisation for Economic Co-operation and Development (OECD)/Nuclear Energy Agency (NEA) through the International Common-Cause Data Exchange (ICDE) project has sought to:

- collect and analyse CCF events over the long term so as to better understand such events, their causes, and their prevention;
- generate qualitative insights into the root causes of CCF events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences;
- establish a mechanism for the efficient feedback of experience gained in connection with CCF phenomena, including the development of defences against their occurrence, such as indicators for risk based inspections;
- generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries; and
- use the ICDE data to estimate CCF parameters.

To date this has considered diesel generators, motor-operated valves, batteries, control rod drives and circuit breakers. The Nuclear Regulatory Commission (NRC) has collated and analysed CCF events from

the United States of America in the Common Cause Failure Database, coding and classifying events. As part of this, NRC have selected the following specific topics; Emergency Diesel Generators, Motor-Operated Valves Pumps and Circuit Breakers.

Additional events can be extracted from the joint IAEA/NEA Incident Reporting System (IRS) database.

4 Recent Experience in the United Kingdom

From the international definitions, UK guidance and research undertaken by the OECD amongst others, the issue of common cause failure is something widely recognised. And whilst it is considered that the big issues have largely been identified and addressed on legacy plant, it is recognised that this is not an issue that has been completely designed out of existing plant. The following are some recent examples from the United Kingdom.

At one site, the emergency generators are located in a single building with internal barriers to provide fire segregation. A single fire fighting distribution system feeds a fixed jet system for each generator. During routine testing of the system for one generator, the flow was detected as a transient by the flow switches of two of the systems which protect the remaining generators. Since these generator control systems considered their respective fire fighting systems had operated, they inhibited the ability to start them. The problem was immediately detected through alarms in the control room. Once the cause had been identified and confirmation made that the fire system had not actually operated, the generators were started and synchronised to demonstrate the availability of all the site generators. In this event, two generators remained available at all times, which is the minimum declarable condition in the safety case, and it should also be recognised that additional levels of electrical generators and diesel driven feed pumps remained available. But this event serves as a reminder as to how a single event can render multiple plant unavailable, even if for a short period. The system has since been modified by the licensee to prevent a reoccurrence.

A similar event occurred at another site with a similar arrangement of multiple gas turbines in a single building. During a post-maintenance test run of a gas turbine, the fixed jet fire system operated. Due to the time taken to isolate the discharge, flooding was caused to the building drawing water into the air duct of the running GT alternator. As a result of the flooding, the availability of the remaining three GTs was challenged requiring a controlled shutdown.

It should be noted that in each of above, whilst a complete line of defence could have potentially been lost, safe shutdown and cooling of the reactors would still have been assured by other systems on-site which were not affected.

However, these issues are not just confined to legacy systems. A deterministic sensitivity study undertaken during the recent GDA process of the UK EPR identified potentially severe consequences to the plant from the postulated loss of the 690V emergency supply or 400V uninterruptible supply. As a result of the sensitivity study, a detailed approach was adopted by the requesting party for the initiating events of loss of 690V switchboards and loss of 400V switchboards based on:

- Identification of SSC/Safety Functions used in normal operation and impacted by the initiating event
- Presentation of proposed design modifications to cope with the fault

- Identification of required and available mitigation safety features/SSCs
- Proposed mitigation strategy taking into account the proposed design changes
- The detailed assessment determined design changes which included changing the operating voltage of some 690V equipment to 400V
- design change to modify some key plant actuators to operate from the 220V DC system

In both cases, this would provide a diverse source of supply for key safety functions. Even with the above modifications, the claimed failure frequency of the remaining loads on the 400V uninterruptible power supply is 7.8×10^{-7} per year. SAP EDR 3, discussed above, places a limit on any single technology of 1×10^{-5} per year unless a strong case can be by the duty holder for better figures. Due consideration has been given within ONR as to whether an acceptable case could be made. We determined that subject to any Licensee meeting the following, the case was acceptable:

- The detailed design of the main switchboards, cables and supporting technology demonstrates that the system is simple and very robust.
- An ALARP analysis is undertaken by the Licensee at an early stage of detailed design to judge whether it is reasonably practicable to provide a diverse manufacturer of equipment for two out of the four trains.
- The detailed design analysis should show that sustained damage to the downstream switchboards from a major failure of the invertors which renders them unable to function can be ruled out deterministically.
- Through life support is at a level commensurate with the very high integrity required of the system.

This work is still ongoing by the licensee of the first proposed UK EPR at Hinkley Point C to close out this aspect.

Summary

Common Cause Failure is something that has been recognised for many years and designed out of many legacy systems through diversity, segregation and separation. This paper has shown that Guidance is available both from the IAEA, as well as national regulatory bodies. Information on CCF in relation to specific equipment types is available from a number of organisations such as OECD or NRC. However, we must never be complacent. There will still be plant safety systems out there which is not resilient against CCF – whether due to changes in the nature of a hazardous event, the way in which the equipment is operated or maintained, or in the design. With the increased reliance on electrical systems to support C&I systems in shutdown and post-trip cooling, it is important that new reactor designs are given the depth of analysis appropriate to ensure resilience against CCFs.

Effects of Common Cause Failure on Electrical Systems

Eur Ing Kevin Pepper B.Eng (Hons) CEng MIET
ONR Inspector - Safety

Common Cause Failure

- What is it?
- Common Cause vs. Common Mode
- UK Regulatory Guidance
- Examples from the UK

What is it?

Failure of two or more structures, systems or components due to a single specific event or cause.

For example, a design deficiency, a manufacturing deficiency, operation and maintenance errors, a natural phenomenon, a man-induced event, saturation of signals, or an unintended cascading effect from any other operation or failure within the plant or a change in ambient conditions.

IAEA Glossary Definition

International Operational Experience

- Fukushima Daiichi
 - Inability to provide electrical power from either:
 - Offsite supplies
 - Onsite supplies
 - Loss of multiple generators
 - Loss of multiple switchboards

Common Cause vs. Common mode

- In the UK, we use the term Common Cause not Common Mode
- Reason being Common Cause bounds Common Mode failures
- IAEA Glossary Definition – Common Mode

*Failure of two or more structures, systems or components **in the same manner or mode** due to a single event or cause. i.e. common mode failure is a type of common cause failure in which the structures, systems or components fail in the same way.*

UK Regulatory Guidance

- ONR “Safety Assessment Principles”
 - Design of Reliability
 - *The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of common cause failure. Examples of diversity are different operating conditions, different working principles or different design teams, different sizes of equipment, different manufacturers, different components, and types of equipment that use different physical methods. The design should also be tolerant of random failure occurring anywhere within the safety systems provided to secure each safety function.*

SAP Principle EDR.3

- *Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.*
- Where required reliabilities cannot be achieved due to CCF considerations, the required safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures
- This is further clarified by the following paragraphs in the text that places limits which are generally between 1.0×10^{-5} – 1.0×10^{-3} /yr for continuously acting safety Class 1 support systems.



ONR Safety assessment guide on safety systems

ONR's Guidance on Safety Systems (T/AST/003) sets expectations for the common cause failure analyses of all nuclear safety support systems such as electrical systems.

Considering electrical systems, we separate CCF of diesel generators from CCF of Switchboards. Both need to be analysed but switchboard failures are often more severe and can be bounding.

Classification based on ONR [SAP ECS.2](#)

System Class	Failure Frequency/yr (<i>ff</i>)
Class 1	$10^{-3}/\text{yr} \geq ff \geq 10^{-6}/\text{y}$
Class 2	$10^{-2}/\text{yr} \geq ff > 10^{-3}/\text{y}$
Class 3	$10^{-1}/\text{yr} \geq ff > 10^{-2}/\text{y}$



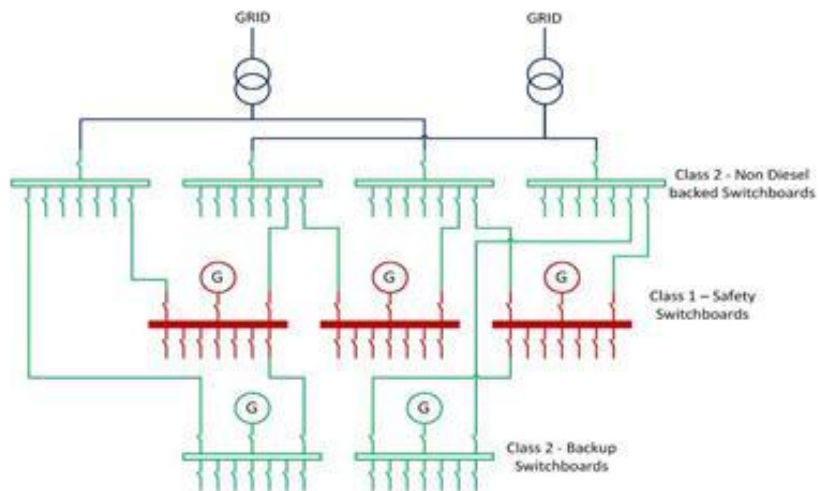
Approach to analysing CCF

- The table in the previous slide means that deterministically the following applies:
 - As the diesel generators are demand based their CCF is analysed in conjunction with an initiating event such as loss of offsite power
 - The switchboards are generally in operation at all times and therefore their CCF, based on common voltage levels distributed by redundant divisional switchboards, is an infrequent design basis event for Class 1 and frequent design basis event for Class 2.
- There is a difference in that the CCF of the EDGs is a demand based failure in response to a loss of offsite power **whereas the switchboard failure is assumed to occur suddenly.**
- The analyses of spurious switchboard CCF should cover a 72 hour period

Switchboard Failures

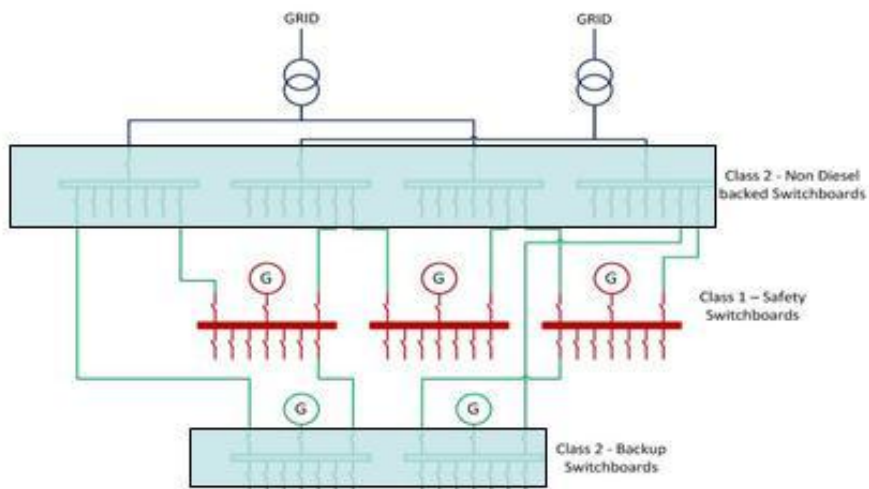
- Wherever there is common switchboard technology at the same voltage level then:
 - Class 1 switchboards must be analysed for infrequent design basis events.
 - Class 2 and 3 switchboards for frequent design basis events.

Example - Before



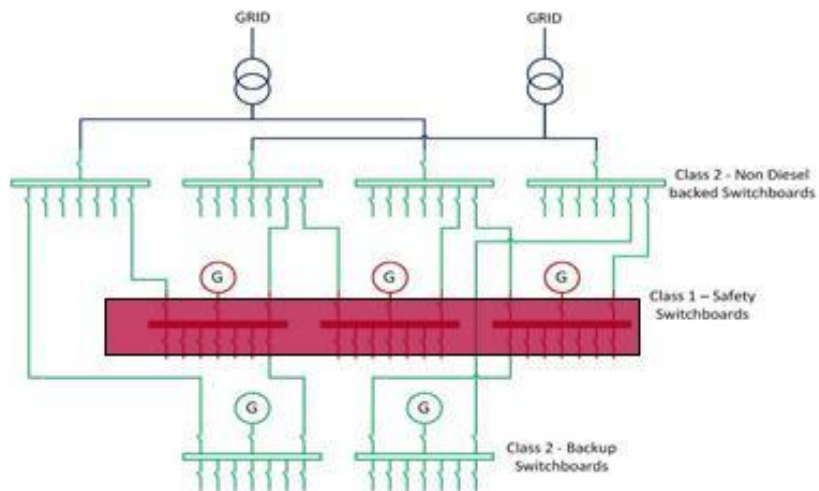
 Office for Nuclear Regulation

Example - Class 2 CCF



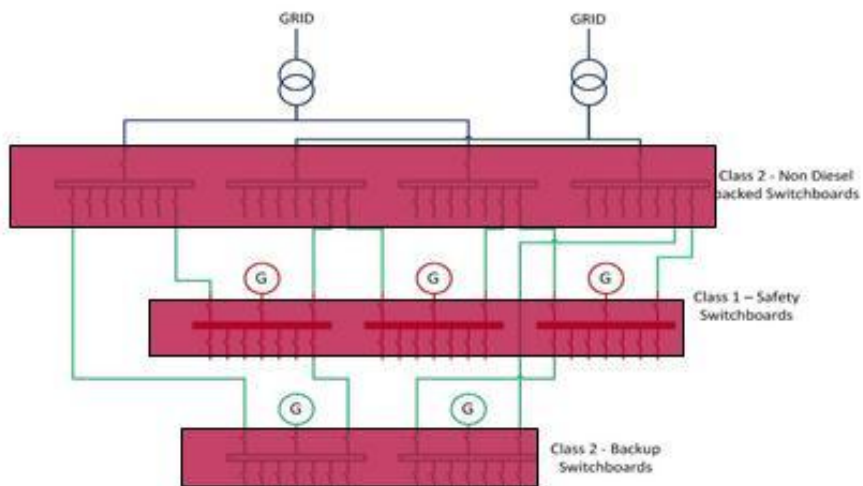
 Office for Nuclear Regulation

Example – Class 1 CCF

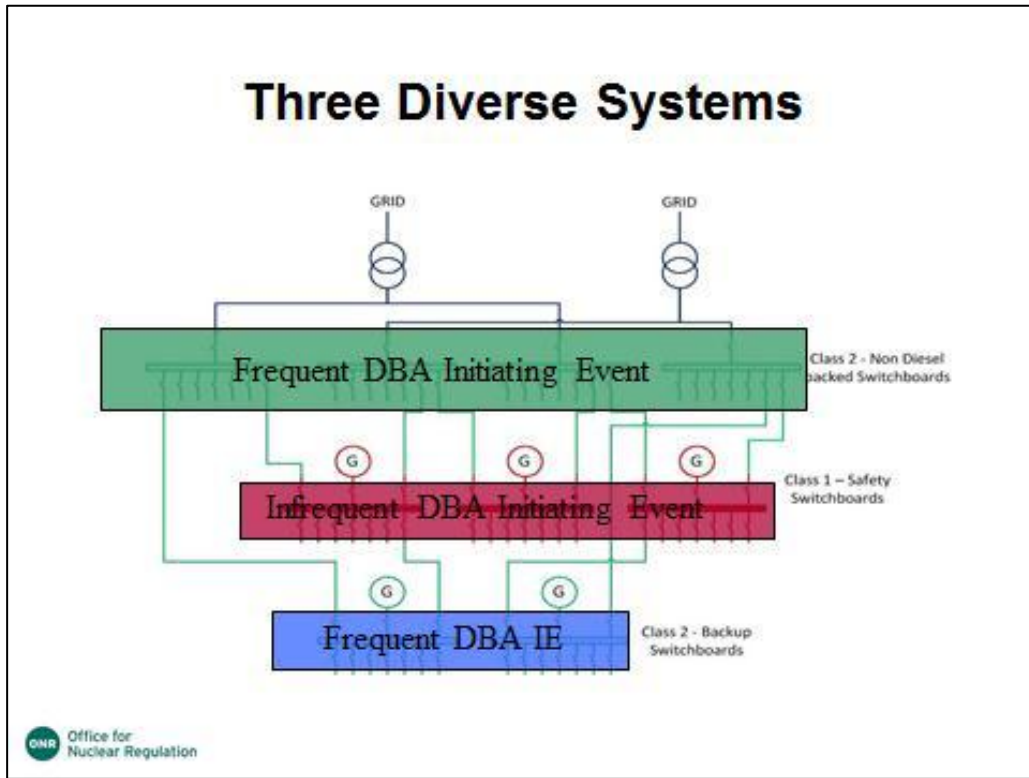


 Office for Nuclear Regulation

No Diversity – Complete Failure for an Infrequent Fault



 Office for Nuclear Regulation



- ### Recent UK Experience
- Failures of fire fighting systems leading to multiple unavailability of essential generators through
 - Inhibiting of control systems
 - Flooding of generator building
 - In all cases
 - complete failure was prevented
 - Additional diverse cooling systems remained available
- Office for Nuclear Regulation

Recent Generic Design Assessment Experience

- Deterministic study identified loss of 690V emergency or 400V uninterruptible system could lead to potentially severe consequences
- Detailed review by Requesting Party:
 - Identification of SSC/Safety Functions
 - Proposed design modifications
 - Identification of required and available mitigation SSC/Safety Functions
 - Relocation of certain SSCs to alternative voltage supplies (690V -> 400V ; 400V -> 220Vdc)

Recent Generic Design Assessment Experience

- Claimed failure frequency (7.8×10^{-7}) still lower than SAP guidance (1×10^{-5})
- ONR determined the case was acceptable based on:
 - Detailed design demonstrating design of system is simple and very robust
 - ALARP analysis to consider use of diverse manufacturer for two out of the four trains
 - Detailed analysis to show that failure of inverters cannot result in sustained damage to switchboards
 - Through life support is commensurate to the very high integrity required.

Conclusion

- Common Cause Failure is something recognised across the industry as something to be considered
- Significant improvements have been made over the years in respect of newer design and retrofits
- Must never be complacent
- With increased focus on electrical and C&I systems to support reactor shutdown and post-trip cooling, it is important that new reactor designs are given the appropriate depth of analysis against CCFs.

Any Questions?

Email : Kevin.Pepper@onr.gsi.gov.uk

A Survey of the Hazards to Electrical Power Systems

Gary Johnson

Independent Consultant, USA

Abstract

This paper presents the preliminary results of a survey of severe accidents and the lessons learned that are important to the design of electrical power systems. This survey of historical accidents since 1952 identified 19 known incidents in which significant fuel melt occurred within a reactor core. In each of these incidents unexpected events or event sequences played an important role. In all cases the event sequences resulted in bypass of two or more levels of defense in depth.

This study offers clear lessons for electrical power robustness: 1) Robust design must be based upon a clear understanding of what can go wrong, and 2) Robust design will reduce, but cannot eliminate, the potential for failure of electrical power systems.

In order to better understand “what is the worst that can happen” known hazards are reviewed to identify the challenges that they can present to electrical power systems.

Recognizing that unexpected events cannot always be prevented the paper discusses the need for methods to restore plant power sources or provide for alternate power supplies when the plant power sources fail.

1. Lessons learned from historical severe accidents

A literature review identified 19 severe accidents since criticality of the first man-made nuclear reactor on December 2, 1942. These events occurred in very diverse reactor types. A report on these events is expected in early 2015.

Many of the events happened before modern safety regulations and expression of safety culture. All plants included defense in depth features, but most were designed before defense in depth principles¹ were formally expressed. At some plants national security benefits took priority over design safety.

All of these accidents resulted from events that were either unforeseen or discounted as incredible. Consequently provisions to prevent and to mitigate the effects of the events were inadequate, multiple layers of defense failed and operators did not have the knowledge, training or procedures for response.

¹. International Nuclear Safety Advisory Group-10, “Defense in Depth in Nuclear Safety,” INSAG-10,” International Atomic Energy Agency, 1996.

In short, severe accidents result from limits to our knowledge, i.e., “unknown-unknowns” - things that we cannot imagine, and “known-unknowns” - things that we can imagine, but cannot accurately predict their probability or effects. The more formal expression for these limits to knowledge is “epistemic uncertainty.” Robust design must account for epistemic uncertainties.

The health and environmental effects of severe accidents have been lower than those resulting from accidents or normal operation of other modes of energy generation². The following discussion considers three types of effects: prompt fatalities, delayed health effects, and interference with the enjoyment of property outside of the plant premises.

Prompt fatalities

Two events, SL-1 in 1961, and Chernobyl in 1986 caused fatalities from the direct effects of radiation exposure or from other causes during the emergency response at the plant site. At both SL-1 and Chernobyl national security benefits took priority over design safety.

Three died in 1961 at SL-1, a US transportable power reactor.

At Chernobyl 28 deaths were attributed to acute radiation exposure. Another 19 highly exposed survivors died in the next few years³. Some of these deaths were not due to radiation exposure. There were no cases of acute radiation exposure to members of the public.

Chernobyl seems to bound the worse radiation environment that can result from a reactor accident. It shows that early estimates of the prompt fatalities among the general public were exceedingly conservative. By comparison Wikipedia recognizes 430 prompt worker fatalities and 100,681 prompt public fatalities from other forms of energy production since 1965. The event that created the largest number of fatalities was the 1975 collapse of a hydropower dam in China, which killed 100,000.

Delayed health effects

Three events, Windscale, Chernobyl and Fukushima have caused, or will still cause, delayed health effects or fatalities. Epistemic uncertainties regarding health effects of low levels of radiation exposure, and confounding effects of other possible causes make estimates of these effects controversial.

A 1988 report on the Windscale⁴ event estimated an upper bound for public health effects of 100 fatal cancers, 90 non-fatal cancers, and 10 heredity effects. The author went on to state that the actual numbers are likely to be lower and may be zero.

For Chernobyl the main harmful radiation exposure to the public was increased thyroid cancer rates in people who were children or adolescents at the time. Twenty years after the accident 6000 thyroid cancers, 15 of which were fatal, were observed in these groups³. A substantial fraction of these cancers probably resulted from the lack of prompt action to prevent ingestion of milk contaminated by ¹³¹I.

². Caution. The analysis behind the following discussion was not very rigorous, but it is thought that a more rigorous analysis would more fully support the conclusions. A more rigorous analysis would be very interesting.

³. “Sources and Effects of Ionizing Radiation, Volume II,” United Nations Scientific Committee on the Effects of Atomic Radiation, 2011.

⁴. Clarke, R., “The 1957 Windscale Accident Revisited,” paper presented at the REAC/TS International Conference on the Medical Basis for Radiation Accident Preparedness, Oak Ridge, 1988.

It will be many years before such information is available for the Fukushima accident, but based upon the lower level of release and the more aggressive prevention and mitigation of radioactive iodine intake, the Fukushima event will result in substantially fewer thyroid cancers than occurred at Chernobyl.

By comparison recent studies⁵ estimate nuclear power has prevented 1.84 million air-pollution related deaths that would have occurred if the nuclear energy had been produced instead using coal or gas.

Interference with the enjoyment of property outside of the plant premises

Two events, Chernobyl and Fukushima resulted in long-term evacuation of a sizeable area. At Chernobyl approximately 130,000 people were relocated and a 2600-km² exclusion area was established. For Fukushima the numbers are about 90,000 people and 300-km². By comparison the tsunami alone destroyed about 45,000 structures and is responsible for 200,000 people now living in evacuation shelters. Another comparison can be made with the Three Gorges Dam that caused relocation of 1.2 million and it impounds an area of 1045-km².

Severe accidents contributes little to energy risks, so it seems reasonable that improving electric power robustness may be an “as low as reasonably achievable” (ALARA) effort.

Severe accidents also have economic consequences. All of the severe accidents have resulted in significant recovery and restoration costs. Plant replacement and cleanup costs at Fukushima may be in the range of 100 to 300 billion US\$. To utility CEOs a new nuclear power plant must look like a “you bet your company” proposition. We must give buyers and operators confidence that this is not the case. Consideration of the economic effects may justify more robustness measures than consideration of health and environmental effects alone.

2. Reliability, defense in depth, and diversity in electrical power systems

Electrical power systems in today’s nuclear power plants are designed for extremely high reliability and incorporate defense in depth strategies. Most of these systems were produced using management systems that provided for design bases that are informed by plant safety analyses. The designs foster high reliability and tolerance of failure; and provide redundant and diverse power sources and distribution so that nearly every load can be supplied by two or more sources and via several paths.

IAEA DS 430⁶ describes these strategies. These design strategies have served the nuclear industry well. Nevertheless, events such as the 25 July 2006 Forsmark incident⁷ and the Fukushima Daiichi accident show that we cannot envision all events that may defeat these measures.

The concern is hazards that might cause common cause failure (CCF) of redundant or diverse supplies making critical loads inoperable. Loss of all DC power would be the most severe event as most plants can be brought to a controlled state for some time if DC is available. Also, without DC power many electrical

⁵. Kharecha, P. and Hansen, J., “Prevented Mortality and Greenhouse Gas Emissions from Historical and Projected Nuclear Power,” *Environmental Science and Technology*, 47, p. 4889-4895, 2013.

⁶. DS-430, “Design of Electrical Power Systems for Nuclear Power Plants,” International Atomic Energy Commission, in publication.

⁷. NEA/CSNI/R(2009)10, “Defense in Depth of Electrical Systems and Grid Interaction,” Nuclear Energy Agency, 2009.

switchgear and standby AC power sources may be inoperable. Normal and emergency supplies should also be robust with the highest attention paid to standby AC supplies and distribution.

Much attention has been given to emergency power sources, but the distribution systems are more important. Batteries or generators might be available or brought in fairly rapidly; distribution systems cannot so easily be replaced. Repair is time consuming and the events that caused failure of distribution may prevent repair or impede the installation of temporary cabling, protective devices, and motor controls.

Further improvement of electrical power systems robustness will come from better understanding of and better means to cope with the epistemic uncertainties concerning the hazards to electrical systems.

3. Hazards to electrical power systems

Hazards to electrical power systems can be categorized as:

- Internal Hazards: hazards that originate within the site boundary;
- External Hazards: hazards that originate outside of the site boundary; and
- Human Hazards: Hazards created by design mistakes, operational mistakes, or malicious acts.

Internal Hazards

IAEA Safety Guides NS-G-1.7⁸, and NS-G-1.11⁹ describe the recognized internal hazards and discuss means for preventing hazard events and mitigating their consequences. Table 1 summarizes internal hazards and the typical means for preventing CCF. These means are identified as:

- Location: Location of electrical equipment and cable away from hazards,
- Separation: Physical separation and electrical isolation of redundant equipment and cable,
- Barriers: Local barriers that protect equipment and cable from the hazard,
- Coordination: Protective device coordination,
- Qualification: Qualification of equipment and cable for the hazardous environment,
- Fire protection: Provision for suppression of and protection against fire,
- Drains: Provisions to prevent accumulation of water in electrical equipment.

Internal hazards result from design features. Designers try to minimize hazards but cannot eliminate them all. Epistemic uncertainties for internal hazards are low because they are man-made. The greatest uncertainties may concern the efficacy of the existing preventative and mitigative measures.

Following the Browns Ferry fire, existing cable and equipment separation criteria were questioned. Before Browns Ferry separation distances of a few feet were assumed sufficient to prevent CCF in a fire. Afterwards it was assumed that everything within a given fire area could be destroyed unless it was specifically protected. The US industry performed analyses to confirm that plants could be brought to, and maintained in a controlled state, if all equipment and cables in any fire area were destroyed. These analyses were called “safe shutdown analyses.” The robustness of electrical systems in plant fires depends upon such analyses. It also depends upon continued maintenance to ensure that the assumptions of the

⁸. NS-G-1.7, “Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants,” International Atomic Energy Commission, 2004.

⁹. NS-G-1.11, “Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants,” International Atomic Energy Commission, 2004.

analysis remain valid, e.g., that fire barriers including doors, dampers, and penetration seals remain effective. It is incumbent upon plant electrical staff to be aware of the maintenance of such items.

Safe shutdown analysis should be maintained and extended to cover other hazards, such as flooding and structural collapse, that affect large local areas.

Protective device coordination contributes to protection against every internal and external hazard. Coordination studies should be documented and maintained for the life of the plant.

External Hazards

IAEA Safety Guides NS-G-1.5¹⁰, and NS-G-1.6¹¹ describe the recognized external hazards and discuss means for preventing hazard events and mitigating their consequences. Table 2 summarizes the external hazards and the typical means for preventing CCF. These means are identified as:

- Location: Location of electrical equipment and cable away from hazards;
- Separation: Physical separation and electrical isolation of redundant equipment and cable;
- Barriers: Local barriers (including structures) that protect equipment and cable from the hazard;
- Coordination: Protective device coordination;
- Qualification: Qualification of equipment and cable for the hazardous environment;
- Fire protection: Plans, facilities, and staff for fighting external fires;
- Electrical protection: Protective devices, grounding, surge suppressors, filtering, shielding.

Except for geomagnetic events, the epistemic uncertainty about external hazards is moderate. We have studied these events for decades. Still events that exceed design bases occur nearly every year.

Our knowledge about geomagnetic events is more limited. We have been aware of such events for about 150 years. Our knowledge comes from a relatively short period when we have been able to make measurements and a longer time for which we have anecdotal information about aurora observations or the effects on telegraph communications. Geomagnetic effects have been observed as far south as 8° south latitude. Space weather researchers conclude that we should not be surprised when space weather effects exceed the currently known events¹².

We should understand the epistemic uncertainties in plant external event design bases and the possibilities for more extreme events at each site. Where this identifies undesirable risks, practical means for improving electrical system robustness should be considered, e.g., having both electrical and a driven emergency feedwater pumps, berms around external equipment or improved electromagnetic decoupling.

Some hazards, such as flooding other than tsunamis, volcanism, or geomagnetic storms, may give advance warning. In these cases plans for taking protective measures on warning should exist.

The most troublesome consequences for some events will be indirect. For example, during the Mt. St. Helens eruption, diesel air filters, and structural collapse of buildings containing power system equipment

¹⁰. NS-G-1.5, “External Events Excluding Earthquakes in the Design of Nuclear Power Plants,” International Atomic Energy Commission, 2003.

¹¹. NS-G-1.6, “Seismic Design and Qualification for Nuclear Power Plants,” International Atomic Energy Commission, 2003.

¹². Cliver, E, Svalgaard, L, “The 1859 Solar-Terrestrial Disturbance and the Current Limits of Extreme Space Weather Activity,” *Solar Physics*, 224, p. 407-422.

were among the concerns. Geomagnetic storms might not directly affect plant power systems but could cause long-term loss of offsite power and hamper resupply of fuel for emergency generators.

Human Hazards

Human hazards include Operational Errors, Design Errors and Malicious Acts. IAEA DS-430⁶, DS-431¹³, Security Series 4¹⁴, Security Series 8¹⁵, NSS-13¹⁶, and NSS 17¹⁷ deal with these topics. Table 3 summarizes the human hazards and the typical means for preventing CCF. These means are identified as:

- Human Factors Engineering: Design of operational interfaces and maintenance provisions to reduce the potential for human error,
- Training: Education, and qualification of operations, maintenance, design, and manufacturing personnel for the tasks that they must perform,
- Procedures: Established, documented, verified and validated means for performing operations, maintenance, design, and manufacturing activities,
- Design Standards: Corporate, national, and international standards that convey proven methods for achieving technical and reliability characteristics of electrical systems,
- Access Control & Monitoring: Physical, administrative, and technical measures to inhibit unauthorized physical or electronic access to electrical system equipment and to detect such access if it does occur.
- Secure Development Environments: Design, implementation, and maintenance environments having physical, logical, and programmatic controls to ensure that unwanted, unneeded, and undocumented functionality is not maliciously introduced into digital systems,

Humans may be the largest source of epistemic uncertainty. Fourteen of the accidents considered were initiated by human errors, and in some cases clever or heroic human actions terminated accidents.

NEA/CSNI/R/2009(10)⁷ identified 23 events involving human errors. Most involved missteps during maintenance. The report recommends task analysis for safety-related operations and maintenance activities. This should also include also maintenance activities that could result in CCF within the preferred power supply. Humans are more reliable if they are prepared in advance, have procedures or guidelines, and realistically practice their tasks. Electrical staff involved in implementing SAMG should have this.

Mechanical and relay-based electrical devices are now being replaced with digital components. This raises the question of how to prevent and mitigate CCF resulting from software errors. The I&C community has settled on the use of rigorous design procedures, design transparency, design standards, defense in depth, and diversity. The electrical community should not uncritically accept the I&C approach. Digital devices for electrical systems are different from I&C. For example, many electrical devices perform

¹³. DS-431, "Design of Instrumentation and Control Systems for Nuclear Power Plants," International Atomic Energy Commission, in final review.

¹⁴. International Atomic Energy Commission Nuclear Security Series No. 4, "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage," International Atomic Energy Commission, 2007.

¹⁵. International Atomic Energy Commission Nuclear Safety Series No. 8, "Preventive and Protective Measures against Insider Threats," International Atomic Energy Commission, 2008.

¹⁶. International Atomic Energy Commission Nuclear Security Series No. 13, "Nuclear Security Requirements on Physical Protection of Nuclear Material and Nuclear Facilities," International Atomic Energy Commission, 2011.

¹⁷. International Atomic Energy Commission Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities," International Atomic Energy Commission, 2011.

exactly the same function in both nuclear and commercial applications, perform the same function during normal operation and accident conditions, and are less likely to see untested operational profiles during accident conditions. Such differences may allow the use of a simpler strategy for at least some electrical equipment. The electrical community should work with researchers and regulators to develop a strategy for electrical systems.

Operational errors and design errors are mistakes. Electrical systems must also deal with the possibility of intentional mal-operation of components either directly or through the introduction of malicious code. Digital devices create the risk of cyber attack. That such events can be created has been demonstrated^{18,19} and at least one serious attack on nuclear facility electrical controls has occurred²⁰. Controlling electronic access to plant equipment, engineering development environments and design tools is critical to controlling the risk. The potential consequences of malicious operation of electrical equipment should be understood. If a cyber attack could result in serious plant consequences, use of non-digital devices to prevent or mitigate these consequences should be considered.

¹⁸. Video, “Staged Cyber Attack Reveals Vulnerability in Power Grid,”
<http://www.youtube.com/watch?v=fJyWngDco3g>, retrieved 2014-02-09, CNN.

¹⁹. “What You Need to Know (and Don’t) About the AURORA Vulnerability,” Power Magazine. 2013-09-01

²⁰. Langner, R. “To Kill a Centrifuge, A Technical Analysis of What Stuxnet’s Creators Tried to Achieve,”
<http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>, retrieved 2014-02-09, Langner Group (2013).

Table 1. Summary of Internal Hazards and Protective Measures

Hazard	Vulnerable Electrical Components	Typical means for preventing common cause failure							Comments
		Location	Separation	Barriers	Coordination	Qualification	Fire Protection	Drains	
Missiles	Cables Local panels	x	x	x	x				Mainly containment and turbine building
Collapse of Structures	Any equipment and cables		x		x				Structural failures have occurred in substations. Structural collapse might result from other events
Falling Objects	Any equipment and cables	x	x		x				In areas where heavy objects are lifted
Pipe Whip	Cables Local panels	x	x	x	x				Mainly containment and turbine building
Jet Effects	Cables Local panels	x	x	x	x				Mainly containment and turbine building
Environmental effects of pipe or vessel breaks	Cables Local panels	x	x		x	x			Mainly containment and turbine building
Floods, leaks, and sprays	Any equipment and cables	x	x	x	x	x		x	Consider also the need for enclosure drains to prevent accumulation of moisture over time
Fires and fire effects	Any equipment and cables	x	x		x		x		
Explosions	Any equipment and cables	x	x		x				

Table 2. Summary of External Hazards and Protective Measures

Hazard	Vulnerable Electrical Components	Typical means for preventing common cause failure							Comments
		Location	Separation	Diversity	Coordination	Qualification	Fire Protection	Electrical Protection	
Earthquake	Any equipment				x	x			Even non-safety equipment is designed for some level of seismic, but qualification may be less rigorous
Aircraft Crash	Any Equipment and Cables	x	x		x				
Fires	Any Equipment and Cables	x			x		x		Applies to out door equipment such as unit transformers and substations.
Explosions	Any Equipment and Cables	x	x		x				
Asphyxiant & Toxic Gases	N/A								A bigger threat to operators than equipment. Could be a maintenance issue
Corrosive Gases & Liquids	Any Equipment and Cables	x	x		x				
Electromagnetic Interference	Any Equipment	x	x			x			Both and internal and an external hazard.
Floods	Any Equipment and Cables	x	x		x				
Extreme Winds	Any Equipment and Cables	x		x				x	Included tornados which could affect indoor equipment if not protected

Hazard	Vulnerable Electrical Components	Typical means for preventing common cause failure							Comments
		Location	Separation	Diversity	Coordination	Qualification	Fire Protection	Electrical Protection	
Extreme Meteorological Conditions	Any Equipment and Cables	x		x				x	Applies to outdoor equipment such as unit transformers and substations.
Biological Phenomena	N/A								Mainly an issue with coolant systems in contact with ultimate heat sink.
Volcanism	Standby Generators			x					Filters may be rapidly consumed. Mudflows may affect UHS. Ash fall could result in structural collapse.
Collisions with Floating Bodies	Standby Generators			x					Affects ultimate heat sink.
Geomagnetic Effects	Any Equipment				x			x	
Grid transients	Any Equipment							x	

Table 3. Summary of Human Hazards and Protective Measures

Hazard	Vulnerable Electrical Components	Typical means for preventing common cause failure						Comments
		Human Factors Engineering	Training	Procedures	Design Standards	Access Control & Monitoring	Secure Development Environment	
Operational Errors	Any equipment	x	x	x				
Design Errors	Any equipment and cables		x	x	x			
Malicious Acts	Any equipment and cables		x	x	x	x	x	Threats to hardware are mainly insider threats needing physical access control only

4. Extremely extreme events

It would be foolhardy to believe that we can completely eliminate the possibility of total loss of plant power such as happened at Fukushima-Daiichi.

Plants must be prepared for the worst-case events. Some necessary functions might be accomplished without electrical power, but where it is needed electrical systems should provide power to implement Severe Accident Management Guidelines (SAMG). These power systems should be independent of the plant electrical systems to the extent possible (including independence from the distribution systems) and must be suitable to supply at least the loads needed to support the “last ditch” efforts of the SAMG, including pumps, valves, air compressors, lighting and instrumentation. These goals might be accomplished with very simple portable supplies and battery backup for designated severe accident monitoring instruments.

5. Conclusions

Severe accidents result from unexpected events that were not considered or were discounted in the plant design or operations and that were not sufficiently mitigated by defense in depth measures.

Electrical power systems can be made more robust to such events by understanding the epistemic uncertainties behind design basis requirements and taking action to deal with more extreme events.

Non-nuclear sources present greater risks to humans and the environment than nuclear power. Thus, it is reasonable that improvements to the robustness of nuclear power plants follow an ALARA approach. That being said, the cost of replacement power, plant replacement and cleanup following an accident might justify more extensive measures.

Epistemic uncertainties are low for internal hazards. The main uncertainties may be the continued effectiveness of the preventative measures. Safe-shutdown analyses should be kept up to date and extended to cover other wide area hazards, such as, structural collapse and floods. Also electrical coordination studies should be reviewed and maintained up to date.

Epistemic uncertainties are moderate for most external hazards. We understand the hazards reasonably well, but hidden evidence is still to be uncovered and predictive models continue to improve. Events that exceed external hazard design bases seem to occur every year. Electrical system engineers should be aware of the epistemic uncertainties behind their external event design bases and consider if practical measures can be taken to make the systems more robust.

Humans represent the greatest hazard to plants, including the electrical power systems. Human error contributed to all nineteen severe accidents. Management systems have served us well, but more effort needs to be given to imagine what failures errors might create and how they might be practically addressed.

Electrical systems are beginning to extensively use digital components. This creates new possibilities for CCF. The I&C community has dealt with this issue. The electrical community should consider if the I&C approach or some other approach is appropriate for electrical systems.

The use of digital components raises the potential for cyber attack. Computer security features should be introduced when digital components are installed in power systems. If potential

consequences of cyber attack are unacceptable, hardware measures should be introduced to prevent or mitigate these consequences. Reference 20 is highly recommended reading.

We can never eliminate the occurrence of unimagined events nor can we afford to build for all worst imaginable cases. Plans and equipment must to be in place to deal with such occasions. This should include plans for complete loss of plant AC and DC power. Electrical supplies that are independent of the plant electrical power system should be available to service SAMG loads for “last ditch” scenarios. Plant electrical staff should also be trained for and realistically practice their role in implementing SAMG.

The next generation plants can tolerate loss of all site AC power for days as opposed to hours. These features will improve safety, but we must consider the possibility of more extreme events such as the loss of plant DC power, the failure of plant distribution systems, or longer-term station blackout.

A Survey of Hazards to Electrical Power Systems

Presented to

CSNI International Workshop on Robustness of Electrical
Systems of NPPs in Light of the Fukushima Daiichi Accident

Paris

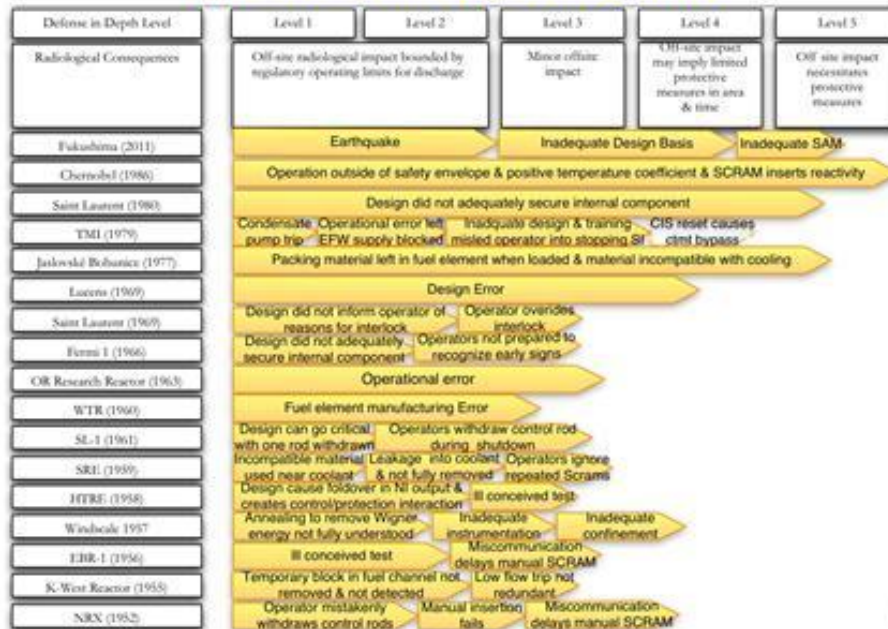
2014 April 1 to 4

Gary Johnson
Independent Consultant
gjohnson@ieee.org

Agenda

- Historical severe accidents & lessons learned
- Survey of hazards
- Priorities
- Uncovered extreme events
- Conclusions

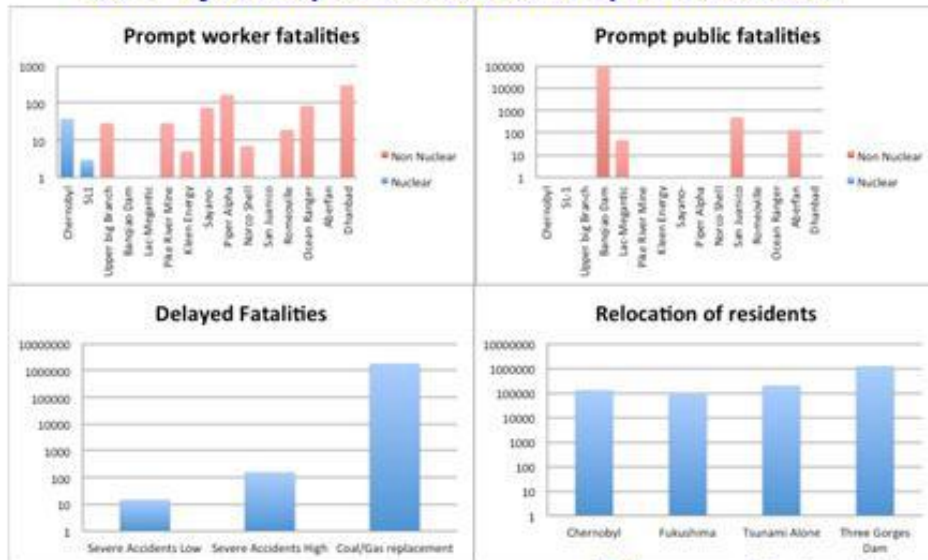
Nineteen severe accidents



Failure of imagination (sometimes) leads to severe accidents

- Severe accidents happen because of limits to our knowledge for which:
 - Plant is not designed to cope,
 - Operators are not prepared to respond, and
 - Multiple levels of defense in depth are often bypassed
- Most were initiated by operational errors, design errors or both
- Design should consider epistemic uncertainties
 - Unexpected events
 - Hazards that may be bigger than design bases
 - Unexpected consequences

Severe accidents are bad, but safety risks don't justify extraordinary measures*



*But economic risks might

What's the worst that can happen to electrical systems?

- Failure of all onsite and offsite power sources
- Failure of distribution systems
- Failure of all DC supplies
- Station blackout
- Consideration of CCF should go beyond safety systems
 - Off site supplies
 - Normal supplies

It is not meant that these should be treated as safety systems, but that CCF vulnerabilities should be identified and means for reducing vulnerabilities ALARA should be applied

Internal Hazards

Are existing protective measures still effective?

Are further practical improvements possible?

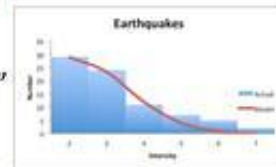
- Epistemic uncertainties about hazards is low
 - Bigger uncertainty: effectiveness of protective measures?
- Potential consequences should be fully studied,
 - E.g., large local events fire, flood, structural collapse
- Safety depends on continued effectiveness of protective & mitigative measures
 - Physical, e.g., fire barriers, dampers, cocoons
 - Analytical, e.g., safe shutdown analyses
 - Electrical, e.g., coordination
- Active maintenance and configuration control is needed

7

External Hazards:

Consider improvements that can deal with fat tails?

- Epistemic uncertainties are mostly moderate
 - Events > design bases are frequent (~1/yr)
- Understand limits and uncertainties
 - Worst consequences, shape of “fat tails”
- Take ALARA measures
 - For slow developing events – plans may be enough
- Uncertainties for geomagnetic events are high
- Keep in mind that effects on electrical power may be indirect
 - E.g., the important threats from volcanoes might be sulfur dioxide concentration in the atmosphere or ashfall



8



Human Hazards

Prepare for the unpredictable

- Humans are the least understood hazard
- All severe accidents involved human error
 - For most, human errors were the initiator
 - Humans also took actions to terminate the accidents
 - Humans are more reliable if they are properly prepared
 - Imagine, plan, educate, train, and practice for the worst
- The DIDELSYS report recommends task analysis for safety system maintenance
 - This should include preferred power supply
- Digital devices creates risks of “software CCF”
 - A prevention and mitigation strategy is needed
 - The I&C strategy might not be right for electrical

10

Malicious acts are also a human hazard

Limit the threat and control the consequences

- So far personnel vetting and physical access control have been effective
- Digital devices create new pathways
 - Via plant networks
 - Via development process
- Introduce cyber security measures when digital devices installed
 - Vendors should have secure development environments
- Understand worst consequences
 - Non-digital measures to protect or mitigate high consequence events.

11

Demonstration of cyber attack

Connecting generator to live bus, out of sync



12

Extremely extreme events

- Some hazards can't be predicted
- Some hazards that can be predicted cannot be reasonably prevented or adequately mitigated
- Remedy is severe accident management
 - SAMG need a path for loss of all plant power
 - Electrical staff need to be trained and practiced for their role
 - Power supplies, independent of plant power systems, should be available to support these paths.
 - These might be relatively simple
 - Stand alone battery backup for designated instruments
 - Simple AC supply for "last ditch" pumps and vents
 - Not just more diesels, but sources and connections that support specific loads

13

Conclusions

- Improvement to electrical system robustness can have an ALARA goal
- Epistemic uncertainties and the most extreme consequences should be understood
 - Take practical measures
- It is not possible to be robust to the unimaginable, or even to most worst cases
 - SAMG should include a loss of plant power supplies path
 - Provide supplies and connections that are independent of the plant to implement this path

14

Modernization of Unit 2 at Oskarshamn NPP– Main Objectives, Experience from Design, Separation of Operational and Nuclear Safety Equipment – Lessons Learned

Author Salah K. Kanaan

Nuclear Safety Analysis, El and I&C, OKG, Sweden

This paper aims to give a picture of Oskarshamn Nuclear Power Plant (OKG) experience from design for one of the biggest modernization project in the world and focuses on what was learned that is specific to robustness of electrical power systems, especially through Fukushima Station Blackout (SBO).

The planning for unit 2 at OKG was initiated in 1967 and the plant was completed on time and was synchronized to the grid October 2, 1974 and is of type BWR. Unit 2 was originally on 580 MW. In 1982 a thermal power uprate was performed, from 1700 MWh to 1800 MWh (106% reactor output).

A decision was made to perform a modernization and a new power uprate to 850 MW and there were several reasons for this decision; New safety regulations from Swedish Radiation Safety Authority (SSM), Ageing of important components and the initial focus was on safety and availability – Project Plant Life Extension (Plex) was established and became the largest nuclear power modernization in the world.

The modernization will lead to:

- ✓ New safety concept with 4 divisions instead for existing 2 with 2 new buildings South Electrical Building (SEB) and North Electrical Building (NEB)
- ✓ Completely new software - based equipments for monitoring, control and I&C
- ✓ New Low Pressure Turbine, new generator and main transformer
- ✓ New MCR and simulator
- ✓ Compliance with modern reactor safety requirements
- ✓ Redundancy, Separation, Diversification, Earthquake
- ✓ Reinforcement of existing safety functions
- ✓ New Electricity - I&C (electric power incl. reinforced emergency power and control systems)
- ✓ New buildings for Electricity - I&C
- ✓ Reinforcement of existing process systems as well as installation of new ones

Based on studies and good experiences on how to separate the operational and the safety equipment, the project led to a completely new safety concept. The safety concept is based on fully understanding the safety system that shall encompass all of the elements required to achieve a protective or safety function. It is of utmost importance that the requirements on redundancy, separation, diversification and earthquake will be fulfilled.

Okg had long technical discussions with the suppliers and the manufacturers of the new electrical equipment including the power electronic to understand the idea of a proper design margins how to be

specified, how to follow the regulations and how to be tested as part of the FAT. The experience stretches to include the testing of the new EPS in accordance with the new regulations. The paper will include some of the outcomes and the lessons learned from the installation of cable routing, new switchgears, transformers, batteries and rectifiers.

Definition and Abbreviations

The following terms and definitions are used in this paper:¹

diversification: two or more alternative systems or components that independently of each other perform the same safety task, but in essentially different ways or by having different characteristics.

common cause failure: a failure which simultaneously occurs in two or more systems or components due to one specific event or cause.

ELAP Extended Loss of Alternating current Power

ELAP-PS ELAP dedicated Power Source

Benefits and Challenges

The Road to a future Modernized Plant

OKG contains 3 units of different generations. Unit 1 has been in operation since 1972, unit 2 since 1974 and unit 3 since 1985. All units are highly dependent on electrical power for cooling Reactor Pressure Vessel (RPV) and Spent Fuel Pools (SFP).

The configuration and design of OKG is created by the Swedish company Asea-Atom with a strong influence from the US safety requirements that is documented in 10CFR50, 10CFR50 Appendices and Regulatory Guides. The US requirements are continuously screened by OKG and new or revised requirements are assessed with respect to positive impact on the safety of OKGs nuclear power plants.

The content of the present paper is primarily related to matters "within design basis" except for the questions specific to robustness of electrical power systems through Fukushima SBO, the content is related to matters "beyond design basis".

The main objective of project PLEX is to increase the safety measures and secure the availability, power uprate unit 2, address some environmental measures and a step by step implementation during the time period.

The purpose of the Project PLEX is among others to upgrade, to adapt and to modernize to state of- the - art standards the Reactor Protection System (RPS), associated IE controls and the Diverse Protection System (DPS) including monitoring systems. Two new I&C platforms, one for RPS and DPS respectively, are provided to implement the logic and control for all safety functions.

¹. The Swedish Radiation Safety Authority's Regulations concerning the Design and Construction of Nuclear Power Reactors, SSMFS 2008:17

Safety & Availability

The safety increasing measures and securing the availability of unit 2 will ensure 60 years of technical lifetime, as from 1974. Analysis regarding a power uprate was initiated, postponed and then resumed during the period 2003-2007.

The focus in Plex is on the safety measures and is aimed at meeting the modern reactor safety requirements stated in SSMFS 2008:17. A great number of measures are performed in order to meet the requirements regarding redundancy, separation, diversification and earthquake protection. One of the most important measure is to build a new diversified cooling chain for residual heat.

The modernization will lead to:

- ✓ New safety concept with 4 divisions instead for existing 2 with 2 new buildings South Electrical Building (SEB) and North Electrical Building (NEB)
- ✓ Completely new software - based equipments for monitoring, control and I&C
- ✓ New Low Pressure Turbine, new generator and main transformer
- ✓ New MCR and simulator
- ✓ Compliance with modern reactor safety requirements
- ✓ Redundancy, Separation, Diversification, Earthquake
- ✓ Reinforcement of existing safety functions
- ✓ New Electricity - I&C (electric power incl. reinforced emergency power and control systems)
- ✓ New buildings for Electricity - I&C
- ✓ Reinforcement of existing process systems as well as installation of new ones

Several large components required replacement at unit 2 to secure the availability once the unit's expected technical lifetime had been increased from 40 years to 60 years. Even before Plex was initiated there was a decision made regarding replacing the generator and transformer at unit 2, which was also done in 2005 and 2006.

A new low pressure turbine was required. Cracks on the low pressure rotors had been discovered. New low pressure turbines were installed during the outage in 2009. At the same time, some repair work was done on the condenser as well as some modernization work of auxiliary systems such as oil system.

Project Turbic was planned before Plex. Control systems were changed to software based and the control room interface was modified in connection to the outage in 2007.

A new and different design on inlet ports and blades leads to improved efficiency. Performance measurements conducted afterwards indicate almost 45 MW higher output power, far better than the 35 MW that were promised beforehand.

Power uprate

Preliminary studies regarding a power uprate at unit 2 were successively performed during the period 2003-2007 and the conclusion was reached that it would be possible. The final decision was made in 2007. An environmental court order approving the power uprate was granted during the autumn of 2009 and later on the government decision was granted.

An increase of the power output means that the fuel will be more stressed and that the percentage of fresh fuel increases. This will evidently lead to an increased use of fuel in proportion to the power uprate.

Together with the efficiency improvement the total power uprate at unit 2 will be 36 percent, which on a percentage basis is the highest power uprate in the world.

This means that there are new requirements imposed on the process systems, which in some cases require reinforcement, such as valves with greater capacity and stronger mounting. Analyses are being performed in order to establish the need.

Environmental

In connection to the environmental court examination of the entire OKG business including power uprate at unit 3 and the modernization at unit 2, the Environmental Court established a set of conditions to OKG for continued operation. Some of these conditions have been incorporated in project Plex. These conditions concern the deep sea water intake for unit 1 and unit 2, the installation of recombiners at unit 1 and unit 2, and the installation of carbon columns at unit 2.

A deep sea water intake will provide colder water to the station and thereby also colder water out in to the bay. The objective is to protect the fish living in the bay from too high temperatures. Improved efficiency in the units is a positive resulting effect, the colder the cooling water is, the higher the production.

A reduction of the releases of radioactive substances to air and water is crucial. OKG's emissions are already far lower than the set limit values, but with the help of recombiners and carbon columns these will be even further reduced.

Implementation

A decision regarding implementation over several years was made on an early stage in the process. Experiences from modernization project at unit 1 (MOD) showed that logistically it would be very difficult to perform all the planned activities during only one outage. A step by step implementation during the time periods was crucial.

The Challenge of New Technical Requirements

Diversification:

The diversification design principle shall be applied in the design of the reactor's defence in depth to the extent that is reasonably practicable. Diversification in the power supply system was discussed as a measure to avoid Common Cause Failures in the future.²

The requirement upon diversification in the new trains versus the existing trains of the electrical power supply system had to be further emphasized. Attention to that question was taken up in the design as well as in the validation of the system. It was recommended that a requirement on

². The Swedish Radiation Safety Authority's Regulations concerning the Design and Construction of Nuclear Power Reactors, SSMFS 2008:17

diversification should be valid for the following types of equipment: Diesel-generator sets, Rectifiers, Inverters, Batteries, Circuit breakers, Relay protections.

Diesel generators belonging to division A and B shall be of diversified type and manufacture versus the diesel generators in division C and D.³

The plant consists of about 9000 functions and components with some kind of electrical connection. About 1300 are modernized in earlier projects and about 2200 of them are foreseen to be modernized during the safety upgrade. The rest needs future modernization to secure another 30 years operation.⁴

Figure 1 shows the idea behind the new safety concept with 4 sets of EDG in which each set forms a complete autonomous unit.

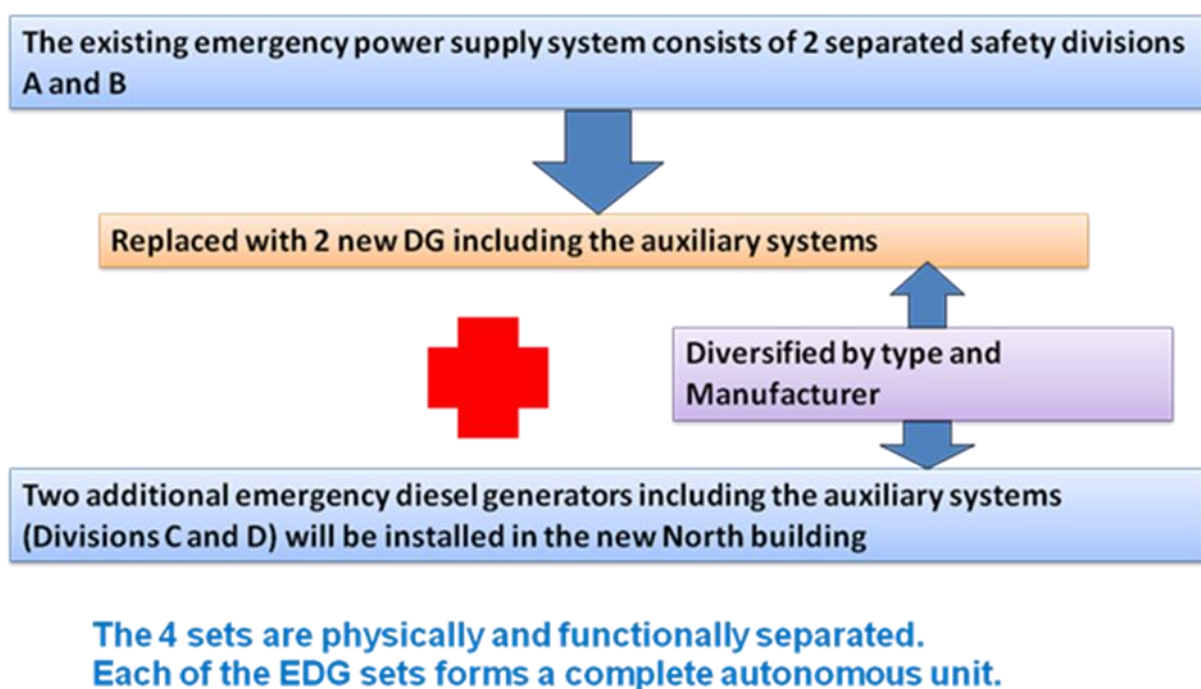


Figure 1. Safety concept with 4 divisions instead of existing 2

General Functional Requirements

New general functional requirements are for example:

- ✓ Separation requirements (such as the separation of 1E/2E functions),
- ✓ Redundancy requirements (such as a 4 channel structure for the new RPS),
- ✓ Diversity requirements (such as usage of diversified input conditions).

³. Oskarshamn 2 - Project Plex - Technical Requirements - Subproject Reactor (BETA)

⁴. I&C Modernization Strategy and Estimated Volumes

Detailed functional requirements

Detailed functional requirements on system level are specified in:

- ✓ The current OKG logic diagrams, which document the proven I&C design that meets the presently applicable general requirements and
- ✓ The Basic Design system descriptions which specify the new requirements on system level that result from project PLEX.

Other Considerations

Unit 2 has 4 different diversified power generation systems. Se Figure 2

- ✓ Offsite grid (with possibility for house load operation)
- ✓ Gas-turbine generators
- ✓ Emergency Diesel Generators (EDG)
- ✓ Batteries

The core cooling function at unit 2 is jeopardized only if the four diversified power generation systems are lost.

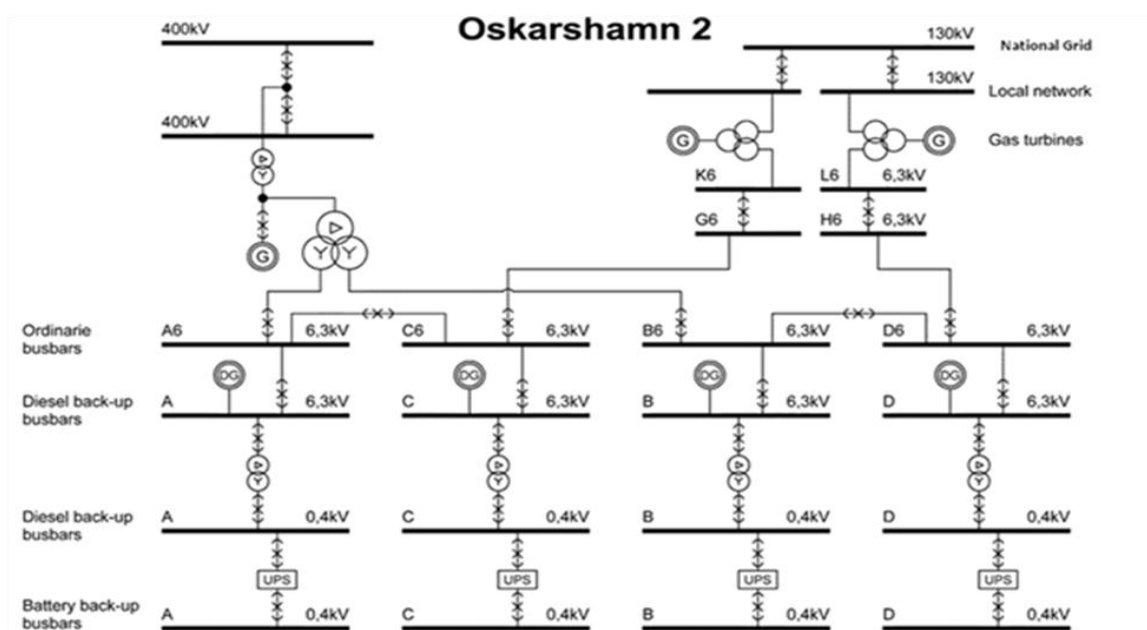


Figure 2. One-line diagram for Oskarshamn 2

The Gas Turbine Plant has historically been allocated to Unit 2 and it has been included in the safety concept, classified as safety class 3 and electrical functional class 1E. Due to Project Plex, the importance for Unit 2 will decrease.

Specific Challenges and lessons learned

Okg and for the EDG solution for unit 2 had long technical discussions with the suppliers and the manufacturers of the new electrical equipment including the power electronic to understand the idea of a proper design margins how to be specified, how to follow the regulations and how to be tested as part of the FAT. The experience stretches to include the testing of the new EPS in accordance with the new regulations.

Regulatory studies

In NPP, the importance of the formal using of Governmental regulations and industrial standards has been highlighted in the Safety Analysis Report (SAR) for each NPP⁵. OKG has built a committee known as Standard committee with the task to provide guidance for developing and implementing standards to ensure reactor safety and evaluate new and revised codes, standards and documents dealing with the design of nuclear power reactors before writing or updating the SAR. The codes and standards that are prioritized at OKG are in accordance with SAR hierarchy.

At the design stage, OKG can address the interpretation of the Governmental codes and industrial standards by attempting to find answers to two questions: how to tie in the Governmental codes e.g. Regulatory Guides and the industrial standards e.g. IEEE standards, and how to integrate both types of requirements in the design process.

It has been discussed at all levels at the plant to find an easy way of presenting the codes in question and their related industrial standards in a good practical hierarchy. The work led to finding modules presenting the hierarchy connections between the industrial IEEE standards related to class 1E power systems and Regulatory guide codes of the NRC Government regulations. Project PLEX presented a hierarchy in which helped identifying the proper standards as early as possible in the design process. The hierarchy can help OKG staff to better incorporate codes and standards and implement them in the right way by⁶:

- ✓ Making the hierarchy available in OKG homepage and have an easy access to them.
- ✓ Conducting standard training for engineers, maintenance staff and for the management.
- ✓ Developing and disseminating standards education materials that can be incorporated into existing courses at the plants. Materials may include tutorials, case studies, lectures by industry professionals and Standard committee personnel on the basics of standards, and instruction on how to read and use the hierarchy lists.
- ✓ Developing examples of how to use standards in various foundations and experience change from different projects at the plant.
- ✓ Using the hierarchy lists when discussing different kinds of technical issues with suppliers and the manufacturers at any level of the projects.

⁵. Oskarshamn 2 – Safety Analysis Report (SAR)

⁶. The state of the use of hierarchy structure between IEEE standards and Nuclear Regulatory Guides related to class 1E Power Systems by Salah Kanaan

Dynamic Simulation Studies

In order to verify that the AC auxiliary power system at unit 2 is capable of providing sufficient electric power to the modernised plant with preserved tolerances regarding frequency, current ratings and voltage, a package of simulation studies was performed.

The auxiliary power system is modelled in Simpow power system simulation software. The modelling scope included component details from the 400 kV and 130 kV connection points to the power transmission network down to 400 V AC network. The DC network was represented as PQ – load. The asynchronous loads on safety related busbars are modelled down to 10 kW. The loads at non-safety busbars are modelled down to 75 kW. The rest of loads are modelled as lumped equivalent loads.

The component data available was often not detailed enough for modelling purpose, especially for asynchronous machines. Instead of being forced to use extremely conservative assumptions during simulation studies, a lot of emphasis was put on modelling asynchronous machines correctly. For this purpose we conducted extensive measurements of asynchronous machine start-ups. The measurements were used for development of a parameterisation method based on IEEE standard. Machine parameters generated with this method resulted in satisfactory results when dynamic simulations were compared to measurements even for those cases when only rated machine parameters were available at start.

Measurement based modelling was also applied for the diesel generator engines and control systems as satisfactory data could not be obtained from the contractors. From the measurement data obtained during set of dynamic tests the models of governor, AVR and excitation system were developed. Even dynamic temperature dependence of engine turbo operation was represented in detail which plays important role in dynamic simulation studies of diesel start sequences with cold engine.

The simulation studies performed were:⁷

- ✓ Operation currents on all busbars
- ✓ Short-circuit currents on all busbars
- ✓ Start sequence on gas turbine secured non-safety busbars
- ✓ Start sequence on diesel secured busbars
- ✓ MAVA pump start and stop on non-safety busbars
- ✓ Start of largest load on diesel secured busbars
- ✓ Loss of largest load on diesel secured busbars

Factory Acceptance Test related to the Disturbances in the External Grid

The design basis events and the disturbances in the external grid were discussed during different phase at the project. The incident at Forsmark nuclear power plant in Sweden on the 25th of July 2006 has focused the interest on the interaction between events in external grid and the performance of safety related equipment in the nuclear power plants.

The result of the simulations of all short-circuits or earth-fault cases have resulted in a set of a limited number of design voltage and frequency profiles. Such profiles can be used in specification

⁷. Oskarshamn 2 – Study outline – Analysis in PLEX Modernized Plant

and testing of safety related equipment. The profiles have been used as initial conditions, and already incorporated in SAR for unit 2.

The project faced a big challenge for testing the new UPS and the rectifiers to ensure that they withstand all the voltage and frequency design profiles. The discussions with the supplier and the manufacturers lead to a specific test adaptation resulted in an accepted output. Fig 3 shows the single line diagram for the test facility for the tested rectifier.⁸

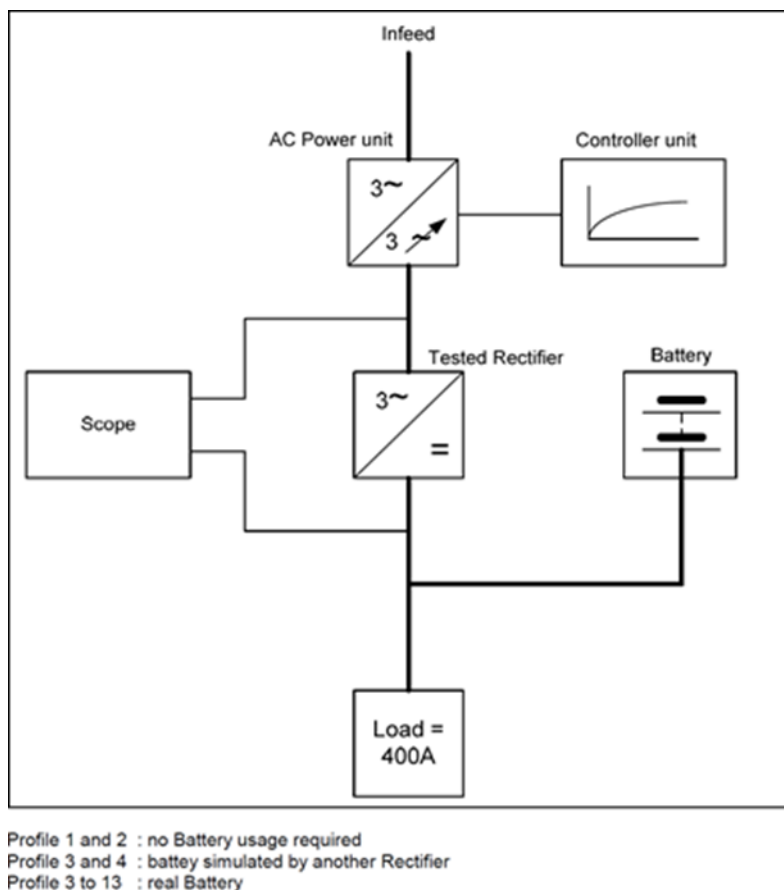


Fig 3 Single line diagram of test facility

Implementation during different time period

OKG learned from the modernization project at unit 1, that implementation during one time period and one big outage was not the most optimal solution. Project PLEX planned the implementation during different outages and a step by step during the time periods:

- ✓ Outage 2007
- ✓ Outage 2009

⁸. Factory Acceptance Test, FAT 115105 for Battery Charger/Battery Cubicle, AEG Power Solutions

- ✓ Outage 2013
- ✓ Outage 2015 (Some other small implementation was planned in between presented periods).

Separation of 1E and 2E

Based on studies and good experiences on how to separate the operational and the safety equipment, the project led to a completely new safety concept. The safety concept is based on fully understanding the safety system that shall encompass all of the elements required to achieve a protective or safety function. It is of utmost importance that the requirements on redundancy, separation, diversification and earthquake will be fulfilled.

The Challenges specific to robustness of electrical power systems through Fukushima SBO

Following the nuclear accident in Fukushima the European Council of Ministers decided, March 25, 2011 that Member States would begin to review the safety of their nuclear facilities through a comprehensive risk and safety assessment, so-called *stress test*.

A group was built and made an international survey of the most important historical events. The complete picture shows a position beyond the design bases for the nuclear power plants.

On March 20, 2012 the USNRC issued an “Advance Notice of Proposed Rulemaking” regarding a change of the 10CFR50.63, also known as the “Station Black-out rule”. The proposed change is to extend the coping time for a SBO-situation to 8 hours without any AC-sources available and a coping time of 72 hours without any external supplies arriving to the site.⁹

OKG took into account national and international experiences and future requirements and followed Fukushima event continuously to understand what happened and what was needed to be addressed.

Our assessment was that new postulated events like Loss of AC-power; Station Blackout (SBO) for design of back fitting measures shall take expected requirement changes in the US into account.

Each function was analyzed with respect to their prerequisites (technical/functional, maintenance, operation) and the prerequisites for the function were analyzed based on how they were affected by external events.

Some of the conclusions from performed analysis are shown below: ¹⁰

- ✓ Ensuring that consumables are accessible (fuel, oil, filters, etc.) in the required amount and in direct connection with diesel generators (and gas turbines) to withstand at least 72 hours of operation as well as central storage for a total of at least seven days’ operation
- ✓ Increased robustness may also be achieved by changing to a common fuel for all diesel engines, if possible, and ensure that equipment for the transport of fuel within the site from units not needed to other units with acute needs

⁹. Project Kent - OKGs Position related to experiences after Fukushima

¹⁰. Project Kent – Consequences on OKG after Fukushima incident

- ✓ Existing instructions are developed with the assumption that external net return within a few hours.
- ✓ Review of existing relevant instructions and training/coaching of staff should be implemented to improve the ability to maintain the power supply function in a long term process.
- ✓ Day tank volume for unit 1/unit 2 is not sufficient for multi-day operation. Fuel supply in relation to long-term operation depends on storage tanks within the area, and associated electric powered heating cables and pumps.
- ✓ Review should be made of systems and equipment for fuel supply without any manual steps to ensure fuel supply for at least seven days without influence of initial event (earthquake) and external events (cold).

New requirements on ELAP-PS after Fukushima incident

After Loss of off-site power, emergency diesel generators and any alternate AC source but not the loss of AC power to buses fed by station batteries through inverters, the alternate auxiliary power source (ELAP-PS) shall be credited after 8 hours.

The ELAP-PS shall be designed for continuous operation (>72 hours)¹¹

The results of the study and the work done led to general improvements:

- ✓ Extend batteries discharge time by higher capacities and load shedding (The limiting case for battery capacity sizing will normally be station blackout)
- ✓ Secure power from the gas-turbines to all units
- ✓ The power systems shall withstand severe weather conditions like low and high temperature, heavy snowfall, seismic condition, flooding and ice storms.
- ✓ Seismic resistance up to 10^{-5} /year
- ✓ Stationary diesels to feed the Multi Venting Scrubber System (MVSS), (Filtered containment venting through an inerted multi-venturi scrubber system with a decontamination factor of at least 500 was installed after Three Mile Island accident in 1979. Based on a governmental decision, all Swedish Nuclear Power Plants were back fitted with severe accident mitigation systems)
- ✓ Mobile diesels to charge the batteries
- ✓ Enhancement between ordinary and alternative power sources by:
 - i. For unit 1: Install a new Reserve Diesel-Generator (RDG) and possibility to decrease the demand and the requirement on the gas-turbines
 - ii. For unit 2: Install 2 new EDG
 - iii. For unit 3: Install automatic connection to the gas-turbines to cope with CCF of the diesels.

Unit 1 and unit 3 take credit of an alternate AC power source in order to fulfil SSMFS 2008:17 §10. (CCF in reactor protection system in unit 1 and CCF in diesel generators or diesel cooling systems in unit 3). OKG had to face the fact that the existing Gas Turbine Plant, including the GTGs, that supply electrical backup power were commissioned in 1972 and have to be renewed and/or go a major over-hauled. Availability of the Gas Turbine Power Plant is decreasing and maintenance cost is

¹¹. ENSREG - Interpretations and assumptions

increasing. Main supplier Siemens has in 2012 withdrawn the service and spare parts for these power packs, due to a low quantity.

There is an ongoing study at OKG to decide whether it is feasible possible to exchange the existing GTP with a new Power turbine or even with a Diesel-Generator (DG). The study preliminary points out the reliability and availability for both GTG and DG, but the background is not to full extent clear.¹²

Many lessons were learned from the maintenance departments, main supplier, international and national forum to cope with the ageing auxiliary power supply at OKG.

New Alternate Power Source Classification

The classification of the alternate AC power source is affected by a number of parameters. We still have conflicted interpretation on how we deal with whether this should be classified as a Non-Nuclear Safety (NNS) or not.

In a non released SSM document they required classification of systems and components credited to cope with CCF as follows:

- If existing system and components are credited NNS is acceptable with additional requirements regarding testing and readiness for operation

- If new systems and components are credited the classification these should be in accordance with the ordinary function (Safety classified).

Due to this uncertainty an investigation is on-going to prepare a quality assurance concept which allows industrial standard components to be used. The working title of the new safety class is "Safety Class 3*".

Conclusion

The importance of the modernization of unit 2 is to fulfil the requirements on redundancy, separation, diversification and earthquake. This OKG has learned through compliance with the Swedish Radiation Safety Authority new requirements especially after Forsmark 1 incident on the 25th of July 2006.

Parallel with the modernization project at unit 2, OKG has learned from the experiences in the Fukushima event; took into account national and international experiences and future requirements, followed Fukushima event continuously and finally the results of the study and the work done led to general improvements presented in this paper.

¹². Oskarshamn 1, 2 och 3 - Project KENT - Recommendation of concept for new auxiliary power generation facility

CSNI International Workshop on

ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs in Light of the Fukushima Daiichi Accident

Modernization of unit 2 – Main objectives, experience from design, separation of operational and nuclear safety equipment – Lessons learned

Salah Kanaan Engineer Nuclear Safety Analysis



S Kanaan Oskarshamn NPP CSNI Workshop 1th-4th of April 2014. ROBUSTNESS OF ELECTRICAL SYSTEMS of NPPs

1

Oskarshamn NPP (OKG)

Electrical Systems

The site contains 3 units of different generations

Unit 1 in operation since 1972

Unit 2 since 1974

Unit 3 since 1985

All units are highly dependent on electrical power for cooling (Reactor Pressure Vessel, RPV) and (Spent Fuel Pools, SFP)



S Kanaan Oskarshamn NPP CSNI Workshop 1th-4th of April 2014. ROBUSTNESS OF ELECTRICAL SYSTEMS of NPPs

2

Configuration and design of OKG NPP

The configuration and design of OKGs nuclear power plants is created by the Swedish company Asea-Atom with a strong influence from the US safety requirements that is documented in 10CFR50, 10CFR50 Appendices and Regulatory Guides.

The US requirements are continuously screened by OKG and new or revised requirements are assessed with respect to positive impact on the safety of OKGs nuclear power plants.



S Kärnan Oskarshamn NPP CSNI Workshop 1th-4th of April 2014. ROBUSTNESS OF ELECTRICAL SYSTEMS of NPPs 3

The road to a future modernized Plant

New safety regulations

- SKIFS 2004:2 (Swedish Radiation Safety Authority Regulatory Code)

Power uprate

- The power output situation in Scandinavia led to preliminary studies especially after the decommissioning of Barsebäck NPP.

Ageing replacements and maintenance

- O2 was commissioned in 1974
- Modernization required, old parts require replacement
- Strategic decision regarding extended technical lifetime to 60 years of operation



S Kärnan Oskarshamn NPP CSNI Workshop 1th-4th of April 2014. ROBUSTNESS OF ELECTRICAL SYSTEMS of NPPs 4


Modernization of unit 2

Project Plex

Plant


Life

EXtension




© Kärnten Oskarshamn NPP/CSNI Workshop 1th-4th of April 2014. ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs

Modernization of unit 2




The largest nuclear power modernization in the world



© Kärnten Oskarshamn NPP/CSNI Workshop 1th-4th of April 2014. ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs

Benefits & Challenges

- Safety increasing measures in accordance with SSM's regulations (Diversification, separation, earthquake etc.)
- Secure the availability (ensuring 60 years)
- Power uprate (To meet the demand)
- Environmental measures (fresh fuel increase due to power uprate, A deep water intake, protect the fish in the bay from high t and new recombiners and carbon columns for CO2
- A step by step implementation during the time periods:
 Outage 2007
 Outage 2009
 Outage 2013
 Outage 2015
 implementation in between periods




okg
- ett företag i E.ON-koncernen

S Kärnan Oskarshamn NPP/CSNI Workshop 1th-4th of April 2014. ROBUSTNESS OF ELECTRICAL SYSTEMS of NPPs 7

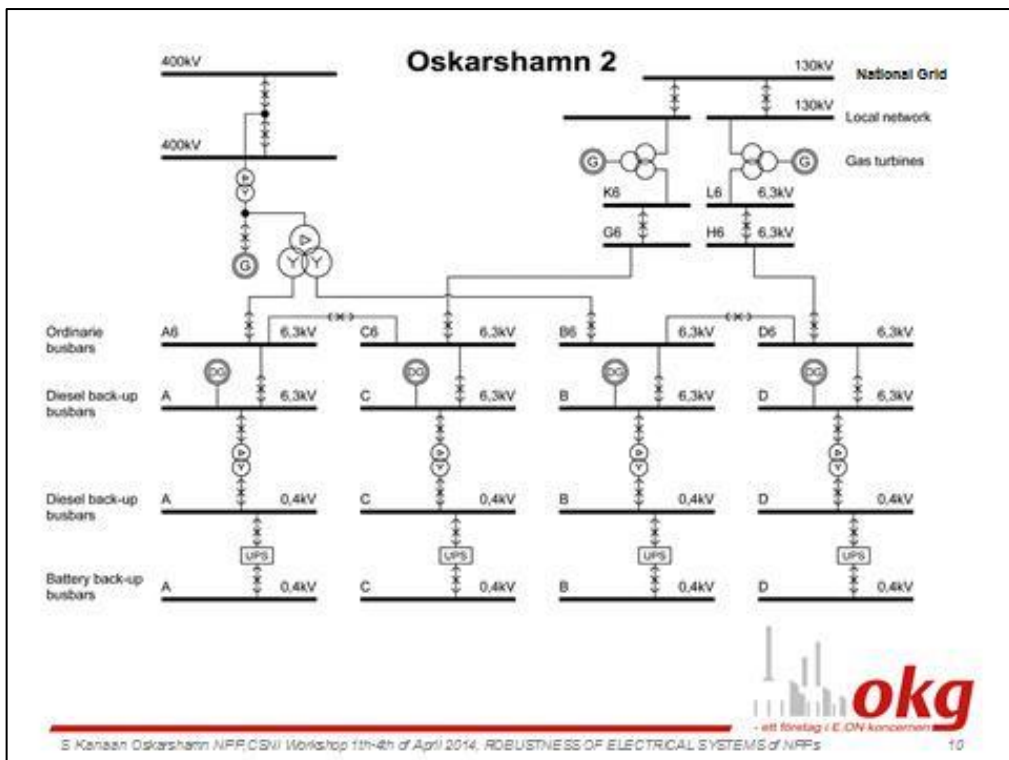
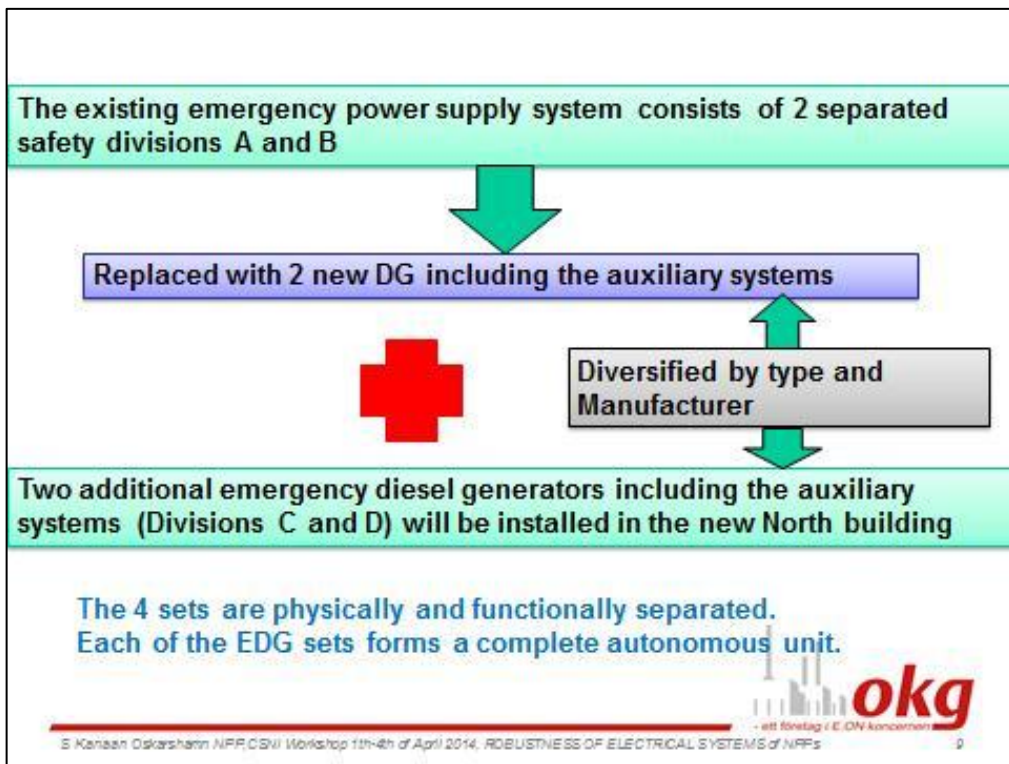
Safety Increasing measures

<p>Compliance with modern reactor safety requirements</p> <ul style="list-style-type: none"> • Redundancy → • Diversification • Separation • Earthquake 	<p>Main measures</p> <ul style="list-style-type: none"> • New cooling chain for residual heat • New Reactor Protection System including the modernization of the MCR. • New Electricity - I&C (electric power incl. reinforced emergency power and control systems). New buildings • Separation between operational and safety classified electric power • New protection in the ventilation system during fire • Enhanced barrier function and reinforcement in some process systems
--	---



okg
- ett företag i E.ON-koncernen

S Kärnan Oskarshamn NPP/CSNI Workshop 1th-4th of April 2014. ROBUSTNESS OF ELECTRICAL SYSTEMS of NPPs 5



Power uprate measures in year 2015

- Increase the thermal power output from 1800MW to 2300 MW (an increase of circa 28%)
- Increased thermal output by increasing the power output of fuel
- These measures together with the turbine work (ca 50MWe) will give an increase from circa 610 MWe to circa 840 Mwe (approximately 37 %)
- Upgrading the capacity of process systems (safety functions as well as operational functions)
- License from the Environmental Court and SSM/the Government



Specific Challenges and lessons learned

1. Regulatory studies

□ It has been discussed at all levels at the plant to find an easy way of presenting the Governmental Codes and their related industrial standards in a good practical hierarchy. The work led to finding modules presenting the hierarchy connections between the industrial IEEE standards related to class 1E power systems and Regulatory guide codes of the NRC Government regulations.

The presented hierarchy helped identifying the proper standards as early as possible in the design process. The hierarchy can help OKG staff to better incorporate codes and standards and implement them in the right way.



Specific Challenges and lessons learned

2. Dynamic Simulation Studies

□ In order to verify that the AC auxiliary power system at unit 2 is capable of providing sufficient electric power to the modernised plant with preserved tolerances regarding frequency, current ratings and voltage, a package of simulation studies was performed.

1. A parameterisation method for AM based on IEEE standard was developed
2. Satisfactory data could not be obtained from the contractors. From the measurement data obtained during set of **dynamic tests** the models of governor, AVR and excitation system were developed.
3. Even dynamic temperature dependence of engine turbo operation was represented in detail which plays important role in dynamic simulation studies of diesel start sequences with cold engine.



Specific Challenges and lessons learned

3. FAT related to the disturbances in the External Grid

□ The project faced a big challenge for testing the new UPS and the rectifiers to ensure that they withstand all the voltage and frequency design profiles.

The discussions with the supplier and the manufacturers led to a specific test adaptation resulted in an accepted output.



Specific Challenges and lessons learned

4. Implementation during different time period

☐ OKG learned from the modernization project at unit 1, that implementation during one time period and one big outage was not the most optimal solution.

Project PLEX planned the implementation during different outages and a step by step during the time periods:

Outage 2007

Outage 2009

Outage 2013

Outage 2015 (Some other small implementation was planned in between presented period).



Challenges specific to electrical power systems through Fukushima SBO

Following the nuclear accident in Fukushima the European Council of Ministers decided, March 25, 2011 that Member States would begin to review the safety of their nuclear facilities through a comprehensive risk and safety assessment, so-called stress test.



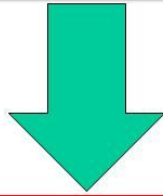
A group was built and made an international survey of the most important historical events. The complete picture shows a position beyond the design bases for the nuclear power plants.



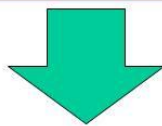
Our assessment was that new postulated events like Loss of AC-power; Station Blackout (SBO) for design of back fitting measures shall take expected requirement changes in the US into account.



The ELAP-PS shall be designed for continuous operation (>72 hours based on ENSREG - Interpretations and assumptions)



Ongoing study to use GTP or DG. The study preliminary points out the reliability and availability for both, but the background is not to full extent clear



The results of the study and the work done led to general improvements.



The improvements are as follow:

1. Extend batteries discharge time by higher capacities and load shedding (*The limiting case for battery capacity sizing will normally be ELAP & LUHS*)
2. Secure power from the gas-turbines to all units
3. The power systems shall withstand severe weather conditions like low and high temperature, heavy snowfall, seismic condition, flooding and ice storms.
4. Seismic resistance up to 10^{-5} /year



5. Stationary diesels to feed the MVSS, Multi Venting Scrubber System (*Filtered containment venting through an inerted multi-venturi scrubber system with a decontamination factor of at least 500 was installed after Three Mile Island accident in 1979. Based on a governmental decision, all Swedish Nuclear Power Plants were back fitted with severe accident mitigation systems*)

6. Mobile diesels to charge the batteries



7. Enhancement between ordinary and alternative power sources by:

-For unit 1: Install a new RDG and possibility to decrease the demand and the requirement on the gas-turbines

-For unit 2: Install 2 new EDG

-For unit 3: Install automatic connection to the gas-turbines to cope with CCF of the diesels.



Existing Gas Turbine Plant

- The Gas Turbine Plant has historically been allocated to Unit 2 and it has been included in the safety concept, classified as safety class 3 and electrical functional class 1E. Due to Project Plex, the importance for Unit 2 will decrease.
- Unit 1 MOD-project installed RPS and diesel control equipment based on the same platform which creates CCF. To cope with that the Diversified reactor Protection System (DPS) and the high pressure core injection system are fed from the gas turbines.
- Unit 3 is dependent on the gas turbines due to CCF in the diesels and their cooling system. The regulator have stated that new equipment used to diversify a function must be classified as the system it diversifies.



Existing gas turbine plant status

The main conclusions of the gas turbine status are:

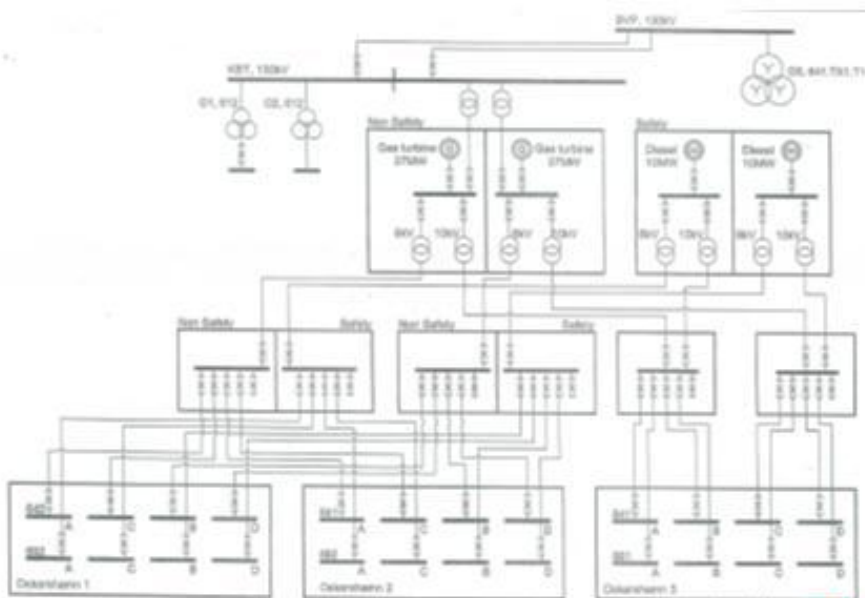
- All Units are dependent on the existing gas turbines. The criteria for repairing them will be 28 days after project Plex, today it is 14 days. If a break down occurs that would take longer to repair, than 14 or 28 days, all Units have to shut down.
- The buildings are poor, there is leakage and the weak design has to be upgraded to fulfill extreme weather conditions. The chimneys are damaged.
- The Power Turbine have had problems with cracks in the inner guide vanes. This has led to 2 break downs in the past.
- There is lack of spare parts for the auxiliary systems. Old relay technology and availability is decreasing



New alternate power source classification

The classification of the alternate AC power source is affected by a number of parameters:

- We still have conflicted interpretation on how we deal with whether this should be classified as a Non-Nuclear Safety (NNS) or not.
- Due to this uncertainty an investigation is on-going to prepare a quality assurance concept which allows industrial standard components to be used. The working title of the new safety class is "Safety Class 3*"





RCC-E A Design Code for I&C and Electrical Systems

JM HAURE

EDF SEPTEN, Villeurbanne

Abstract: RCC-E a design code for I&C and electrical systems

The paper deals with the stakes and strength of the RCC-E code applicable to Electrical and Instrumentation and control systems and components as regards dealing with safety class functions.

The document is interlacing specifications between

Owners, safety authorities, designers, and suppliers

IAEA safety guides and IEC standards.

The code is periodically updated and published by French Society for Design and Construction rules for Nuclear Island Components (AFCEN).

The code is compliant with third generation PWR nuclear islands and aims to suit with national regulations as needed in a companion document.

The Feedback experience of Fukushima and the licensing of UKEPR in the framework of Generic Design Assessment are lessons learnt that should be considered in the upgrading of the code.

The code gathers a set of requirements and relevant good practices of several PWR design and construction practices related to the electrical and I&C systems and components, and electrical engineering documents dealing with systems, equipment and layout designs.

Comprehensive statement including some recent developments will be provided about:

- Offsite and onsite sources requirements including sources dealing the total loss of off sites and main onsite sources.
- Highlights of a relevant protection level against high frequencies disturbances emitted by lightning strokes,

Interfaces data used by any supplier or designer such as site data, rooms temperature, equipment maximum design temperature, alternative current and direct current electrical network voltages and frequency variation ranges, environmental conditions decoupling data,

- Environmental Qualification process including normal, mild (earthquake resistant), harsh and severe accident ambient conditions. A suit made approach based on families, which are defined as a

combination of mission time, duration and abnormal conditions (pressure, temperature, radiation), enables to better cope with Environmental Qualifications.

- Electrical equipment separation requirements and isolation and decoupling solutions.

1. Introduction

The nuclear safety of the nuclear power stations is articulated around a certain number of important aspects for the maintenance and the improvement of the level of safety. The following fields are very largely dependent:

- standardization and the development of the codes,
- The standardization facilitates the analysis of the experience feedback and vice versa, the benefit drawn from the experience feedback and all the more considerable as the standardization is high.
- The international exchanges contribute significantly in the research and the experience feedback.

French nuclear industry (owners and industrialists) mobilizes engineers and technicians whose work is devoted to safety: organization, studies, tests, monitoring, audits internal and external, etc.

The roles of the various partners are summarized:

- the public authorities define the general objectives of safety,
- the owner proposes technical methods to reach them and justifies them,
- the public authorities make sure of the adequacy of these methods to the laid down objectives,
- The owner implements the approved provisions.
- The public authorities check the good implementation of the provisions.

The presentation hopes to contribute to clarify the relationship of trust brought by the standardization, the development of the codes in answer to technical recommendations of the Safety Authorities.

2. Standardization

The standardization initiated by EDF with the fossil power plants during the Sixties was implemented for the nuclear plants. It consists to build units identical with the differences limited to the site adaptation (riverside or seaside), the nuclear steam supply systems, the turbo-generator group and the same suppliers provide all the equipment and circuits identical. Three great series were launched:

- PWR 900, 34 units
- PWR 1300, 20 units
- PWR 1450, 4 units

The generic studies, evaluations of safety, manufacturing drawings, the equipment of machine, manufacturing methods, of construction, are deadened on all the series, of reproducible quality and faster to implement. The spare parts are the same ones for all the series. The erection teams are acquainted with the methods; the procedures of control are applicable to all the series, the operating teams trained on simulators.

The generic defects, i.e. common to all the power plants of the series cost sometimes expensive. The experience shows that the systematic vigilance and inspections make it possible to be alerted of certain defects before they degenerate and to bring their solutions adapted on the NPP series or the whole NPP fleet.

To maintain the principle of standardization, the detail improvements made to a NPP of a series are then implemented to all the NPP of the series, to keep the standardized series of plants.

3. Regulations Codes and Standards

A series of directives fixes rules and practical technical as regards with nuclear safety are emitted by the NNSA, lay down the general objectives, and are relatively very few. It is up to industry to propose the application methods that are subjected to the NNSA approval. The figure 1 shows an example of regulatory pyramid.

A series of directives fixe rules as regards nuclear safety. It deals with four important topics:

- the equipment under pressures,
- the organization of quality,
- withdrawals and discharges from nuclear facilities,
- Nuisances and external risks arising from operation of nuclear facilities.

Two on four themes are related to design and construction codes:

- With regard to the equipment under pressure, nuclear installations include two of them: on the one hand, those, which are nuclear, field specific, i.e. those that confine of the radioactive releases, on the other hand those of the conventional field that are not specific nuclear installations.
- As regards quality, the rules of assurance and organization of the quality, which the owners shall follow at the three stages of the design, the construction, and the exploitation of the nuclear installation. It is indeed fundamental for the safety that the nuclear island either built in strict conformity with the specifications fixed at the time of its design. It is the object of the provisions known as “of quality assurance” reinforced by the IAEA GSR3 guide and its updating under drafting.

The safety options are specified by the NNSA when reviewing a project basic design. The recommendations put forth by the NNSA that define in various technical fields of the objectives of safety and describe practices that they judge satisfactory to respect these objectives.

The codes of nuclear industry such as the *Rules of Design and Construction (RCC) and EPR Technical Codes (ETC)* provide the set of the rules, codes, and standards that the owner implements at the time of the design, the realization, and the start-up of the important equipment for safety. The owners and manufacturers have developed “Rules of Design and Construction” (RCC) which concretely transpose the requirements of the regulations while reflecting the industrial good practice. The RCC and ETC cover the following fields:

- RCC-M: Rules of design and construction applicable to the mechanical components for the pressurized water reactors,
- RCC-MRx: Rules of design and construction applicable to the mechanical components for the fast and 4th generation reactors,
- RCC-E: Rules of design and construction applicable to the electrical and I&C equipment,
- RCC-C Rules of design and construction applicable to the fuel assemblies,

Initially had been created codes for the following fields:

- RCC-G: Rules of design and construction applicable to civil works engineering,
- RCC-I: Rules of design and construction applicable to fire protection,

They were replaced respectively by the codes:

- ETC-C: EPR Civil Technical Codes for works,
- ETC-F: EPR Technical Codes for Fire protection.

One specific to the in-service inspection and maintenance:

- RSE-M: In-Service Inspection Rules for Mechanical Components of PWR Nuclear Islands

These rules are written and published by French Association for the rules of design, construction, and monitoring in exploitation of the Nuclear Steam Supply System (AFCEN), in which in particular EDF, AREVA NP and CEA take part.

The NNSA carries out the evaluation of the codes and their revisions.

4. RCC-E

History The coding process related to nuclear island was undertaken in April 1978 under the leadership of EDF and AREVA NP (ex-FRAMATOME) and with the participation of the principal industrialists implied in the realization of the nuclear program. Thirty plants of the French nuclear program were already in construction or service. The practices of design and construction were already highly standardized. A high level of quality had been reached and maintained in spite of the difficulties of realization of a so wide program. These practices were dispersed in a great number of technical specifications established by the manufacturers and checked by the architect-owner EDF. The implementation of this code aimed:

- to simplify the circuits of approval of the documents,
- to fix a precise contractual base,
- to improve the effects of the standardization,
- to enable doing offers for the exportation,
- To clarify the applicable rules for the NNSA.

The development of the RCC-E allowed a wide dialog between owner (EDF), the manufacturers, and the various suppliers whose objective was to examine from every angle the “state of Art”. The industrialists were not ready to let a code specifying requirements on a part of their know-how; finally, they ended up collaborating in its development. The RCC-E gathers in one document the generic rules making possible to specify the various packages, electrical equipment, and instrumentation and control equipment contributing to safety classified functions. These requirements are defined for a safety redundancy of a pressurized water reactor. Project Data Books respectively supplement the generic rules for the NPP in exploitation and the EPR, 3rd generation of NPP.

Design Experience and references: The RCC-E was used:

- in France for the NPP series PWR 1300, PWR 1450 and EPR, i.e. 13 NPPs,
- In South Korea, South Africa and China. France for the PWR900 sold, i.e. 10 NPPs,
- in China for the

- CPR 1000 Program, 19 NPPs (HongYangHe 4*1000MW, Ningde 4*1000MW, Yangjiang 4*1000MW, Fuqing 2*1000MW, Fangjiashan 2*1000MW)
- EPR Taishan 2*1650MW

The appropriation of the RCC-E 2005 and its translation were undertaken by China in 2009.

Actually, the RCC-E code has been used for the design and construction of above 50 NPPs.

The 2012 version is the sixth edition of RCC-E. It is applicable to existing NPP and NPP 3rd generation EPR. The later shall be used for UK EPR.

Project Data books supplement rules generic rules with specific characteristics to existing NPP or NPP 3rd generation EPR.

The scope of application of the requirements is the activities of design, manufacture, and construction and of maintenance. The industrial architect, engineering of NPPs, the installation engineering departments, the clients and the manufacturers and suppliers follow the RCC-E. The applicability of the RCC-E can be summarized through the

The referenced standards, International standards account for 84% of the standards used. Few remaining French standards correspond to requirements that are not yet within the international standardization.

The input data result from the safety analyses report and the national technical regulations. They include/understand in particular

- the definition of the characteristics of the extra high voltage grid-NPP interface,
- the project industrial policy,
- the project safety classification,
- the number of safety train, and
- The accidents envelopes of basic design accidents and severe accidents.

The documentation used is described and contents defined for some the engineering documents:

- Electric systems,
- I&C control systems,
- Equipment and its manufacturing and environmental qualification,
- Layout engineering
- Engineering documentation.

Electrical equipment and/or I&C equipment contributing to safety-classified functions are powered by power and control sources that fulfil the requirements concerning:

- the independence of the off-site electric sources,
- the sizing of the power transformers,
- the sizing of the on-site power sources (standby sources, ultimate power sources, DC and AC vital sources)
- the coordination of the characteristics of the plant electric network (voltage, current and insulation),
- the personnel safety and the equipment protection against the electromagnetic interferences,
- the electric separation between equipment of different safety classes,
- guarantee of availability of the equipment and functions,

- Interchangeability of the materials,
- Use of smart devices.

The I&C equipment, contributing to the safety functions implemented in the reactor protection system fulfils in more the requirements:

- Of I&C general architecture,
- Of development and qualification of the programmed software system according to the required safety class,
- Engineering of the human factor,
- Means of control, communications, and safety information in control rooms.

The demonstration of equipment environmental qualification An electromechanical chain (figure 3) defines the list of equipment to be qualified. The proof, that equipment withstands the environmental conditions, is provided by conformity to the establishment of qualification requirements that rely on:

- Agreement of a supplier and its material,
- Establishment of a program of qualification based on one of the following methods, analysis, the analogy, modelling, tests of the type (preferred solution) or a combination of these methods qualification.
- Documentation associated with the process of qualification, identification of the qualified model and its manufacturing processes and of control, the guarantee of compliance of the materials of series with the qualified model material, the program of qualification and specifications of tests associated, the anomalies of test, the reports of test and the report of qualification.
- The approach of ambience families determines, on the basis of the time of mission of the equipment, the customized conditions of environment envelopes of the constraints resulting from design accidents and severe accidents including seismic loads.
- Electrical and electronic materials qualification master list.

Supplemented requirements are raised for the construction of the small electric and electronic components such as the sensors, electronic circuits, the terminals and clips, the cabinets, boxes etc... Those requirements make it possible to conceive all the industrial aspects for this equipment. They are supplemented by requirements about the obsolescence of the components, electronic cards.

The great principles of nuclear safety are identical in all the countries. However, the differences in their application can lead to differences in the requirements in safety, even on different levels of safety. The approaches of safety were indeed constituted progressively of the construction of the successive generations of nuclear installations, and were developed by the originators according to the technologies selected.

The various actors, authorities of safety, experts, research organizations, owners, and manufacturers for a long time tied relations for exchange information on their approaches and their practices, to even harmonize them. In addition to the numerous relations and bilateral agreements, it is necessary to underline the work of harmonization made within international agencies.

The regulation concerns the responsibility for the authorities for each country, but, today, several interests convergent to go further in the harmonization:

- in the long term, the requirements as regards protection of the populations and the environment should not be significantly different,

- The harmonization of safety is one of the answers to the opening of the markets and the internationalization of the nuclear safety operators at least in the European plan, for the nuclear power plants.

5. CONCLUSION

RCC-E Evolutions have been requested by:

- The export of nuclear power stations,
- The development of the EPR in collaboration with SIEMENS, AREVA and of the German owners.
- The UK EPR licensing process,
- DIDLESYS recommendations.

These modifications have already purged the code of the discriminatory requirements.

A last stage consists to maintain the code as close as possible with the evolution of:

- the feedback experience of the Chinese users and manufacturers;
- IEC standards,
- IAEA safety guides and relevant good practices,
- The WENRA Safety Reference Levels.
- The Fukushima and ROBESYS feedback experience.

ACRONYMS

NNSA: National Nuclear Safety Authority

EDF: Électricité de France, French nuclear power station operator

CEA: French Atomic Agency

NPP: Nuclear Power Plant

AFCEN : French Association in charge of RCC writing

REFERENCES

- [1] SFEN - AFCEN November Conference, 23rd 1989.
- [2] RCC-E 2012 AFCEN and projects data books

ANNEX A FIGURES

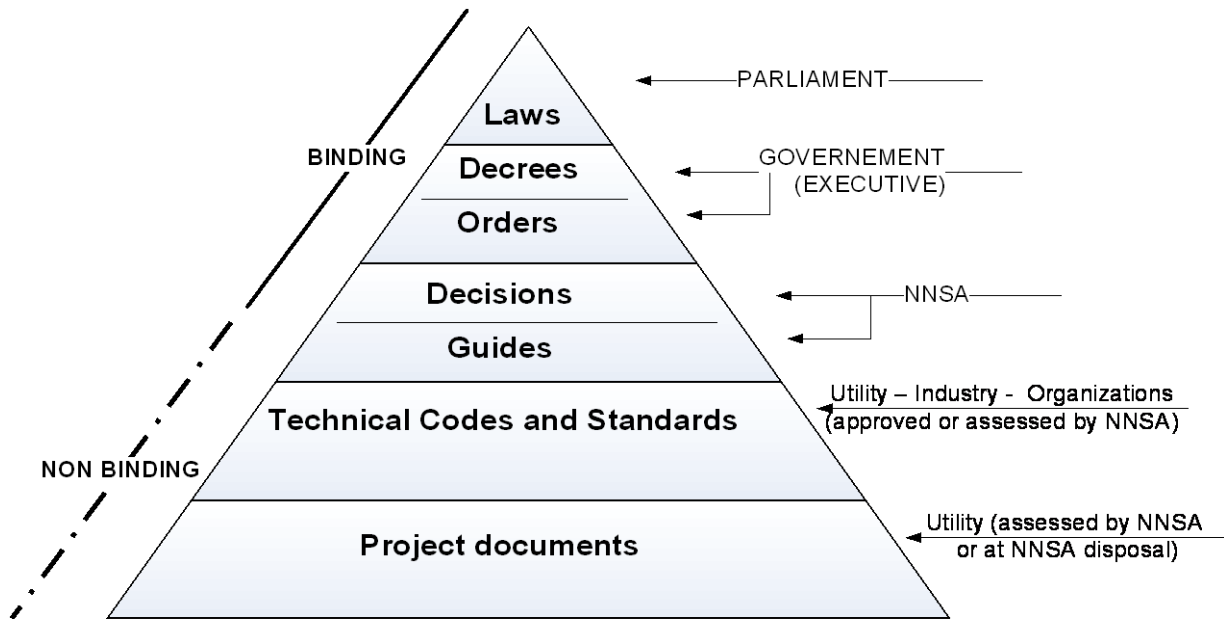


Figure 5: A regulatory pyramid

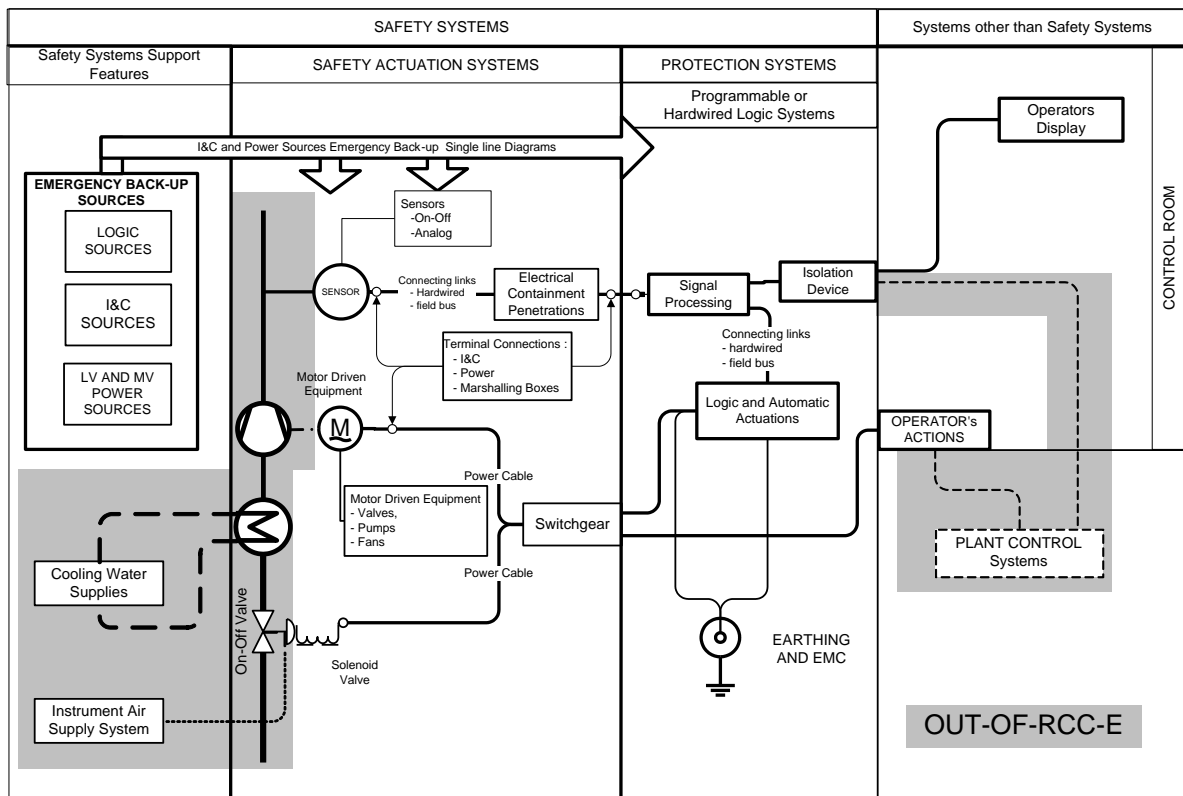


Figure 2 : Scope of RCC-E

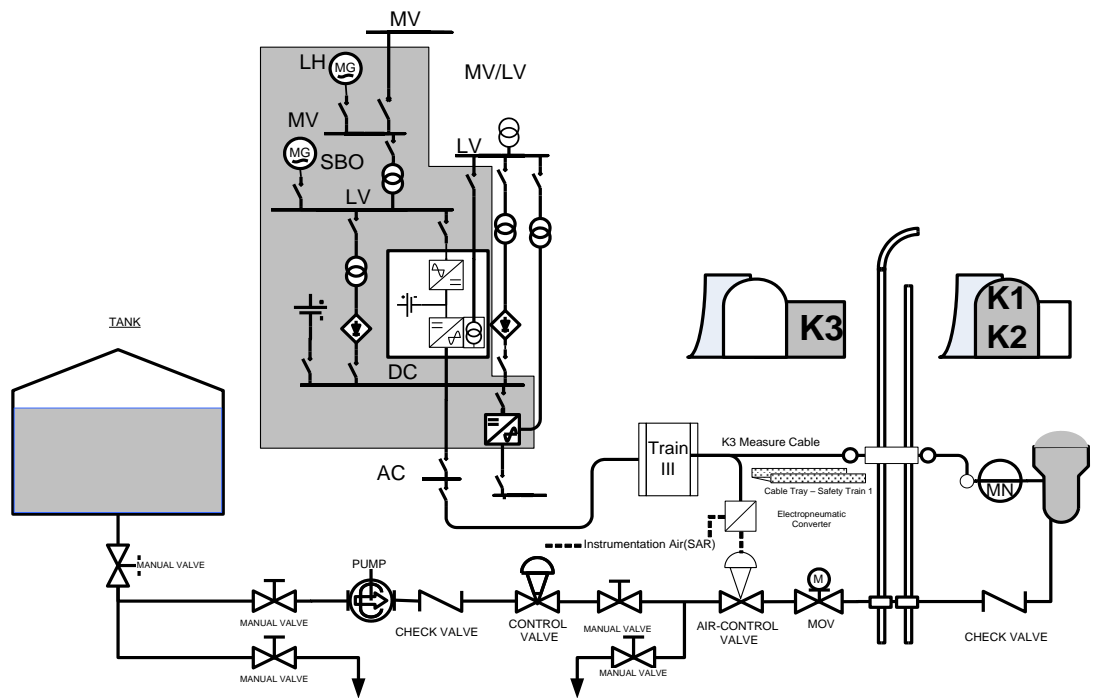



Figure 3: Establishing Qualification, list of qualified Equipment

afcen
Association Française pour les règles de conception, de construction et de surveillance en exploitation des matériels des Chaudières Electro-Nucléaires



ROBELSYS: Robustness provided by RCC-E in electrical systems

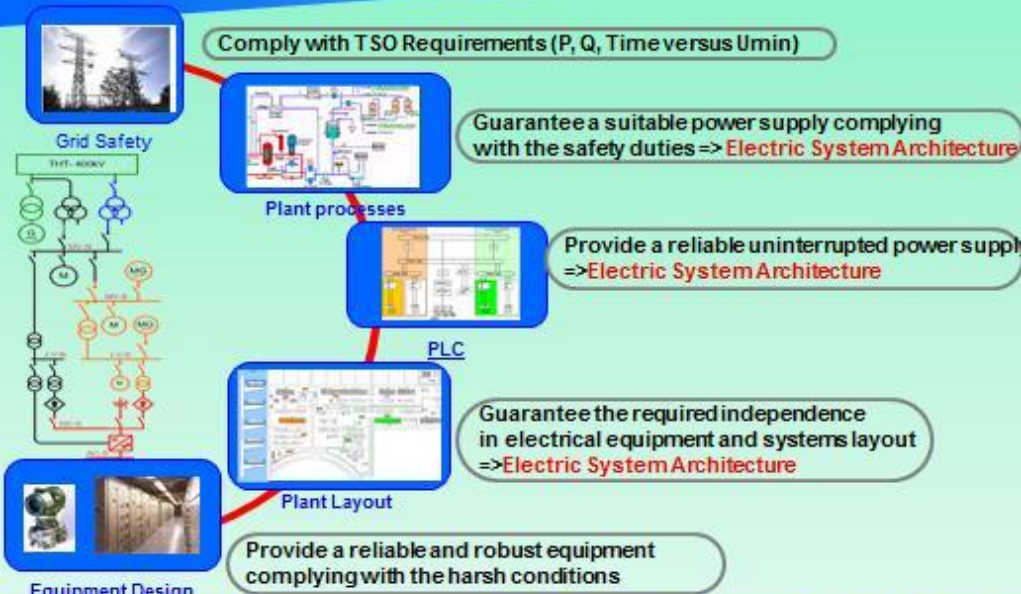
RCCE
Electrical and I&C systems, equipment and Layout – Design and Construction rules for Nuclear Islands
published in English, French, and Chinese
www.afcen.com

JM. HAURE – RCCE Chairman
Phone: +33 (0) 4 72 82 70 92
e-mail : jean-michel.haure@edf.fr
12-14 avenue Dutrievoz
F - 69628 Villeurbanne

ROBELSYS – April 2nd, 2014 – Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 1

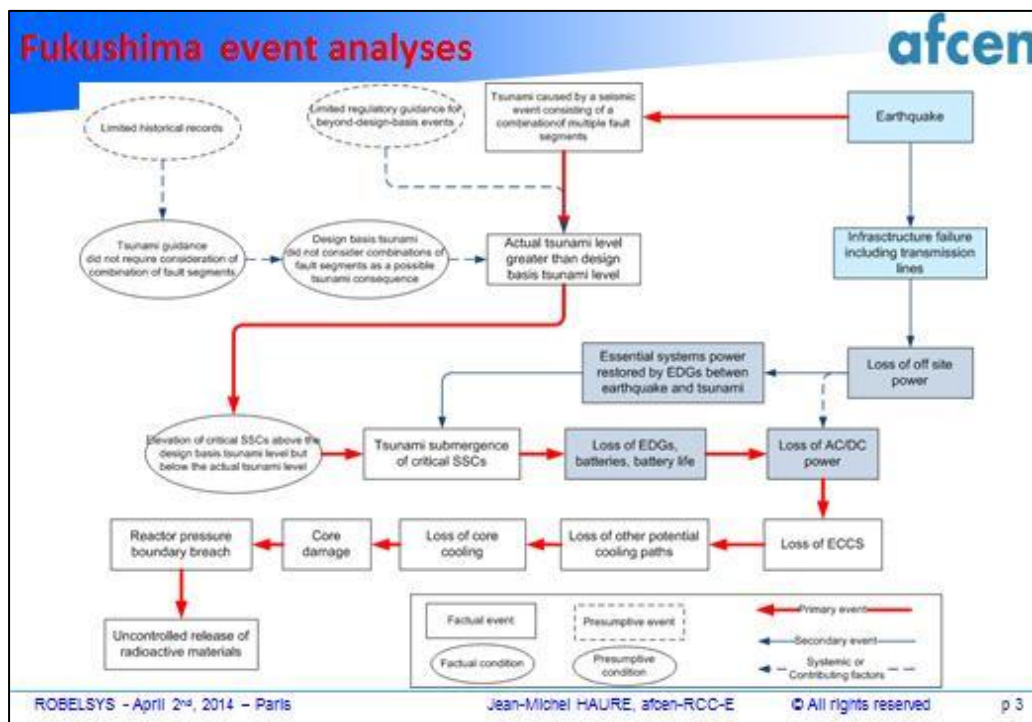
afcen

Robustness main challenges



- Grid Safety** (THT, 400kV): Comply with TSO Requirements (P, Q, Time versus U_{min})
- Plant processes**: Guarantee a suitable power supply complying with the safety duties => **Electric System Architecture**
- PLC**: Provide a reliable uninterrupted power supply => **Electric System Architecture**
- Plant Layout**: Guarantee the required independence in electrical equipment and systems layout => **Electric System Architecture**
- Equipment Design**: Provide a reliable and robust equipment complying with the harsh conditions

ROBELSYS – April 2nd, 2014 – Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 2




- ### Examples of measures taken
- ✓ **Flooding**
 - Water tightness: HVAC air intake, SBO/UDG and Battery rooms doors
 - Add requirements related to the hazards management and the layout
 - ✓ **Loss of power supplies**
 - AC/DC
 - Severe accidents batteries autonomy increase
 - Portable backup AC/DC sources
 - ✓ **Earthquake**
 - Equipment Seismic withstanding
 - Project specific
 - ✓ **Station Blackout**
 - EDGs and SBO diesels diversity
 - Number of SBO,
 - Fuel tank sharing,
 - Designed fixed connections towards the internal network
- ROBELSYS - April 2nd, 2014 - Paris | Jean-Michel HAURE, afcen-RCC-E | © All rights reserved | p 4



GRID REQUIREMENTS

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 5



ENTSOE requirements consequences

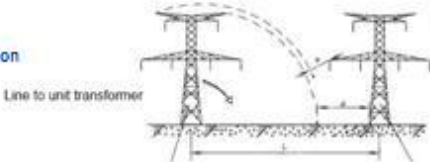
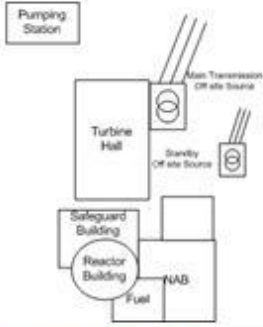
- Nuclear power plant (CI and NI parts) has to fulfill the requirements of the grid code,
 - i.e. the power production part and the auxiliary systems in CI and NI.
- Grid code frequency range requirements induces consequences on the design of
 - electrical systems;
 - fluid and safety systems;
 - reactor core design;
- Discussions shall be launched to define a fair agreement between Grid Operator, Safety Authorities and Plant designers

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 6

afcen

RCC-E Off site transmission lines independency requirements

- High reliability of the switchyard station
 - The collapsing of one tower
 - shall not impact the other transmission line.
 - Rotate towards the other line
 - Shall respect electrical distance
- High reliability of the connection to the switchyard station
 - The station transformer and the standby transformer connections of the same unit towards the switchyard shall
 - not be installed on a common tower or gallery.
 - have separate routes


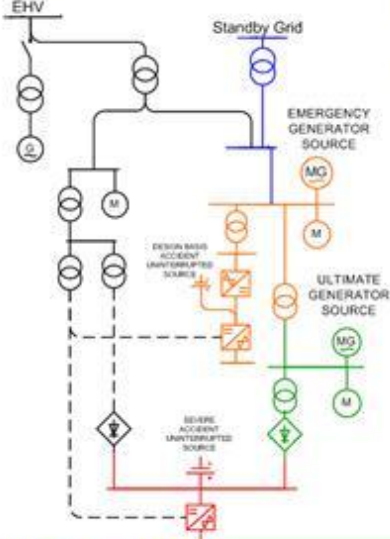
ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 7

afcen

ELECTRICAL SYSTEM ENGINEERING


ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 8

Robustness of electrical system

- ✓ Coordination of electrical parameters
 - Voltage, current and insulation
- ✓ Verification and validation of internal robustness
 - Circa 50Hz
 - Short-circuit, voltage transients with penalising load balances
 - Ferroresonance
 - Harmonics
 - Resupply by portable sources (fukushima)
 - High frequency phenomena
 - Overvoltages (lightning, surges)
 - Acceptance criteria
 - Variation of voltage in the defined tolerances
 - Breaking capacity of switchgear
 - Transformer reactances

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 11



Robustness to Electrical transient

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 12

General Unit Auxiliary Restart Sizing Case

EHV Short-circuit at terminal ends
C2133b

Failure of houseload operation & changeover from ST to AT
C2133b

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 13

Coordinations: Current and Voltage Levels

VOLTAGE COORDINATION

CURRENT COORDINATION

Sizing Cases

$0,95 U_{n} < U_{c} < 1,05 U_{n}$

D2300

$0,94 U_{n} < U_{c} < 1,04 U_{n}$


$0,94 U_{n} < U_{c} < 1,06 U_{n}$

$0,90 U_{n} < U_{c} < 1,06 U_{n}$

Related Equipment: Transformers, Motors, EDG, SBO, Cables, Switchboards, Switchgear, Batteries

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 14

Overvoltages

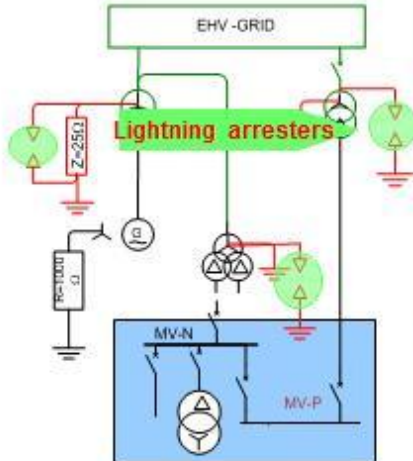


C2132

Fukushima

Lightning and switching impulse


- Limit Overvoltages in ST and AT by phase lightning arresters or spark gaps



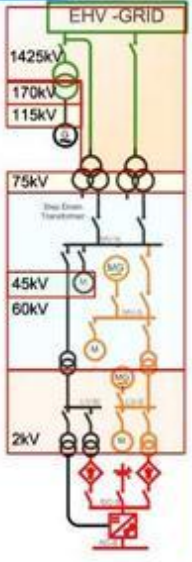
- **MV Networks Overvoltages**
 - MV Network are operated with an isolated neutral,
 - Overvoltages :
 - single-phase-to-earth faults,
 - switching impulses
- **Equipment must withstand these overvoltages.**
- **The switchgear is designed to limit switching impulse.**


ROBELSYS - April 2nd, 2014 - Paris
Jean-Michel HAURE, afcen-RCC-E
© All rights reserved
p 15


Insulation coordination




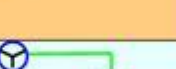
Transformer	
UTG	House load
	ST
MV	Normal Auxiliaries
	Backup Auxiliaries
LV ac	2kV
DC	

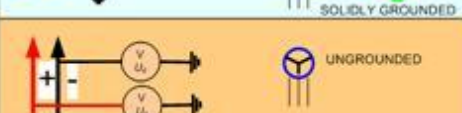












C2132

C2122

C2122

C2125

C2350

ROBELSYS - April 2nd, 2014 - Paris
Jean-Michel HAURE, afcen-RCC-E
© All rights reserved
p 16

afcen

ELECTRICAL EQUIPMENT ENGINEERING

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 17

Emergency Diesel Generator

afcen

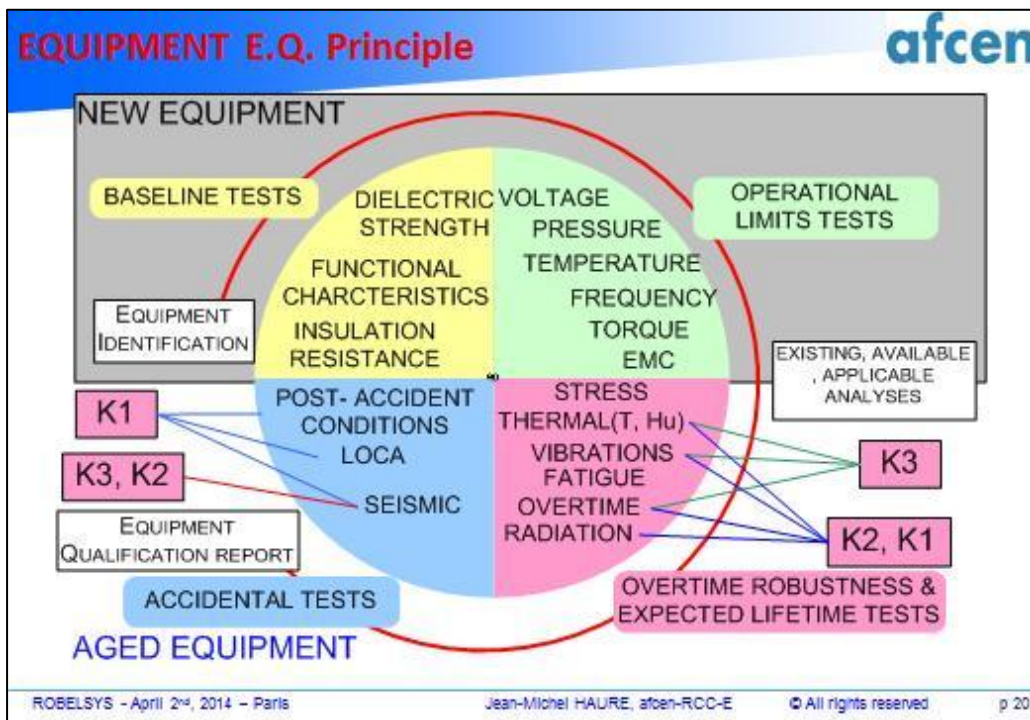
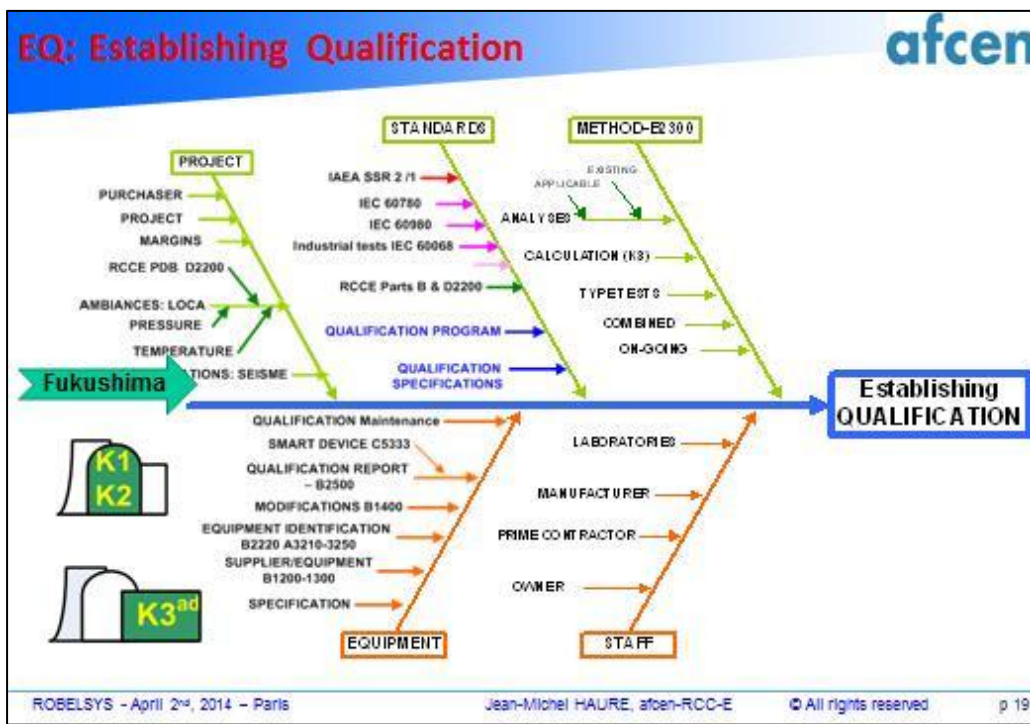
C2400

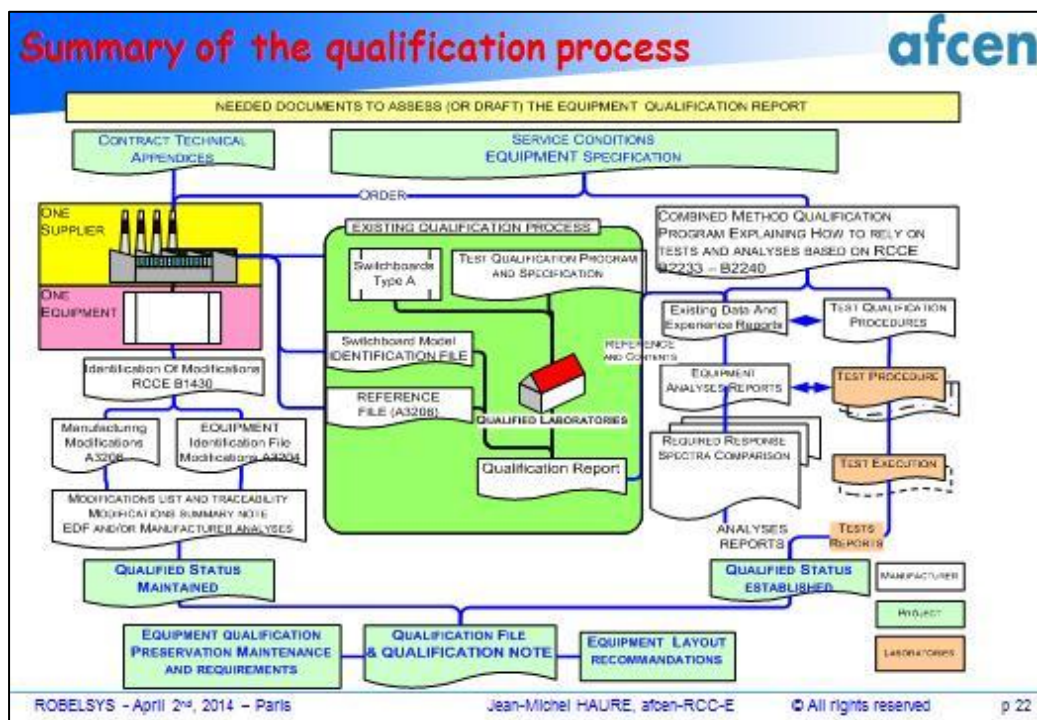
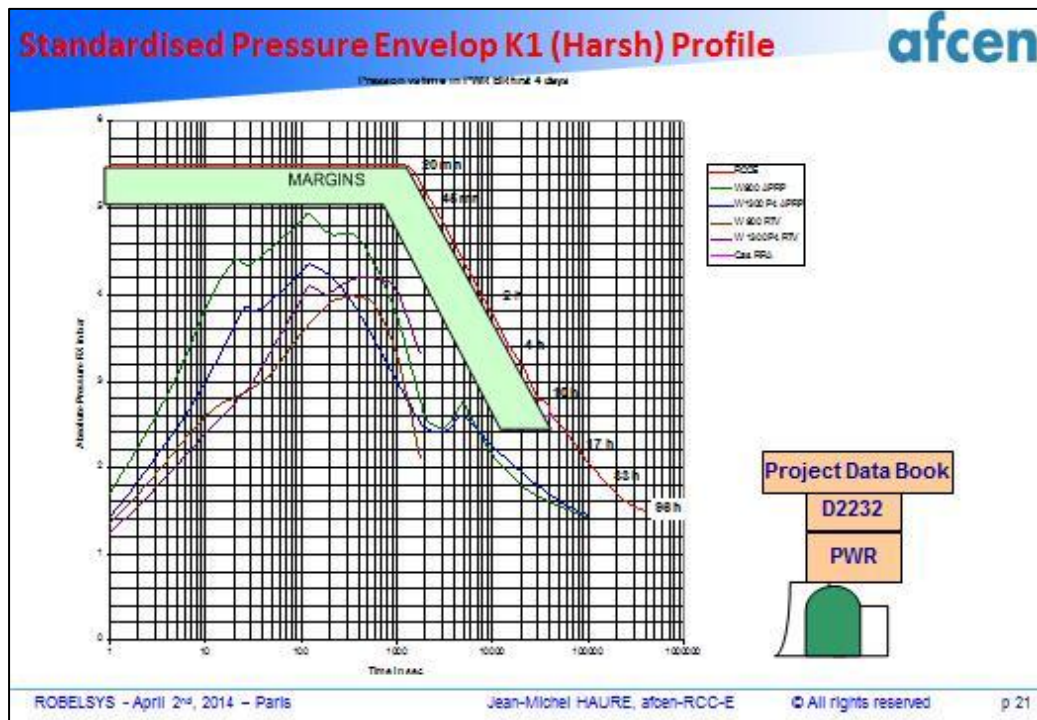
- ✓ Sizing and operational requirements
 - Power rating based on load balance for considered situations + 10% oversizing than worst case load
 - Fuel tank capacity allowing EDG to run for 3 days at full load
- ✓ Loss of off-site power
 - Automatic Start-up within ~15s
 - Sequentially loading of busbar and equipment
- ✓ Backup operations required protections
 - Protection against mechanical overspeed only
 - Other protections if need be, complying:
 - 2 out of 3 logic vote
 - Protect the generator unit from rapid deterioration
- ✓ Start-up and loading conditions, step available each 5s C2412

RCCE C2412-1:
0,6(T₂-T₁)

T ₁ =step _n	T ₂ =step _{n+1}
t > 0,95f _N	t > 0,98f _N
U > 0,75U _N	U > 0,90U _N

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 18





LAYOUT ENGINEERING

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 23

Independency: Electrical and functional separation

EVENTS

- SAR
- External Hazards
- Internal Hazards

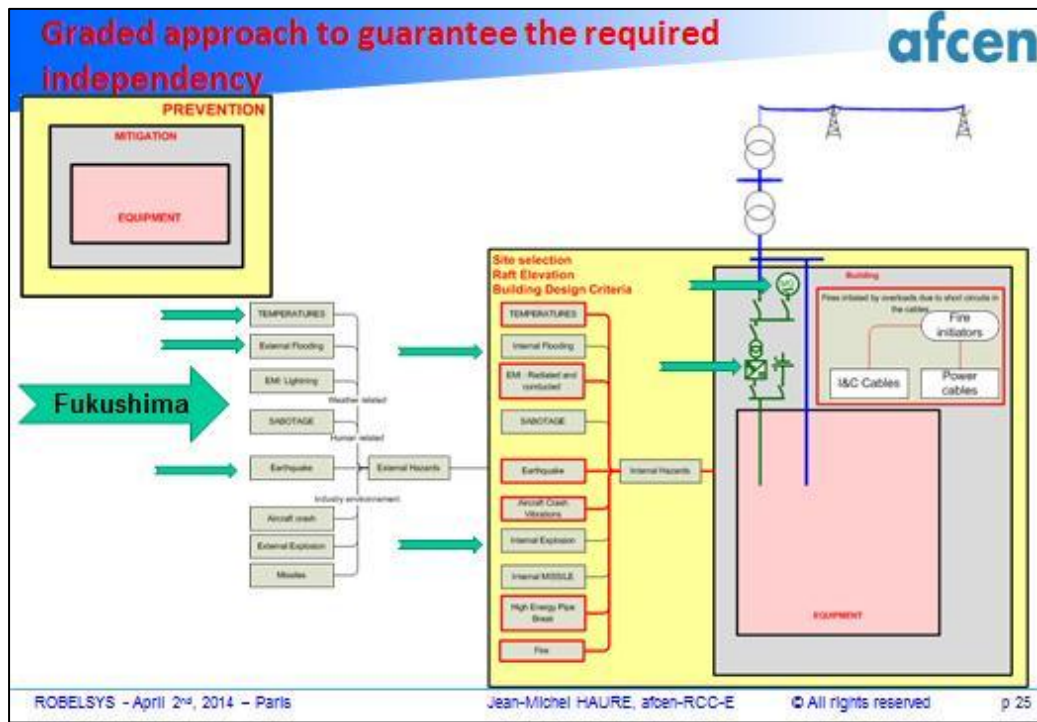
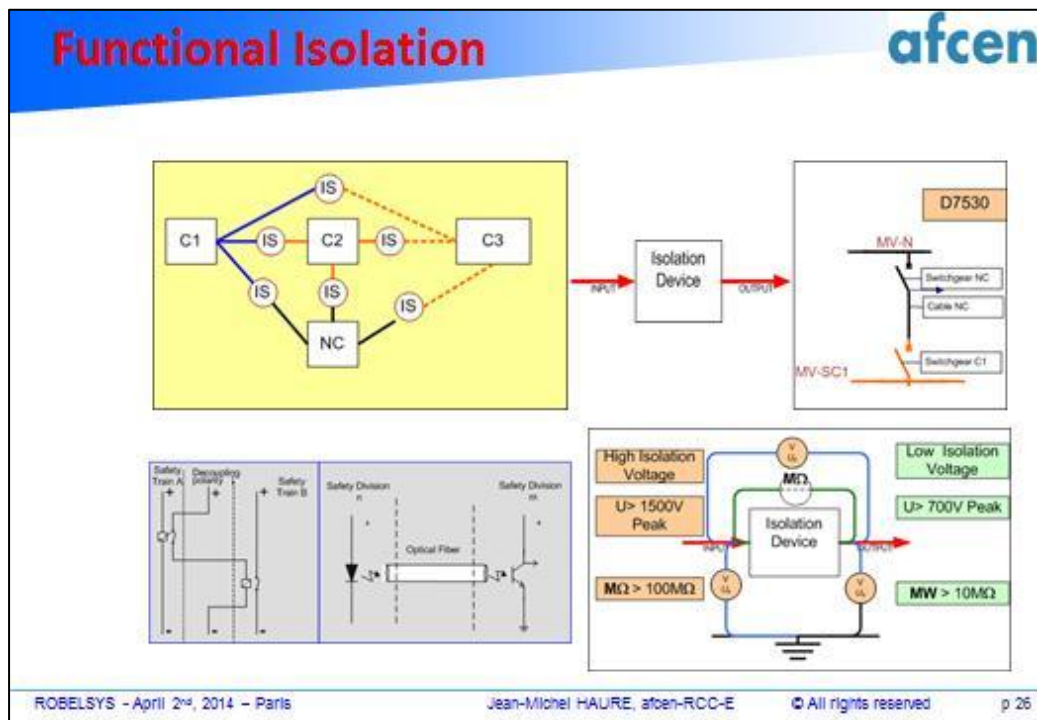
MITIGATION

- Segregation between safety divisions and as regards to Fire
- Safety Division n
- CI class (p) C) class
- Isolation devices
- Safety Classes Isolation
- EMI
- Electrical Separation
- Cable Trays in the Same Plan
- Parallel Cable Trays
- Cable Trays Crossover

PLANT → **TRAINS** → **TRAIN** → **CABLEWAY**

D7400 **ROBUST DESIGN**

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 24



ROBELSYS - April 2nd, 2014 - Paris
Jean-Michel HAURE, afcen-RCC-E
© All rights reserved
p 25


Summary **afcen**

- ✓ **RCC-E is a high level document that**
 - **provides a comprehensive set of requirements on**
 - Grid connection and transmission lines
 - Plant step-down transformers
 - Internal Interruptible and uninterruptible network and power sources
 - The validation and verifications analyses
 - Equipment design and environmental qualification
 - Layout engineering
 - Suitable documentation
 - **Provides confidence to the users, robustness to the design and construction processes**
 - **In other words you**

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 27

CAN RELY ON RCCE **afcen**



AFCEN thanks you for your attention and hope welcoming you in RCC-E committee

Thank You,
Merci

Topic Open for Question

JOIN AFCEN: www.afcen.com
JM. HAURE - RCCE Chairman
Phone: +33 (0) 4 72 82 70 92
e-mail: jean-michel.haure@edf.fr
12-14 avenue Dutrievoz
F - 69628 Villeurbanne

ROBELSYS - April 2nd, 2014 - Paris Jean-Michel HAURE, afcen-RCC-E © All rights reserved p 28

Overall strategy and architecture for Post-Fukushima-mitigation and mitigation on other events in the Electrical System

Waldemar Geissler
AREVA GmbH
Paul-Gossen-Str. 100
91052 Erlangen, Germany

Abstract

1. INTRODUCTION

In NPPs the Electrical System is an auxiliary system which has to deserve other systems important for safety and/or operation like fluid systems, HVAC etc.

A few events during the last years have nevertheless pointed out the crucial importance of this auxiliary system “Electrical System” for the safety of the plant.

The main events are:

- Forsmark 1
- Fukushima Daiichi
- Byron 2
- Forsmark 3

The difference between the other events and the Fukushima-event relating to the Electrical System is the high degree of physical destruction which has not allowed a fast restoration of the power supply in Fukushima.

In the proposed presentation the different events are shortly presented in the field of electrical Ssystems and possible or foreseen countermeasures are also shown.

2. MAIN CONTENT

The presentation will show the following main parts:

- Definition of the main external and internal hazards affecting the Electrical Systems
- Short presentation of Forsmark and Byron events and selected or possible countermeasures
- Considered events (Design Extension Conditions):
 - i. Long Term LOOP
 - ii. Long Term SBO
 - iii. Extended Loss of AC power
 - iv. Combination of events
- The DEC conditions are considered in power and shutdown states of the plant

- Approach based on fixed (non-mobile) installed equipment
- Connection of mobile power sources in the long term phase (after 7 days)
- Conclusions

In more detail the following will be presented:

I. Electrical transients

a) Forsmark 1:

This topic was already treated in the frame of DIDEISYS and will be presented very shortly

b) Byron 2:

Phase interruption due to the break of an insulator in an 345-kV-switchyard. The failure was not detected by the installed measuring system and the EPS-Diesels not started.

c) Forsmark 3:

During the plant outage and the power supply from the main grid via main transformer and auxiliary transformer the HV circuit breaker was opened in two phases only, due to a loose cable connection. Caused by the low currents in the outage phase installed protection devices were not activated. A Station-Black-Out of 26 minutes occurred before the situation was detected in the MCR and the EPS-Diesels started by interruption of the power supply of the EPSS.

d) Technical background and possible countermeasures referring Byron 2 and Forsmark 3:

The influence of transformer connection groups and measuring concepts for EPS-Diesel-starts will be presented.

II. PWR Plant state and restoration of power supply

e) The different power states will be defined in the frame of the Fukushima event:

The power states like Long Term LOOP, Long Term SBO and Loss of AC power will be presented and countermeasures will be shown.

III. Conclusion

f) Conclusion

A general conclusion referring the robustness of Electrical Systems will be shown, especially for the example of the EPR.

3. SUMMARY

The aim of the presentation is to give an general overview over the architecture of the Electrical System in an NPP under consideration of design extension events. The robustness of the Electrical Systems can be verified in this way.

Overall strategy and architecture for Post-Fukushima-mitigation and mitigation on other events in the Electrical System

Waldemar Geissler
AREVA GmbH, Germany

1. Introduction

The Electrical System of a Nuclear Power Plant has a crucial role for the safety of the NPP.

During the last years a few events have shown the vulnerability of the Electrical System referring to external hazards, from the electrical grid and also from natural phenomena.

The main events are:

- Forsmark 1
- Fukushima Daiichi
- Byron 2
- Forsmark 3

Forsmark 1 was treated in the frame of other workshops, therefore the phase interruptions in case of Byron 2 and Forsmark 3 and also the external hazard in case of Fukushima will be treated in this document.

2. Main non-electrical hazards affecting electrical power supply

The main non-electrical hazards which affects the Electrical Power Supply System are:

- Earthquake
- Flooding
- Fire
- Wind and Tornado
- Other extreme weather conditions (e.g. snow, icing, sandstorm...)
- Explosion waves
- Air Plane Crash

The electrical hazards are shown in a separate chapter of this document.

As the Fukushima event and his consequences are generally well known, this will not be handled in this document.

In the next chapter are shown measures in case of beyond-design-accidents, which could be the result of an event like in Fukushima.

3. Post Fukushima – main scenario considered for electrical power supply

The main scenario considered for the Electrical Power Supply System in the frame of the Post-Fukushima investigations are:

- Loss of Offsite Power (LOOP) / Loss of Preferred Power - DBC event, duration: 72 h
- Station Black Out (SBO) – DEC-A event, duration: 24 h
- Long Term LOOP – beyond design, duration > 72 h
- Long Term SBO – beyond design, duration > 24 h
- Extended/Total Loss of AC Power (ELAP) – Grids, EDG, SBO/AAC power sources not available, only the battery buffered DC and AC electrical systems are in operation

Remark: Modern power plants fulfill the DBC- and DEC-requirements (LOOP and SBO), therefore this is not treated in the presentation.

3.1 Long Term LOOP > 72 h

Boundary conditions: LOOP, On-site power sources available (EDG and SBO, also UPS systems)

- EDG has be designed for 72 h continuous operation, SBO for 24 h
- In case of Long Term LOOP the operation of the on-site-power-sources is required to cool the core.
- After a time load shedding of fluid system loads (redundant design) in order to not consume too much fuel.
- Possibilities to increase the fuel as additional tanks or connections between tanks and refilling opportunities.

3.2 Long Term SBO > 24 h

Boundary conditions: LOOP and loss of EDG's, SBO available, also UPS systems

- SBO has be designed for 24 h continuous operation.
- In case of Long Term SBO the operation of the SBO DG is required.
- Load shedding in order to reduce the fuel consumption (redundant systems).
- Possibilities to increase the fuel as additional tanks or connections between tanks and refilling opportunities.

Remark: Fuel tanks are designed for operation with rated load. As the balanced load is generally lower, the SBO fuel tank has a safety margin (operation > 24 h possible).

3.3 Extended/Total Loss of AC Power > 2 h

Boundary conditions: LOOP, On-site power sources not available (EDG and SBO), only battery buffered DC and AC systems available)

- For this beyond design scenario different possibilities to handle for Electrical Systems are imaginable, e.g. use of fixed or mobile power sources at defined switchboards.
- Use of non-electrical power sources for defined functions

For the connection of mobile power sources precautionary measures are recommended.

- Installation of dedicated cabinets in the switchgears.
- Pulling of cables
- Installation of fixed connectors
- Holes in the walls of the buildings, closed in normal cases, as shown in the next picture



3.3 Resume and recommendations

The following conclusions can be drawn:

- For these beyond design scenarios different Defense in Depth lines are necessary.
- The site and buildings of the NPP have to be selected and executed accordingly:
 - The site should be located or protected in such a way that external hazards as flooding have a low probability.
 - The buildings with safety equipment shall be designed and build protected against earthquake and tight in case of flooding, also other hazards as explosion waves or air plane crash should be considered.
- For special measures like connection of mobile power sources precautionary measures should be installed.
- Accident manuals should be adapted and the staff has to be trained for these measures.
- Supply of electrical power is not enough, the process systems and I&C have to be also operable to prevent core melt.

4. Main electrical hazards affecting electrical power supply

The main electrical hazards which affects the Electrical Power Supply System are:

- a) Fast transients
 - Direct and indirect lightning strikes
 - Switching
 - Arcing faults
 - Transmission line phenomena
 - Resonance phenomena
 - Electromagnetic Pulse phenomena
 - Geomagnetic Induced Currents (GIC)

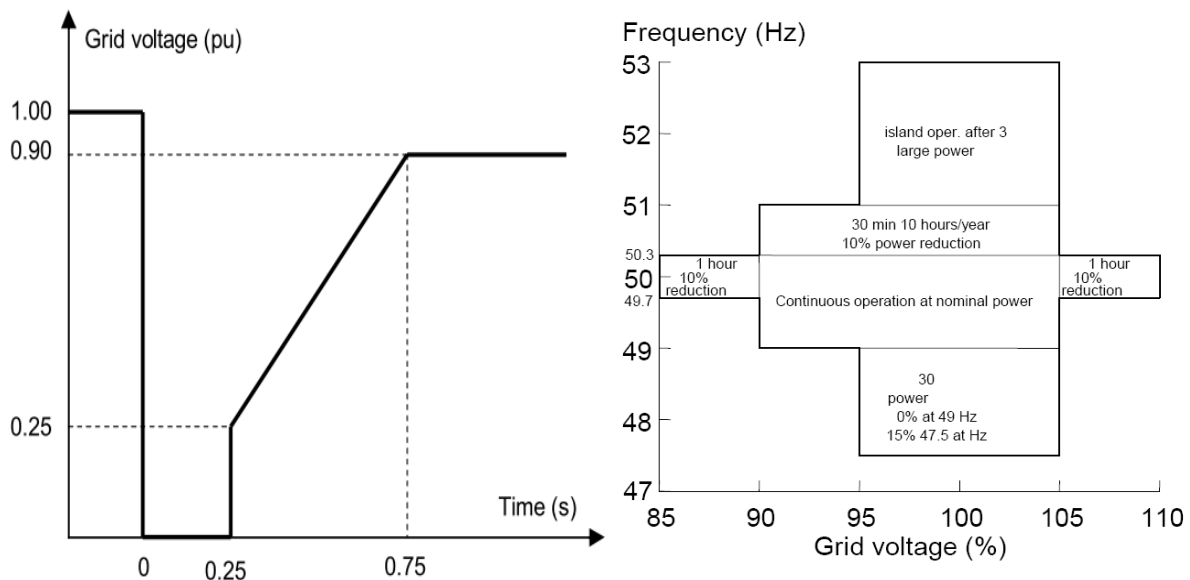
- b) Other failures
 - Earth faults
 - Phase interruptions

4.1 Voltage and frequency variations

Failures in Electrical Systems cause generally variations of voltage and frequency.

- a) Slow voltage variations:
 - Caused by missing or excess reactive power in the grid, large load flows, faulty voltage control equipment in the grid.
 - Compensation by using of on-load tap changer for the step-up and auxiliary (normal, emergency and standby) transformers or should be handled by the automatic voltage regulator (AVR) of the main generator
- b) Fast/transient voltage variations:
 - Caused by short-circuits, switch-over, lightning strikes, transition to houseload operation. Range between 1ms to seconds.
 - No compensation by active measures, equipment has to be designed for such phenomena or protected against them
- c) Frequency variations:
 - Caused generally by missing or excess active power.
 - Several defense lines in the grid and in the plant, e.g. transition to houseload operation. Can not easily be compensated.

An example of defined voltage and frequency limits and variations in case of an FRT (fault ride trough) is shown in the next figures:



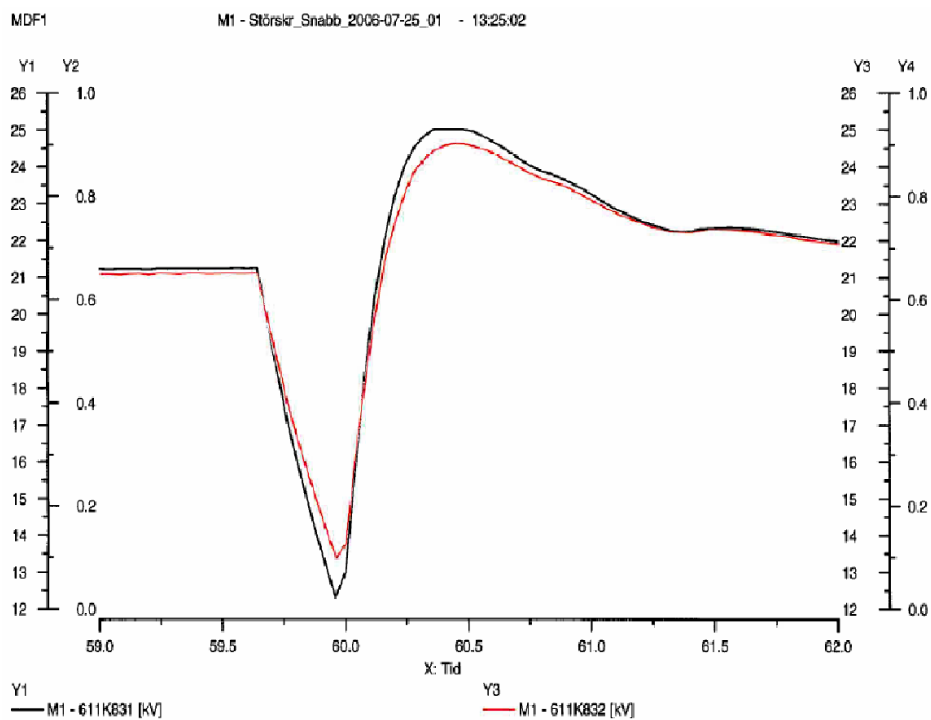
Source: NORDEL

Voltage and frequency variations are also caused by failures which are not “standardized” in grid codes. These failures are:

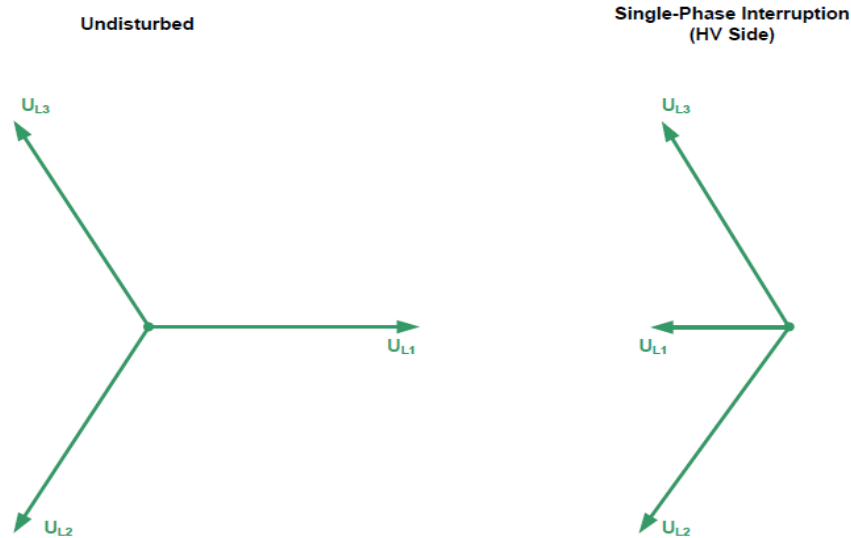
- d) Fast transients
- Direct and indirect lightning strikes
 - Switching
 - Arcing faults
 - Transmission line phenomena
 - Resonance phenomena
 - Electromagnetic Pulse phenomena
 - Geomagnetic Induced Currents (GIC)
- e) Other failures
- Earth faults
 - Phase interruptions

Examples of this type of failures are shown in the next two figures:

Voltage transient in Forsmark 1:



Phase interruption – single phase interruption on the HV side:



4.2 Cases of phase interruptions – Byron 2 and Forsmark 3

Byron 2 event.

During power operation in Byron 2:

- January 30th, 2012 at Byron Unit 2, USA
 - The C-Phase broke, resulting in a Phase C open circuit and a high impedance ground fault
 - Open phase condition and resulting voltage unbalance – unit protective relaying was not designed to detect
 - Reactor trip and finally the control room operators detected the failure and tripped the breakers to separate unit buses from offsite power sources, in order to initiate EDG automatic start and operation
- EDG start is initiated by a voltage measurement in a two-out-of-two-logic, not met in this case

Forsmark 3 event.

During the outage in Forsmark 3:

- only one (of two) external busbars connected to the plant because of maintenance on the external grid switch yard.
- The alternative power source was disconnected because of change to a new 70 kV switch yard (This operating conditions is only allowed during outage)
- On the 30th of May 2013 the plant circuit breaker to the 400 kV grid was disconnected in two phases only, due to a loose cable connected to one of three poles for the breaker tripping device. Breaker failure protection not activated due to low current (limit not reached).
- No start of the EDG's (two-out-of-three-logic at 65%Ur) because limiting values were not reached (Main and auxiliary transformers have a Y/Δ-connection and the star-point ist grounded).
- Voltage measurement for the MCR between L1 and L2 only: value ok, no alarm.

- After 20 minutes the operators separated manually the safety busses from the external grid, after them automatic start of the Diesels and supply of the safety busses.
- Equipment on safety and non-safety busbar with protection for “phase-disconnection” stopped automatically. Electrical machines lacking protection for “phase-disconnection” did not stop and some of them get minor damages.

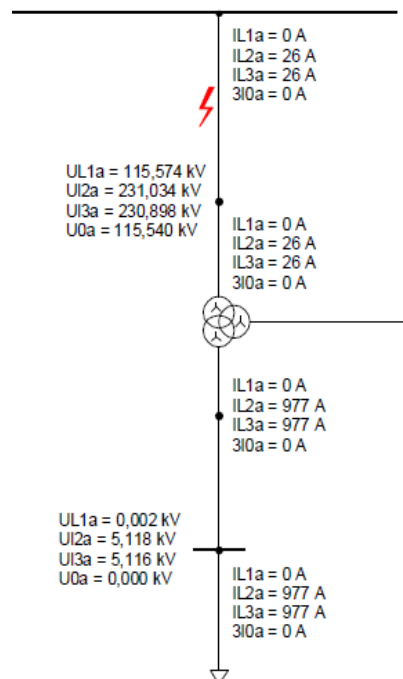
5. Considerations in principle, based on a one-phase-interruption (Byron)

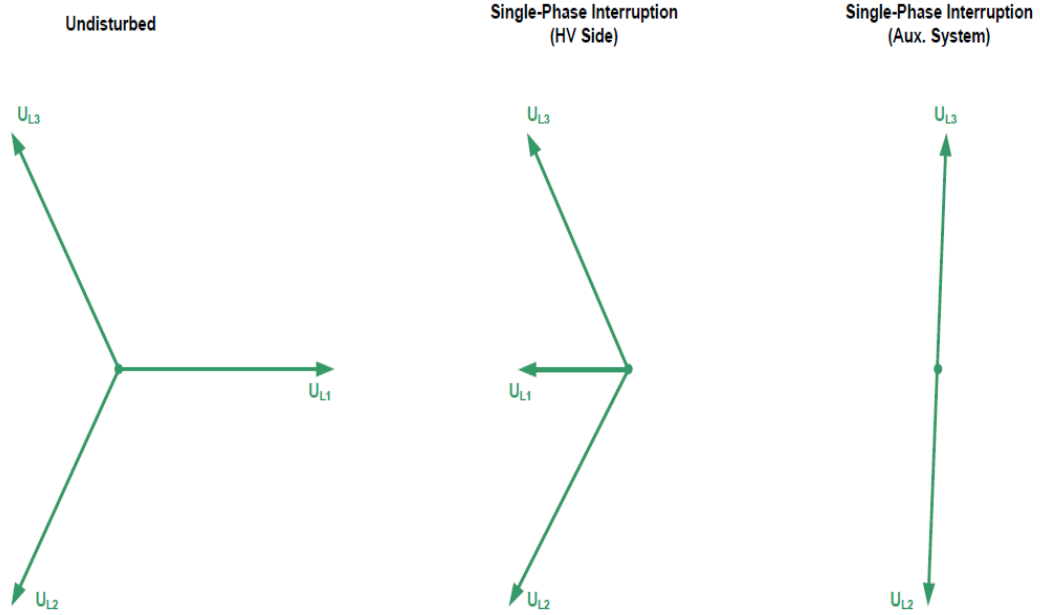
In this chapter are described main influence factors referring the consequences of a phase interruption on the HV side of an Unit Auxiliary Transformer.

The following boundary conditions have to be considered:

- Connection of the Unit Auxiliary Transformer (on the Insulated Phase Busduct or on the HV grid) has an significant importance.
- Open phase transmission over the main, auxiliary or standby transformers depends on the transformer vector group: Yy, Δy, Yd, etc. and the secondary side loading conditions
- Grounding of the transformers (or not) has an significant influence
- Loading conditions of the plant (power operation, outage etc.) has a significant influence
- Start conditions for the Emergency Diesels (e.g. 2of2 or 2of3 measurement, at 80%U_r, at 65% etc.).

a) Voltage in the unit in case of an Unit Auxiliary Transformer with a Y/Y-connection, not grounded.

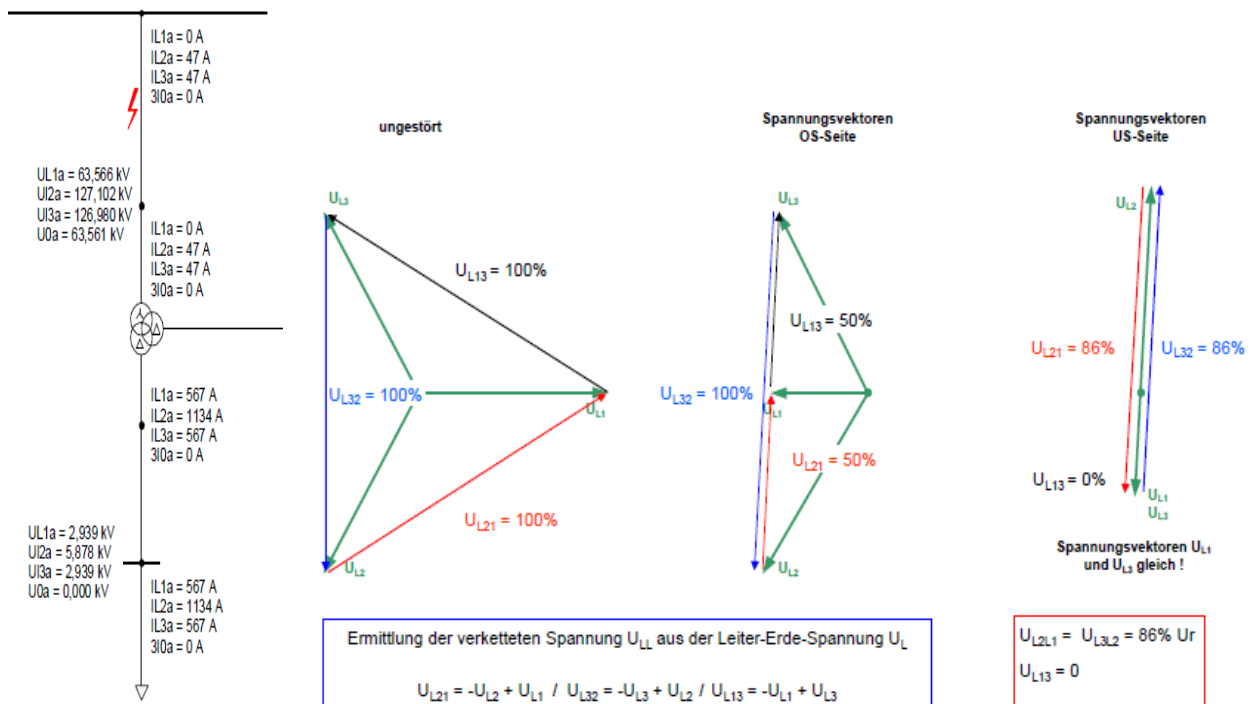




- One phase in the system has voltage 0(zero)
- Phase angle between the two remaining phases changed from 120° to 180°
- Voltage measurement 2of3 would start the Emergency Diesel Generator

Remark: Other treatment of the transformer Y-point (e.g. solid grounding) would produce other results. Furthermore motors in operation would have an influence.

b) Voltage in the unit in case of an Unit Auxiliary Transformer with a Y/ Δ -connection, not grounded.



- No phase in the system has voltage 0(zero)
- Phase angle between the phases changed from 120° to 180° (for L1-L2 and L2-L3) and 0° (for L2-L3)
- Due to the angle shift two voltage values would be 86% U_r (>80% U_r)
- Voltage measurement 2of3 with limit <80% U_r would not start the EDG

Remark: Other treatment of the transformer Y-point (e.g. solid grounding) would produce other results. Furthermore motors in operation would have an influence.

Open phase detection – Resume:

- Connection type of the Unit Auxiliary System is important (via generator transformer or direct on the HV-grid)
- Open phase transmission over the auxiliary and standby transformers depends on the transformer vector group: Yy, Δy etc., the Y-point-grounding and secondary side loading conditions.
- Influence of running motors (load conditions) is high.

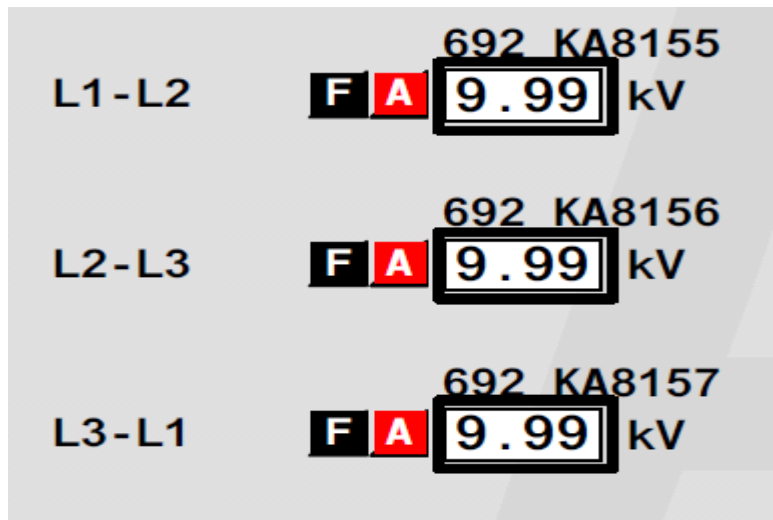
Statement: No general applicable solution is available. Detailed investigations to be done for each plant.

- Electrical Protection:
 - Individual equipment protection, e.g. out-of-balance-protection for motors
 - Digital protection devices for negative sequence measurements could detect the failure. Setting values are challenging.

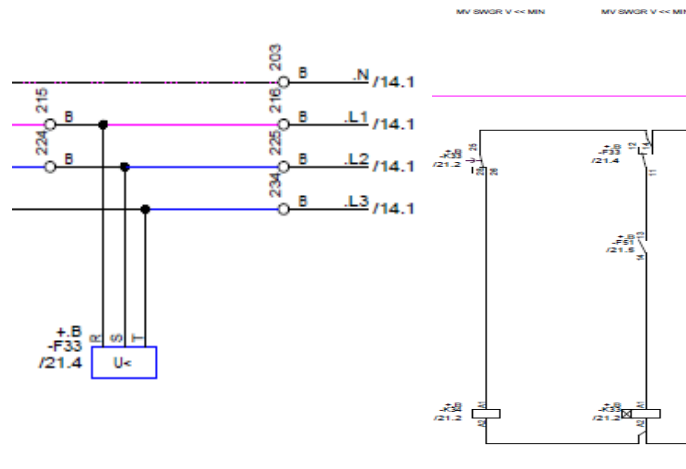
6. Improvements in power plants, without consideration of deeper electrical calculations

In this chapter are described improvements, which do not require deeper investigations in the area of electrical calculations and protection settings.

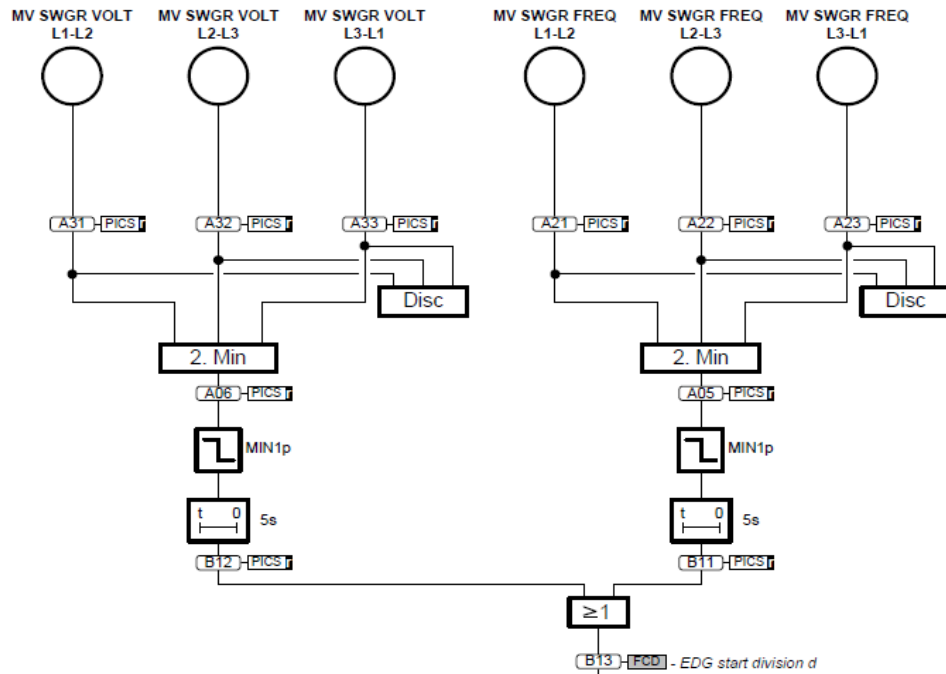
- Show all voltages in the Main Control Room, all the time



- For alarms: Use a type of measurement that all voltages are monitored



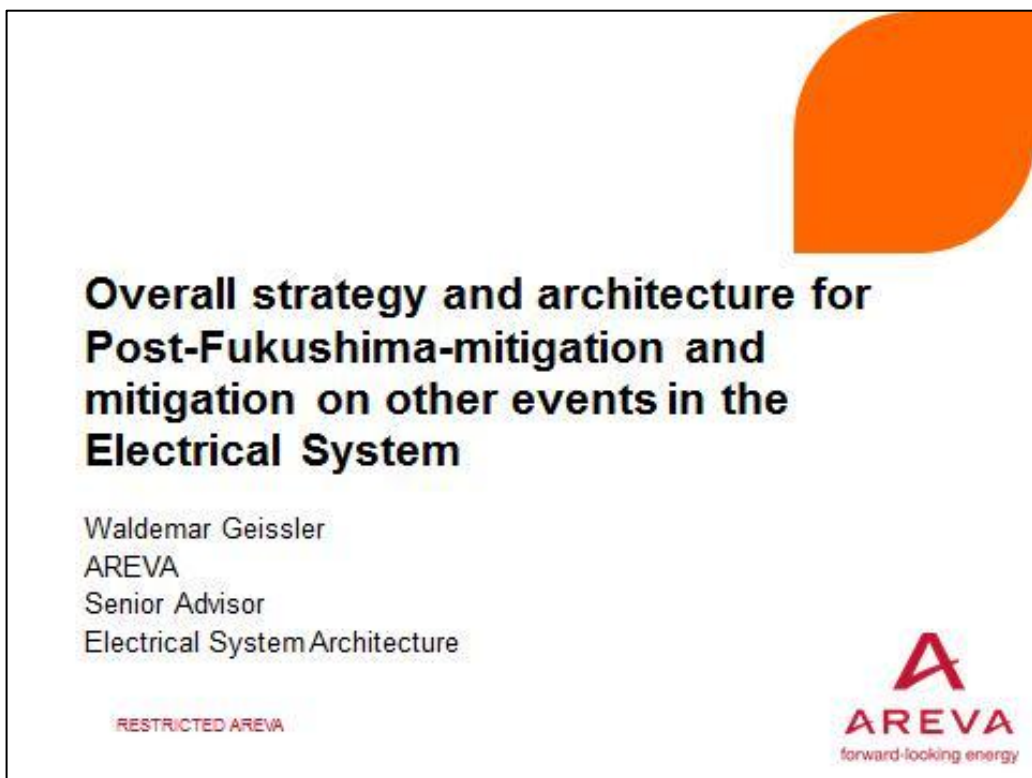
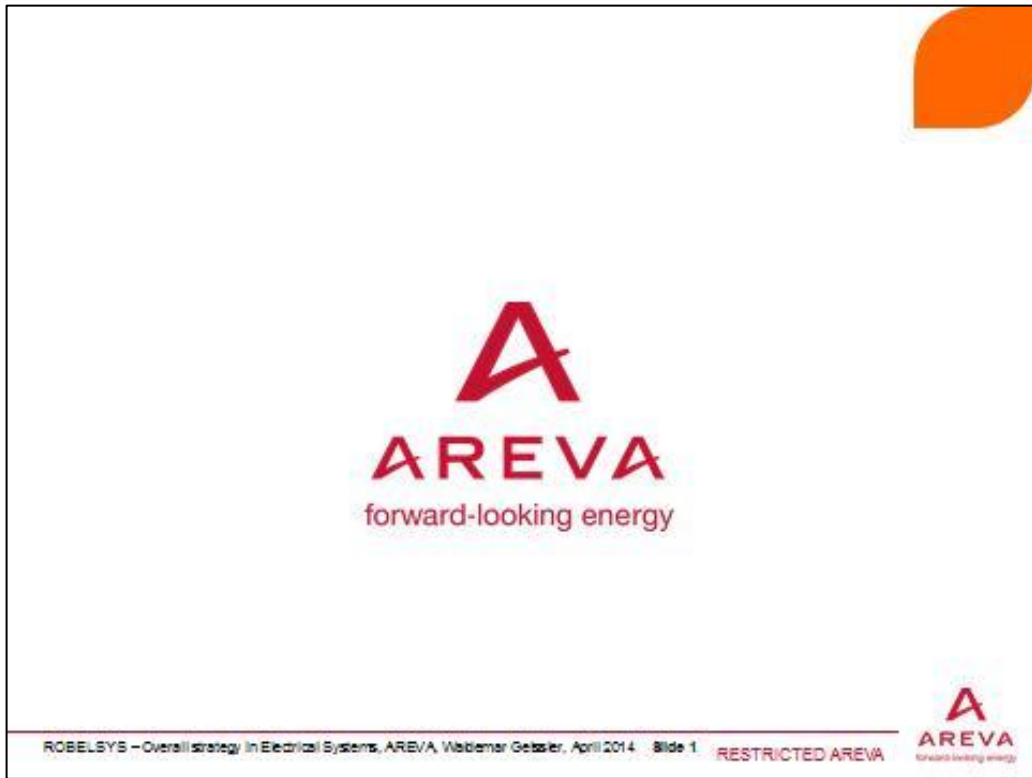
- Use for the automatic start of the Emergency Diesels 2of3 instead 2of2 measurements. Divers measurement to the voltage, e.g. frequency, could also be considered



7. Summary

The following can be summarized:

- Electrical Power Supply System is a supporting system, but the availability and the robustness of the electrical system is of major importance for the safety of the plant.
- Independently from the plant concept, a robustness analysis should be done, considering hazards and electrical transients.
- Robustness against CCF of support systems – analysis should assess the cliff edge effect of unexpected events through ALARP



Content

- ▶ **Main non-electrical hazards affecting Electrical Power Supply**
- ▶ **Post-Fukushima – Main scenarios considered for Electrical Power Supply**
- ▶ **Main electrical hazards affecting Electrical Power Supply**
- ▶ **Considerations in principle, based on a one-phase-interruption**
- ▶ **Improvements in power plants, without consideration of deeper electrical calculations**
- ▶ **Summary**

ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wabtemar Gelsler, April 2014 Slide 3

RESTRICTED AREVA



Main non-electrical hazards affecting Electrical Power Supply

RESTRICTED AREVA



Hazards with influence on the Electrical Power Supply

► Non-electrical hazards:

- ◆ Earthquake
- ◆ Flooding
- ◆ Fire
- ◆ Wind and Tornado
- ◆ Other extremeweather conditions (e.g. snow, icing, sandstorm...)
- ◆ Explosion waves
- ◆ Air Plane Crash

► Electrical hazards:

- ◆ Presented in a following chapter

Post Fukushima – Main scenarios considered for Electrical Power Supply

Events considered after Fukushima for Electrical Systems

- ▶ Loss of Offsite Power (LOOP) / Loss of Preferred Power - DBC event, duration: 72 h
- ▶ Station Black Out (SBO) – DEC-A event, duration: 24 h
- ▶ Long Term LOOP – beyond design, duration > 72 h
- ▶ Long Term SBO – beyond design, duration > 24 h
- ▶ Extended/Total Loss of AC Power (ELAP) – Grids, EDG, SBO/AAC power sources not available, only the battery buffered DC and AC electrical systems are in operation

Remark: Modern power plants fulfill the DBC- and DEC- requirements (LOOP and SBO), therefore this is not treated in the presentation.

Long Term LOOP > 72 h Enhancement of onsite power supply

Boundary conditions:

LOOP, On-site power sources available (EDG and SBO, also UPS systems)

- ▶ EDG has been designed for 72 h continuous operation, SBO for 24 h
- ▶ In case of Long Term LOOP the operation of the on-site-power-sources is required to cool the core.
- ▶ After a time load shedding of fluid system loads (redundant design) in order to not consume too much fuel.
- ▶ Possibilities to increase the fuel as additional tanks or connections between tanks and refilling opportunities.

Long Term SBO > 24 h

Boundary conditions:

LOOP and loss of EDG's, SBO available, also UPS systems

- ▶ SBO has be designed for 24 h continuous operation.
- ▶ In case of Long Term SBO the operation of the SBO DG is required.
- ▶ Load shedding in order to reduce the fuel consumption (redundant systems).
- ▶ Possibilities to increase the fuel as additional tanks or connections between tanks and refilling opportunities.

Remark: Fuel tanks are designed for operation with rated load. As the balanced load is generally lower, the SBO fuel tank has a safety margin (operation > 24 h possible).

Extended/Total Loss of AC Power > 2 h

Boundary conditions:

LOOP, On-site power sources not available (EDG and SBO), only battery buffered DC and AC systems available)

- ▶ For this beyond design scenario different possibilities to handle for Electrical Systems are imaginable, e.g. use of fixed or mobile power sources at defined switchboards.
- ▶ Use of non-electrical power sources for defined functions.

Connection of mobile power sources

- ▶ For the connection of mobile power sources precautionary measures are recommended.
 - ◆ Installation of dedicated cabinets in the switchgears.
 - ◆ Pulling of cables
 - ◆ Holes in the walls of the buildings, closed in normal cases



ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessner, April 2014 Slide 11

RESTRICTED AREVA




Resume and recommendations

- ▶ For these beyond design scenarios different Defense in Depth lines are necessary.
- ▶ The site and buildings of the NPP have to be selected and executed accordingly:
 - ◆ The site should be located or protected in such a way that external hazards as flooding have a low probability.
 - ◆ The buildings with safety equipment shall be designed and build protected against earthquake and tight in case of flooding, also other hazards as explosion waves or air plane crash should be considered.
- ▶ For special measures like connection of mobile power sources precautionary measures should be installed.
- ▶ Accident manuals should be adapted and the staff has to be trained for these measures.
- ▶ Supply of electrical power is not enough, the process systems and I&C have to be also operable to prevent core melt.

ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessner, April 2014 Slide 12


RESTRICTED AREVA






Main electrical hazards affecting Electrical Power Supply

RESTRICTED AREVA




AREVA
forward-looking energy



Voltage and frequency variations and transients from “undefined” grid failures

- ▶ **Fast transients**
 - ◆ Direct and indirect lightning strikes
 - ◆ Switching
 - ◆ Arcing faults
 - ◆ Transmission line phenomena
 - ◆ Resonance phenomena
 - ◆ Electromagnetic Pulse phenomena
 - ◆ Geomagnetic Induced Currents (GIC)
- ▶ **Other failures**
 - ◆ Earth faults
 - ◆ Phase interruptions

ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessner, April 2014 Slide 14 RESTRICTED AREVA



AREVA
forward-looking energy

Voltage and Frequency Variations

- ▶ **Slow voltage variations:**
 - ◆ Caused by missing or excess reactive power in the grid, large load flows, faulty voltage control equipment in the grid.
 - ◆ Compensation by using of on-load tap changer for the step-up and auxiliary (normal, emergency and standby) transformers or should be handled by the automatic voltage regulator (AVR) of the main generator
- ▶ **Transient voltage variations:**
 - ◆ Caused by short-circuits, switch-over, lightning strikes, transition to houseload operation. Range between 1ms to seconds.
 - ◆ No compensation by active measures, equipment has to be designed for such phenomena or protected against them
- ▶ **Frequency variations:**
 - ◆ Caused generally by missing or excessive active power.
 - ◆ Several defense lines in the grid and in the plant, e.g. transition to houseload operation. Can not easily be compensated.

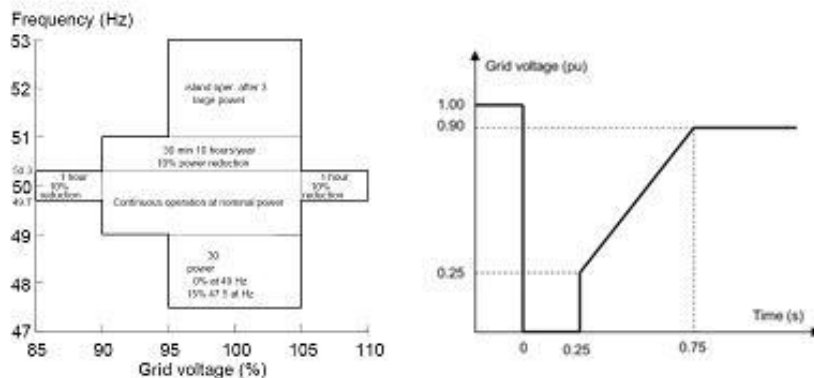
ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessler, April 2014 Slide 15

RESTRICTED AREVA



Voltage and frequency variations – Requirements from grid codes

- ▶ **Nordel grid code and fault ride through characteristic**



ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessler, April 2014 Slide 16

RESTRICTED AREVA



Voltage and frequency variations and transients from “undefined” grid failures

► **Fast transients**

- ◆ Direct and indirect lightning strikes
- ◆ Switching
- ◆ Arcing faults
- ◆ Transmission line phenomena
- ◆ Resonance phenomena
- ◆ Electromagnetic Pulse phenomena
- ◆ Geomagnetic Induced Currents (GIC)

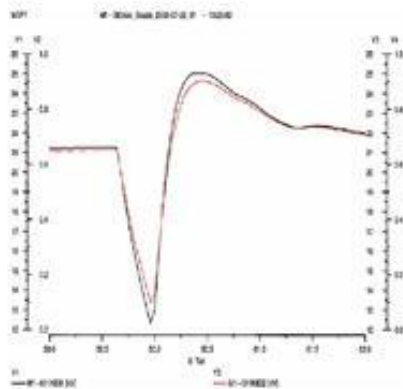
► **Other failures**

- ◆ Earth faults
- ◆ Phase interruptions

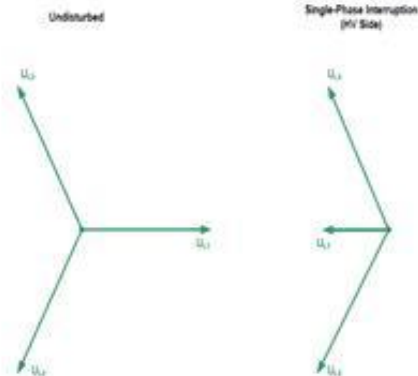


Not “standardized” failures - transients and phase interruptions

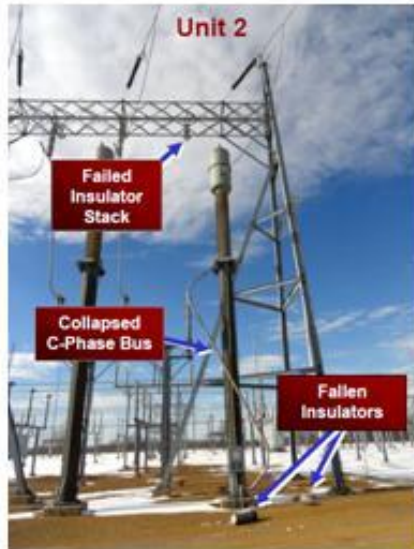
► **Voltage transient Forsmark 1**



► **Phase interruption – e.g. single phase interruption**



Byron 2 event - Interruption of one phase



Source: Exelon

- ▶ January 30th, 2012 at Byron Unit 2, USA
 - ◆ The C-Phase broke, resulting in a Phase C open circuit and a high impedance ground fault
 - ◆ Open phase condition and resulting voltage unbalance – unit protective relaying was not designed to detect
 - ◆ Reactor trip and finally the control room operators detected the failure and tripped the breakers to separate unit buses from offsite power sources, in order to initiate EDG automatic start and operation
- ▶ EDG start is initiated by a voltage measurement in a two-out-of-two-logic, not met in this case

ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessner, April 2014 Slide 19

RESTRICTED AREVA



Forsmark 3 event - Interruption of two phases

- ▶ Outage in Forsmark 3:
 - ▶ only one (of two) external busbars connected to the plant because of maintenance on the external grid switch yard.
 - ▶ The alternative power source was disconnected because of change to a new 70 kV switch yard (This operating conditions is only allowed during outage)
 - ▶ On the 30th of May 2013 the plant circuit breaker to the 400 kV grid was disconnected in two phases only, due to a loose cable connected to one of three poles for the breaker tripping device. Breaker failure protection not activated due to low current (limit not reached).
 - ▶ No start of the EDG's (two-out-of-three-logic at 65%Ur) because limiting values were not reached (Main and auxiliary transformers have a Y/Δ-connection and the star-point is grounded).
 - ▶ Voltage measurement for the MCR between L1 and L2 only: value ok, no alarm.
 - ▶ After 20 minutes the operators separated manually the safety buses from the external grid, after them automatic start of the Diesels and supply of the safety buses.
 - ▶ Equipment on safety and non-safety busbar with protection for "phase-disconnection" stopped automatically. Electrical machines lacking protection for "phase-disconnection" did not stop and some of them get minor damages.

ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessner, April 2014 Slide 20

RESTRICTED AREVA



Consideration in principle, based on a one-phase- interruption (Byron)

RESTRICTED AREVA

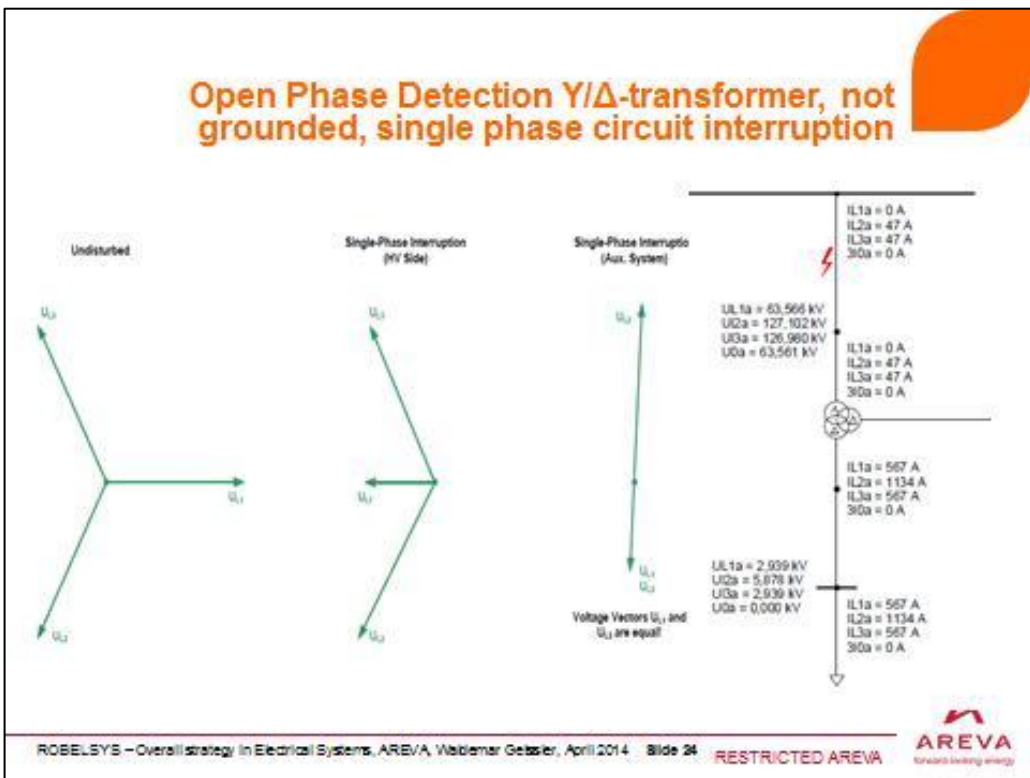
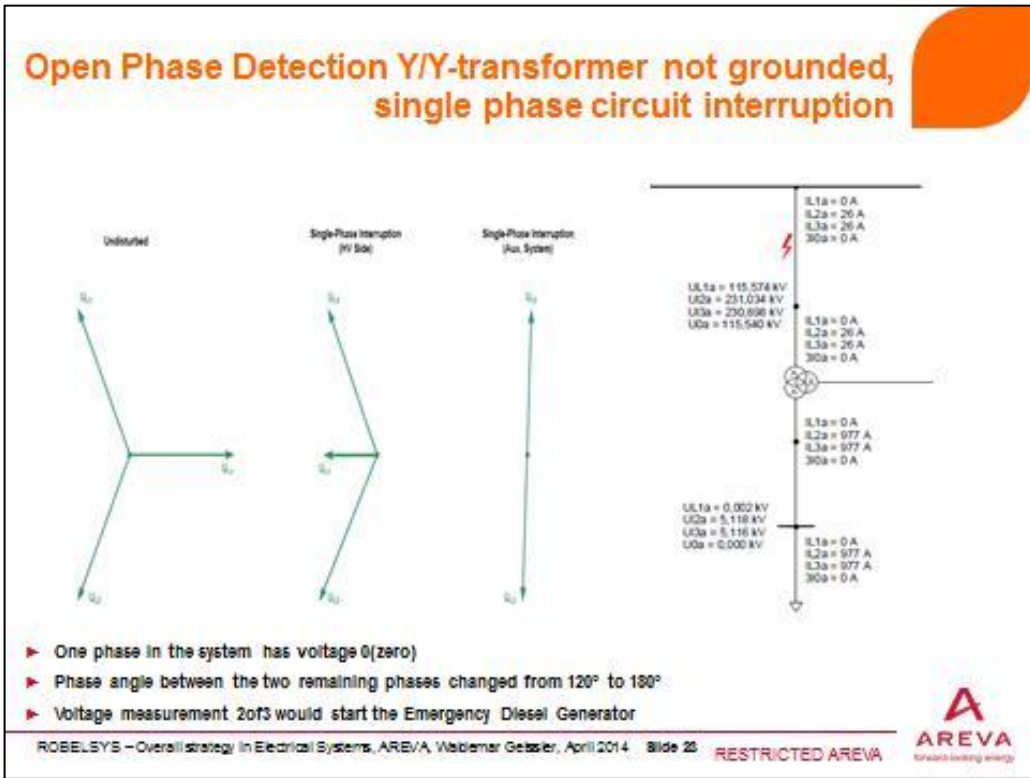


Boundary conditions for open-phase- detections

- ▶ Connection of the Unit Auxiliary Transformer (on the Insulated Phase Busduct or on the HV grid) has an significant importance.
- ▶ Open phase transmission over the main, auxiliary or standby transformers depends on the transformer vector group: Yy, Δ y, Yd, etc. and the secondary side loading conditions
- ▶ Grounding of the transformers (or not) has an significant influence
- ▶ Loading conditions of the plant (power operation, outage etc.) has a significant influence
- ▶ Start conditions for the Emergency Diesels (e.g. 2of2 or 2of3 measurement, at 80%Ur, at 65% etc.).

ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessner, April 2014 Slide 22 RESTRICTED AREVA





Byron Event, Open Phase Detection Y/Δ-transformer single phase circuit interruption – voltage conductor to ground

Ermittlung der verbleibenden Spannung U_{L21} aus der Leiter-Erde-Spannung U_{L1}

$$U_{L21} = -U_{L2} + U_{L1} \quad / \quad U_{L32} = -U_{L3} + U_{L2} \quad / \quad U_{L13} = -U_{L1} + U_{L3}$$

$$U_{L21} = U_{L32} = 86\% U_r$$

$$U_{L13} = 0$$

- ▶ No phase in the system has voltage 0(zero)
- ▶ Phase angle between the phases changed from 120° to 180° (for L1-L2 and L2-L3) and 0° (for L2-L3)
- ▶ Due to the angle shift two voltage values would be 86%Ur (>80%Ur)
- ▶ Voltage measurement 2of3 with limit <80%Ur would not start the EDG

ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessner, April 2014
Slide 25
RESTRICTED AREVA

AREVA
forward looking energy

Open Phase Detection - Resume

Statements:

- ▶ Connection type of the Unit Auxiliary System is important (via generator transformer or direct on the HV-grid)
- ▶ Open phase transmission over the auxiliary and standby transformers depends on the transformer vector group: Yy, Δy etc., the Y-point-grounding and secondary side loading conditions.
- ▶ Influence of running motors (load conditions) is high.

Statement: No general applicable solution is available. Detailed investigations to be done for each plant.

▶ **Electrical Protection:**

- ◆ Individual equipment protection, e.g. out-of-balance-protection for motors
- ◆ Digital protection devices for negative sequence measurements could detect the failure. Setting values are challenging.

ROBELSYS – Overall strategy in Electrical Systems, AREVA, Wablenar Gessner, April 2014
Slide 26
RESTRICTED AREVA

AREVA
forward looking energy

Improvements in power plants, without consideration of deeper electrical calculations

RESTRICTED AREVA

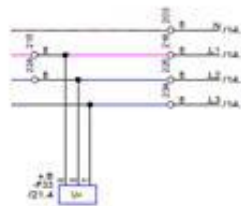


Open-phase-detections – possible improvements

► Show all voltages in the Main Control Room, all the time.

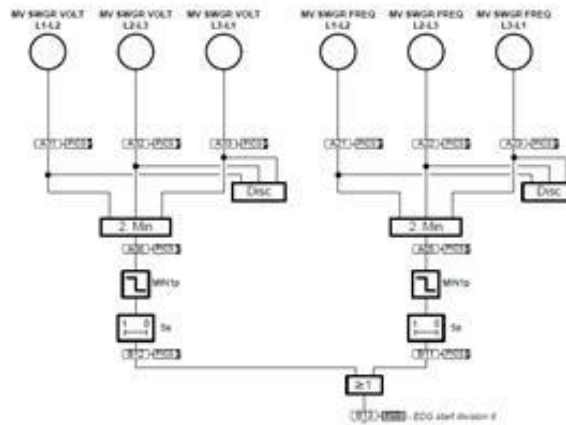
L1-L2	F A	692 KA8155	9.99 kV
L2-L3	F A	692 KA8156	9.99 kV
L3-L1	F A	692 KA8157	9.99 kV

► For alarms: Use a type of measurement that all voltages are monitored.



Open-phase-detections – possible improvements

- ▶ Use for the automatic start of the Emergency Diesels 2of3 instead 2of2 measurements.
- ▶ Divers measurement to the voltage, e.g. frequency, could also be considered



ROBELSYS – Overall strategy in Electrical Systems, AREVA, Woblermar Gessler, April 2014 Slide 26 RESTRICTED AREVA



Summary

RESTRICTED AREVA



Summary

- ▶ Electrical Power Supply System is a supporting system, but the availability and the robustness of the electrical system is of major importance for the safety of the plant.
- ▶ Independently from the plant concept, a robustness analysis should be done, considering hazards and electrical transients.
- ▶ Robustness against CCF of support systems – analysis should assess the cliff edge effect of unexpected events through ALARP

Thank you!

“

Any reproduction, alteration or transmission of this document or its content to any third party or its publication, in whole or in part, are specifically prohibited, unless AREVA has provided its prior written consent.

This document and any information it contains shall not be used for any other purpose than the one for which they were provided.

Legal action may be taken against any infringer and/or any person breaching the aforementioned obligations.

”

Comparison between Different Power Sources for Emergency Power Supply at Nuclear Power Plants

Magnus Lenasson, MSc

Solvina AB, Sweden

Abstract

Currently the Swedish nuclear power plants are using diesel generator sets and to some extent gas turbines as their emergency AC power sources and batteries as their emergency DC power sources.

In the laws governing Swedish nuclear activity, no specific power sources are prescribed. On the other hand, diversification of safety functions should be considered, as well as simplicity and reliability in the safety systems. So far the choices of emergency power sources have been similar between different power plants, and therefore this project investigated a number of alternative power sources and if they are suitable for use as emergency power on nuclear power plants.

The goals of the project were to:

- Define the parameters that are essential for rendering a power source suitable for use at a nuclear power plant.
- Present the characteristics of a number of power sources regarding the defined parameters.
- Compile the suitability of the different power sources.
- Make implementation suggestions for the less conventional of the investigated power sources. (unconventional in the investigated application)

10 different power sources in total have been investigated and to various degrees deemed suitable

Out of the 10 power sources, diesel generators, batteries and to some extent gas turbines are seen as conventional technology at the nuclear power plants. In relation to them the other power sources have been assessed regarding diversification gains, foremost with regards to external events. The power sources with the largest diversification gains are:

- Internal steam turbine
- Hydro power
- Thermoelectric generators

The work should first and foremost put focus on the fact that under the right circumstances there are power sources that can complement conventional power sources and yield substantial diversification gains.

1. Background and purpose

This paper is a shortened version of the report “Comparison between different power sources for emergency power supply at nuclear power plants”¹. The report is financed by Elforsk – Swedish Electrical Utilities’ R & D Company.

The background of the report is that the Fukushima accident showed how redundant but not diversified power sources can be destroyed by external events. This might lead to increased focus on diversification, from the industry and/or the regulating authorities.

A number of essential parameters for a power source to work as emergency power supply at a nuclear power plant have been identified; ten different power sources have then been evaluated with respect to these parameters.

The report is supposed to work as a knowledge base and decision support when new nuclear power plants or reinvestments in old ones are considered.

The studied power sources are:

- Diesel generators
- Gas turbines
- Internal steam turbines
- External steam turbines
- Hydro power plant
- Batteries
- Fuel cells
- Stirling engines
- Thermoelectric elements
- Flywheels

The power sources are evaluated for five different applications, each application with its own acceptance criteria for each of the essential parameters. The five applications are:

- Onsite emergency AC source
- Onsite emergency DC source
- Alternate AC source, small
- Alternate AC source, large
- Alternate AC source, mobile

Mainly Swedish preconditions are considered in the report, but most of the results are applicable in any other country.

2. Essential parameters

In this chapter the parameters that have been identified as essential for a power source to act as emergency power source at a nuclear power plant are listed and explained. In the original report¹ acceptance criteria for the different applications are defined.

Available power

The parameter demonstrates in which power intervals the power sources are available.

Available energy and energy density

The parameter demonstrates how large quantities of primary energy carrier that is required for the different power sources.

Maximum operation time

The parameter demonstrates if there are limitations on how long the different power sources could be in operation without any planned outages given that fuel is supplied.

Dynamic operation

The parameter demonstrates how the different power sources are controlled (frequency and voltage control) and how they react on motor starts and load rejection for example.

Starting time

The parameter demonstrates how soon after a loss of offsite power the supplied grid can be reenergized.

Realizability of power source within or outside the protected area

The parameter demonstrates how large the power source is and which special preconditions it requires. Based on this an assessment is made if it is feasible to realize the power source within the protected area or outside it.

Availability and reliability

The parameter demonstrates the availability and reliability of the different power sources.

Definitions:

$$\text{Availability} = 1 - \frac{t_{fo}}{t_{tot}}, \text{ where}$$

t_{fo} = Forced outage hours during operation and standby

t_{tot} = Total amount of hours in operation and standby

$$\text{Reliability} = \frac{n_s}{n_{as}}, \text{ where}$$

n_s = Number of starts

n_{as} = Number of attempted starts

Possibility to classify as safety equipment

This parameter demonstrates if the different power sources have been classified as safety equipment earlier or if it is possible to do so in the future. To evaluate the possibility to classify a power source in the future the main focus is the accumulated operation time of the power source.

Sensitivity to external events

The parameter demonstrates what kinds of external events the different power sources are sensitive to. The different external events are divided into four groups:

- Mechanical impact, for example wind, precipitation (snow), explosions, earthquake
- Impact of water, for example precipitation (rain), sea waves, high sea level, flood.
- Clogging of dampers, air intakes and heat exchangers, for example precipitation (snow), ice storms, missiles due to wind
- Extreme temperatures

This parameter is used to evaluate diversification gains, i.e. if the different power sources are sensitive to the same types of external events or not. Sensitivity to different types of external events makes it less likely that all power sources are taken out simultaneous.

Additional risks of challenging existing equipment

The parameter demonstrates what additional risks the different power sources pose to the existing equipment on site. The additional risks are divided into the following groups:

- Explosives
- Fire load
- Large rotating masses
- Hazardous substances
- Electrical transients

Aspects of maintenance and operational readiness

The parameter demonstrates if any special maintenance measures or measures to assure operational readiness can prevent the possibility to operate the different power sources in the intended way. Special attention is paid to possible tests or measures that have to be performed during the plant's normal operation period.

Mobility

The parameter demonstrates if the different power sources can be made mobile.

Investment and operational costs

The parameter demonstrates the investment costs and the operational costs for the different power sources. The costs are for the equipment alone, so the additional costs for a possible safety classification process and for the projects installing the equipment are not included.

3. Summaries for different power sources

3.1 Diesel generators

The suitability of diesel generators in different applications is seen in table 1. Diesel generators are already implemented as several redundant units in nuclear power plants worldwide.

Table 1. The suitability of diesel generators

Diesel generators			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source	X		
Onsite emergency DC source			X ¹
Alternate AC source, small	X		
Alternate AC source, large		X ²	
Alternate AC source, mobile	X		

1) Unsuitable due to starting time > 0

2) Suitable if several units are connected in parallel.

3.2 Gas turbines

The suitability of gas turbines in different applications is seen in table 2. Gas turbines are suitable to implement as several redundant units.

Table 2. The suitability of gas turbines

Gas turbines			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source			X ¹
Onsite emergency DC source			X ¹
Alternate AC source, small	X		
Alternate AC source, large	X		
Alternate AC source, mobile		X ²	

1) Unsuitable due to starting time > 20 s

2) Suitable if less than 72 hours' worth of fuel is accepted or a separate solution for the fuel is provided.

3.3 Internal steam turbine

The concept "internal steam turbine" is a steam turbine driven by steam from the main process in the nuclear power plant. The suitability of internal steam turbines in different applications is seen in table 3. Internal steam turbine is only suitable to implement as a single unit due to lack of power.

Table 3. The suitability of internal steam turbine

Internal steam turbine			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source			X ¹
Onsite emergency DC source			X ²
Alternate AC source, small		X ³	
Alternate AC source, large			X
Alternate AC source, mobile			X

1) Unsuitable due to lack of power at reactor outages and damages at the RCPB

2) Unsuitable due to starting time > 0

3) Suitable if the available power is sufficient

4) Unsuitable due to lack of available power

5) Unsuitable power source to make mobile

3.4 External steam turbine

The concept “external steam turbine” consists of an offsite heat and power plant (CHP) that has a dedicated line to the nuclear power plant. At a blackout the offsite plant disconnects from the grid and starts feeding the nuclear power plant. The suitability of external steam turbines in different applications is seen in table 4. External steam turbines can be implemented as several redundant units in case suitable units can be found in the vicinity of the nuclear power plant and the separation between them is sufficient.

The concept with external steam turbines is characterized by:

- Relatively large diversification gains due to a site separated from the nuclear power plant.
- No challenges to existing equipment
- Many external parameters that should coincide: Possibility to dispose enough heat, existence of suitable external power plant (or willingness to invest in one), willingness to act as emergency power supply to nuclear power plant.
- Existing power plants hard to classify as safety (1E / CatA etc.) equipment
- The line between the external power plant and the nuclear power plant must be protected.

Table 4. The suitability of external steam turbine

External steam turbine			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source		X ¹	
Onsite emergency DC source			X ²
Alternate AC source, small		X ³	
Alternate AC source, large			X ⁴
Alternate AC source, mobile			X ⁵

1) Suitable provided that a suitable power plant exists/is built and that safety classification can be achieved

2) Unsuitable due to starting time > 0

3) Suitable provided that a suitable power plant exists/is built

4) Unsuitable due to lack of available power

5) Unsuitable power source to make mobile

3.5 Hydro power plant

The concept “hydro power plant” consists of an offsite hydro power plant that has a dedicated line to the nuclear power plant. At a blackout the offsite plant disconnects from the grid and starts feeding the nuclear power plant. The suitability of hydro power plants in different applications is seen in table 5. Hydro power plants can be implemented as several redundant units in case suitable units can be found in the vicinity of the nuclear power plant and the separation between them is sufficient.

The concept with hydro power plants is characterized by:

- Large diversification gains due to a site separated from the nuclear power plant and that the power generation is not based on combustion.
- No challenges to existing equipment
- Hard to evaluate the suitability of a hydro power plant without testing it’s island operation capabilities.
- Some external parameters should coincide: Existence of suitable hydro power plant (or willingness to invest in one), willingness to act as emergency power supply to nuclear power plant.
- Existing power plants hard to classify as safety class (1E / Cat A etc.) equipment
- The line between the external power plant and the nuclear power plant must be protected.

Table 5. The suitability of hydro power plant

Hydro power plant			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source		X ¹	
Onsite emergency DC source			X ²
Alternate AC source, small		X ³	
Alternate AC source, large			X ⁴
Alternate AC source, mobile			X ⁵

1) Suitable provided that a suitable power plant exists/is built and that safety classification can be achieved

2) Unsuitable due to starting time>0

3) Suitable provided that a suitable power plant exists/is built

4) Unsuitable due to lack of available power

5) Unsuitable to make mobile

3.6 Batteries

The suitability of batteries in different applications is seen in table 6. Batteries are already implemented as several redundant units in nuclear power plants worldwide.

The concept with batteries is characterized by:

- Operation time normally <24 hours
- Possible to dimension power and energy modularly
- Continuously loading and able to deliver power instantly.
- Well established technology, new types are developed continuously

Table 6. The suitability of batteries

Batteries			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source			X ¹
Onsite emergency DC source	X		
Alternate AC source, small			X ¹
Alternate AC source, large			X ¹
Alternate AC source, mobile			X ¹

¹) Unsuitable due to operation time < 72 hours

3.7 Fuel cells

The suitability of fuel cells in different applications is seen in table 7. They have in total too many shortcomings and doubts to be deemed suitable for any application. Their availability and dynamic behavior is insufficient and the diversification gains are small.

Table 7. The suitability of fuel cells

Fuel cells			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source			X
Onsite emergency DC source			X
Alternate AC source, small			X
Alternate AC source, large			X
Alternate AC source, mobile			X

3.8 Stirling engines

The suitability of stirling engines in different applications is seen in table 8. Stirling engines would require higher temperatures than what is available in a nuclear power plant to function satisfactorily, they are therefore deemed unsuitable for all applications.

Table 8. The suitability of stirling engines

Stirling engines			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source			X ¹
Onsite emergency DC source			X ¹
Alternate AC source, small			
Alternate AC source, large			X ¹
Alternate AC source, mobile			X ¹

¹) Unsuitable since the available heat in the process is not sufficient

3.9 Thermoelectric generators

The suitability of thermoelectric generators in different applications is seen in table 9. Thermoelectric generators can only be implemented as a single unit due to lack of power.

The concept with thermoelectric generators is characterized by:

- Relatively large diversification gains due to resilience to low temperature and absence of gas formation.
- Hard to create a robust and simple solution that can supply a sufficient amount of elements with heat.
- Creates heat losses in the process.

- Cannot be charged during times with available AC power.
- Only available when process heat is available, not during outages for example.

Table 9. The suitability of thermoelectric generators

Thermoelectric generators			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source			X ¹
Onsite emergency DC source		X ²	
Alternate AC source, small			X ¹
Alternate AC source, large			X ¹
Alternate AC source, mobile			X ³

1) Unsuitable due to lack of available power

2) Suitable provided sufficient access to heating and cooling and that it is acceptable that it is only available when process heat is available.

3) Unsuitable due to lack of available power and that it is not suitable for mobility.

3.10 Flywheels

The suitability of flywheels in different applications is seen in table 10. Flywheels can only cope with short discharge times and are therefore not suitable for any of the stated applications, the minimum required discharge time is 8 hours.

The concept with flywheels is characterized by:

- Potential for high power discharges. Resilience to large number of discharges of different magnitudes.
- Only viable for short discharge times due to losses.

Table 10. The suitability of flywheels

Flywheels			
Application	Suitable	Suitable under certain preconditions	Unsuitable
Onsite emergency AC source			X ¹
Safety class DC source			X ¹
Alternate AC source, small			X ¹
Alternate AC source, large			X ¹
Alternate AC source, mobile			X ¹

¹) Unsuitable due to insufficient discharge time.

5. Conclusions

Out of the 10 power sources, diesel generators, batteries and to some extent gas turbines are seen as conventional technology at the nuclear power plants. In relation to them the other power sources have been assessed regarding diversification gains, foremost with regards to external events. The power sources with the largest diversification gains are:

- Internal steam turbine
- Hydro power
- Thermoelectric generators

Of these three hydro power is the only one that can be available during reactor outages and accidents where steam is not available in the main process.

References

- [1] Magnus Lenasson, "Comparison between different power sources for emergency power supply at nuclear power plants", Elforsk, Report no 13:87. Available 2014-02-26 at http://elforsk.se/Rapporter/?rid=13_87

Comparison between Different Power Sources for Emergency Power Supply at Nuclear Power Plants

Comparison between Different Power Sources for Emergency Power Supply at Nuclear Power Plants

Nuclear Commission, NRC
Nuclear 101, 10000

Abstract

Currently the United States nuclear power plants using diesel generators can and do meet their obligations to the emergency AC power system and related to their emergency AC power system.

In the event of a nuclear power plant accident, the emergency power system is required to be able to meet the needs of public facilities, avoid the environment, as well as maintain and withdraw to the public interest. In the event of emergency power sources have been shown to have different power sources, and therefore the need to implement a number of different power sources and if they are available for emergency power to the emergency power system.

The goal of this document is:

- Define the parameters that are needed for the emergency power system within the use of a nuclear power plant
- Provide the identification of a number of power sources regarding the different parameters
- Compare the availability of the different power sources
- Provide implementation suggestions for the use of different power sources

20 different power sources to 2000 different power sources are investigated within the emergency power system.

As of the 10 power sources, diesel generators, battery and in some cases gas turbines are used as emergency power at the nuclear power plant. In addition to these the other power sources have been investigated regarding their availability, power, power, reliability in general events. The power sources are investigated in the following way:







- Diesel generator
- Battery
- Gas turbine generator

The study should be used to determine how to use the different power sources in the emergency power system. The study should be used to determine how to use the different power sources in the emergency power system.

1


Jämförelse av olika kraftslag som nödförsörjning vid kärnkraftverk

Elforsk rapport 13.87


Majken Lohmander August 2013

ELFORSK



Background

- Fukushima
- Common Cause Failure due to External Event
- Increased focus on diversification?
- In that case, which power sources should be used?



Method

- Define different applications
- Identify essential parameters
- Identify acceptance criteria for the parameters
- Evaluate a number of power sources with respect to these parameters

Solvina
Energy Excellence

Applications

- **Defined applications:**
 - **Onsite emergency AC Source**
 - The ordinary emergency AC source, today mainly diesel generators, ≈ 2 MW
 - **Onsite emergency DC Source**
 - The ordinary emergency DC source, today mainly batteries, ≈ 200 kW
 - **Alternate AC source, small**
 - An alternate AC source designed to replace one of the ordinary emergency AC sources, ≈ 2 MW
 - **Alternate AC source, large**
 - An alternate AC source designed to supply half of the internal grid, both safety, safety related and non-safety equipment, ≈ 20 MW
 - **Alternate AC source, mobile**
 - An alternate AC source with tasks equal to "Alternate AC source, small" except it is mobile.

Solvina
Energy Excellence

Essential parameters

- Parameters used for evaluation:
 - Available power
 - Available energy and energy density
 - Maximum operation time
 - Dynamic operation
 - Starting time
 - Realizability of power sources within or outside the protected area
 - Availability and reliability
 - Possibility to classify as safety equipment
 - Sensitivity to external events
 - Additional risks of challenging existing equipment
 - Aspects of maintenance and operational readiness
 - Mobility
 - Investment and operational costs

Solvina
Energy Excellence

Power Sources

- Investigated power sources:
 - Diesel generators
 - Gas turbines
 - Internal steam turbine
 - External steam turbine
 - Hydro power
 - Batteries
 - Fuel cells
 - Stirling engines
 - Thermoelectric generators
 - Flywheels

Solvina
Energy Excellence

Results

√=Suitable, X=Suitable under certain preconditions, --Not suitable

Power source	Application				
	Onsite emergency AC source	Onsite emergency DC source	Alternate AC source, small	Alternate AC source, large	Alternate AC source, mobile
Diesel generators	√	-	√	X	√
Gas turbines	-	-	√	√	X
Internal steam turbine	-	-	X	-	-
External steam turbine	X	-	X	-	-
Hydro power	X	-	X	X	-
Batteries	-	√	-	-	-
Fuel cells	-	-	-	-	-
Stirling engines	-	-	-	-	-
Thermoelectric generators	-	X	-	-	-
Flywheels	-	-	-	-	-

Solvina
Energy Excellence

Results continued

- Power sources with large diversification gains:
 - Internal steam turbine
 - Hydro power
 - Thermoelectric generators
- Hydro power does not require any specific operation mode in the NPP to work.

Solvina
Energy Excellence

**Advancing Ruggedness of Nuclear Stations
By Expanding Defence In Depth in Critical Areas**

Thomas Koshy, Section Head, Nuclear Power Technology Development, IAEA, Vienna, Austria

Abstract

The nuclear industry continues to rise above the challenges it has faced over the years from external events and internal events. Fukushima event has shed light on a few vulnerabilities that could be overcome by utilizing the current state of technology.

Common cause from sea water ingress was not conceived to have the entire electrical power system including AC & DC disabled beyond reasonable recovery. Rather than focusing on the solutions for lessons from Fukushima, it is better to address “Fukushima type” events and advance the resilience of the NPPs. The effort needs to be on exploring different approaches to overcome such vulnerabilities so that a variety of solutions are available to make appropriate choices on improving NPP ruggedness based on anticipated challenges in the regions.

In a technology neutral approach for light water reactors (LWR) there are 4 critical areas that are significant for ensuring nuclear safety. (1) Reactor trip, (2) Depressurization, (3) Emergency Core Cooling, and (4) Containment integrity. The reactor trip had not suffered any significant setbacks in the immediate past but provisions to address Anticipated Transients without Scram (ATWS) were generally included in most designs. While the technology has advanced, software driven/assisted trips are becoming popular and desirable. However, a diverse approach with least probability of potential interference needs to be provided in the control room and remote shutdown area to advance the ruggedness of reactor trip. Depressurization is essential for passive as well as active cooling systems and therefore the approaches to depressurize should have more than one approach to ensure its success. In the absence of diverse approaches to depressurize, it is more important to consider RCS cooling capability during accidents or transients while the reactor is at a higher pressure. In the area of Emergency Core Cooling, the events history demonstrates greater success on diversity than increasing redundancy. There are several events both external and internal that could cause the failure of AC motor driven cooling systems. DC operated steam driven systems and diesel driven cooling systems have avoided several near core melt conditions. Containment Integrity is the last defence for protecting the people and the environment. Diversity in containment cooling is essential for keeping the pressure transients under control. Design provisions to connect potable cooling systems for heat removal and capability to flood the reactor cavity are essential. Recognizing the remote possibility of a severe accident, reliable containment venting (capability to operate with potable energy sources) and filtering could be explored as an option for ensuring an additional layer of protection. These four critical areas need to be viewed as layers in the defence of depth and consequently would require a design that fully removes and common cause failures. Ruggedness of these layers can be achieved only when the process signal sources, power supply and processing of the logic is executed independently. The electrical power system should be re-evaluated for bringing flexibility and adaptability for achieving greater level of safety.

Key Words: Fukushima, reactor trip, depressurization, emergency core cooling, containment integrity

1. Background

The nuclear industry has faced several challenges resulting from major plant events but it continues to rise above the challenges from both external and internal events. Fukushima event of 2011 has shed light on a few new vulnerabilities such as common cause failures of the entire electrical power system, extended station blackout, loss of infra-structure for long term, etc., These problems could be overcome utilizing the current state of technology.

External events have been addressed in varying degrees based on the historical data available in several regions. Hurricanes, seismic events, flooding etc., have been considered to be manageable with the design and compensatory measures that were developed for plant specific applications. A large scale Tsunami that could disable the electrical infra-structure for both offsite and onsite was an unprecedented event. A sea water ingress as a common cause was not conceived to have the entire electrical power system including AC & DC disabled beyond reasonable recovery. Rather than focusing on the specific solutions and lessons from Fukushima, it is better to address “Fukushima type” events and advance the resilience of the NPPs. The effort needs to be on exploring different approaches to overcome such vulnerabilities so that a variety of solutions are available to the designers and owners to make appropriate choices for improving NPP ruggedness based on anticipated challenges in specific regions.

2. Nuclear Safety Basics

It is essential to review the primary goals while seeking to find better solutions to the evolving challenges. The reactor can be brought to safe conditions from an operating mode by terminating the chain reaction and making prompt provisions for removing decay heat. Most reactors are operating at an elevated pressure and temperature while sustaining a chain reaction for producing power. In a technology neutral approach for Light Water Reactors (LWR) there are 4 critical areas that are significant for ensuring nuclear safety. (1) Reactor trip, (2) Depressurization, (3) Emergency Core Cooling, and (4) Containment Integrity. The approaches should consider each function to be critical and design a high level of reliability for ensuring nuclear safety under all anticipated conditions.

3. Approaches for Rugged Design

3.1 Reactor Trip

The capability for reactor trip had not suffered any significant setbacks in the immediate past because the lessons from the past have been addressed reasonably well. These lessons have to be guarded adequately to preserve its demonstrated reliability and advance in performance. A failure to trip the reactor occurred resulting from the binding of the breaker trip bar inside the breaker mechanism that was not overcome by the energy stored in the charged spring. The technology at the time was to rely on the compressed spring force for actuating the trip bar on a valid trip demand. This binding issue was removed by adding another DC solenoid that was energized to actuate the trip bar with more force thus bringing in diversity to trip bar operation of the breaker. In addition, further provisions were made to address Anticipated Transients without Scram (ATWS). The concise requirements in this area are in 10CFR50.62¹. The ATWS solutions required alternate methods to terminate the chain reaction. While the technology has advanced, software driven/assisted trips are becoming popular and desirable. However, a diverse approach with least probability of potential interference needs to be provided in the control room and remote shutdown area to enhance the ruggedness of reactor trip.

¹. United States Nuclear Regulatory Commission, Code of Federal Regulations Section 10 Energy Part 50

Reactor Trip (inserting the control rods to terminate fission) is a critical nuclear safety function and therefore, it must be independent of other critical functions. On June 29, 2007, North Anna Power Station experienced a spurious actuation of reactor trip, and emergency core cooling injection into the reactor caused by a diode failure². Because of the nature of the failure, the licensee could not reset from the control room the actuation signal for some “B” train equipment, which resulted in overfilling the pressurizer and multiple actuations of a pressurizer power-operated relief valve (PORV) to limit Reactor Coolant System (RCS) pressure. RCS inventory from the PORV discharged to the pressurizer relief tank (PRT), rupturing one of the PRT rupture disks, which allowed RCS water to reach the containment basement. The operators had to detach relays, remove fuses etc., to reset the actuation. While large scale integration has certain inherent benefits in reducing cost and operational convenience, it is proving to be undesirable for the prompt resetting safety injection actuation or for reverting to manual actions during emergency.

IEEE Std 603-2009
IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

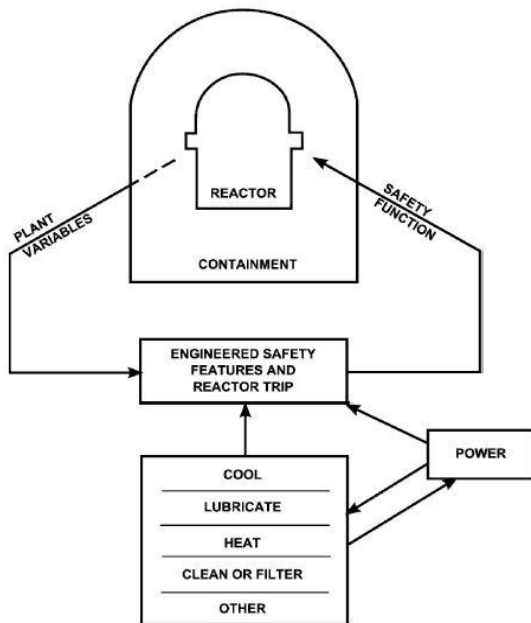


Figure A.2—Typical safety system block diagram

IEEE Std 603-2009
IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

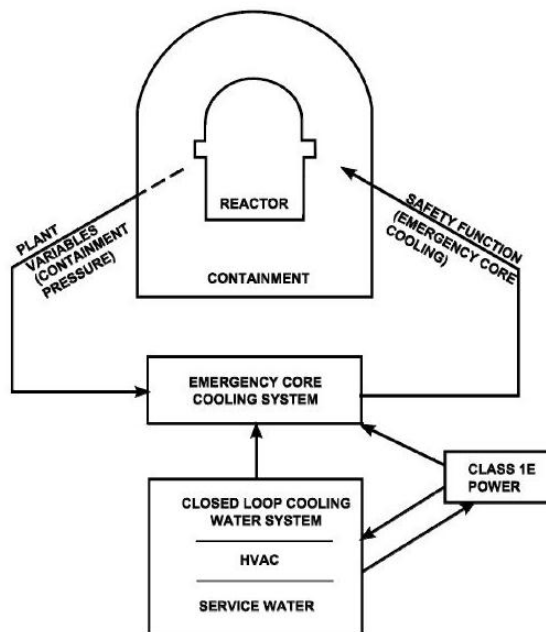


Figure A.3—Elements for emergency core cooling

The Figure A.2 and A.3 are excerpts from the IEEE 603-2009³ that is endorsed by the USNRC. These two diagrams in the appendix are given in the standard to clearly explain that the reactor trip function needs to have independent signals for plant variables, power supply and its actuation. The diagram in the left points to the variables (process signals) exclusively supplying input for reactor trip function. The power supply block is supporting the respective support systems associated with reactor trip function.

The diagram on the right indicates similar requirements for emergency core cooling system. The power supply is shown to be different than for reactor trip with “1E” sign to indicate that it should have a

². US Nuclear Regulatory Commission Information Notice 2009-03
<http://pbadupws.nrc.gov/docs/ML0830/ML083080368.pdf>

³. 603-2009 - IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
<http://standards.ieee.org/findstds/standard/603-2009.html>

higher pedigree in relation to the power supply for reactor trip in that the reactor trip could be accomplished with a fail-safe logic. This approach provides a full diversity between reactor trip and emergency core cooling. (See section 4.0 for specific details on electrical power supply arrangements).

3.2 Depressurization

RCS depressurization is essential for passive as well as active cooling systems and therefore, the approaches to depressurize should have more than one method to ensure its success even though the actuation logic is developed as part of emergency core cooling. The technological advancements have led to software driven systems and usually the manual actions from control room also rely on certain level of software assistance. However, it is highly advisable to preserve a direct wired manual depressurization capability or a manual valve opening provision from an accessible location, to be utilized during emergency to overcome any potential software lock up or other magnetic/electronic interferences.

3.3 Emergency Core Cooling

Even when there is a diverse approach for depressurization, it is essential to consider RCS cooling capability during accidents or transients while the reactor is holding a higher pressure. In the area of Emergency Core Cooling, the events history demonstrates greater success for diversity than increase in redundancy. An extended nuclear station blackout occurred at Narora Unit #1⁴. A main turbine blade ejection resulted in lubricating oil fire that expanded into a hydrogen fire. The entire AC power system failed that disabled all electric driven emergency core cooling. The failures of the electrical buses made all the motor driven cooling systems inoperable even though power sources are available. Diesel driven fire pumps were the only operable safety system and it injected water into the steam generator and prevented a core failure. The Fukushima event of 2011 caused a similar failure of all AC systems beyond reasonable recovery both on site and off site. The isolation condenser and steam driven cooling systems were the only operable systems in this event. These systems should be designed for very long-term operation, well beyond 90 days, to ensure cold shutdown.

There are several events both external and internal that could cause the failure of AC motor driven cooling systems. DC operated steam driven systems and diesel driven cooling systems have avoided several near core melt conditions. Diversity in emergency core cooling capability is critical for overcoming such common cause failures. It is more beneficial to increase diversity rather than increase redundancy beyond three trains.

3.4 Containment Integrity

Containment Integrity is the last defence for protecting the people and the environment. The capability of the containment needs to be evaluated against a severe accident and therefore the design should withstand such events. Diversity in containment cooling is essential for keeping the pressure transients under control. Design provisions to connect potable cooling systems for heat removal and capability to flood the reactor cavity are essential. Recognizing the remote possibility of a severe accident, reliable containment venting (capability to operate with potable energy sources) and filtering would be necessary for ensuring an additional layer of protection especially if the plant is near populous regions.

These four critical areas for nuclear safety need to be viewed as separate layers of the defence in depth and consequently would require a design that fully removes any common cause failures. Ruggedness in each of these layers can be achieved only when the process signals, power supplies and processing of the logic is conducted independently. These systems should have a manual over ride capability with least interferences as an added layer of diversity.

⁴. IAEA International Reporting System (IRS) No: 6341- <http://irs.iaea.org/wfrmAvailableReports.aspx>

4. Robust Electrical Power System

4.1 AC System

The general requirements for reactor safety are addressed in IAEA document on Safety of Nuclear Power Plants⁵. The IAEA safety Guide⁶ on electrical power system is being revised to further enhance the requirements on diversity. In light of the above critical functions discussed above for LWRs, the electrical power system should be re-evaluated for bringing flexibility and adaptability for achieving greater level of safety. The robustness of the onsite power system could be improved by incorporating the lessons from the historical events and preserving them. For reactors with active core cooling systems, onsite AC power is very critical. Even for passive reactors, it is advisable to have reliable onsite offsite power sources as back up for emergency and long term core cooling.

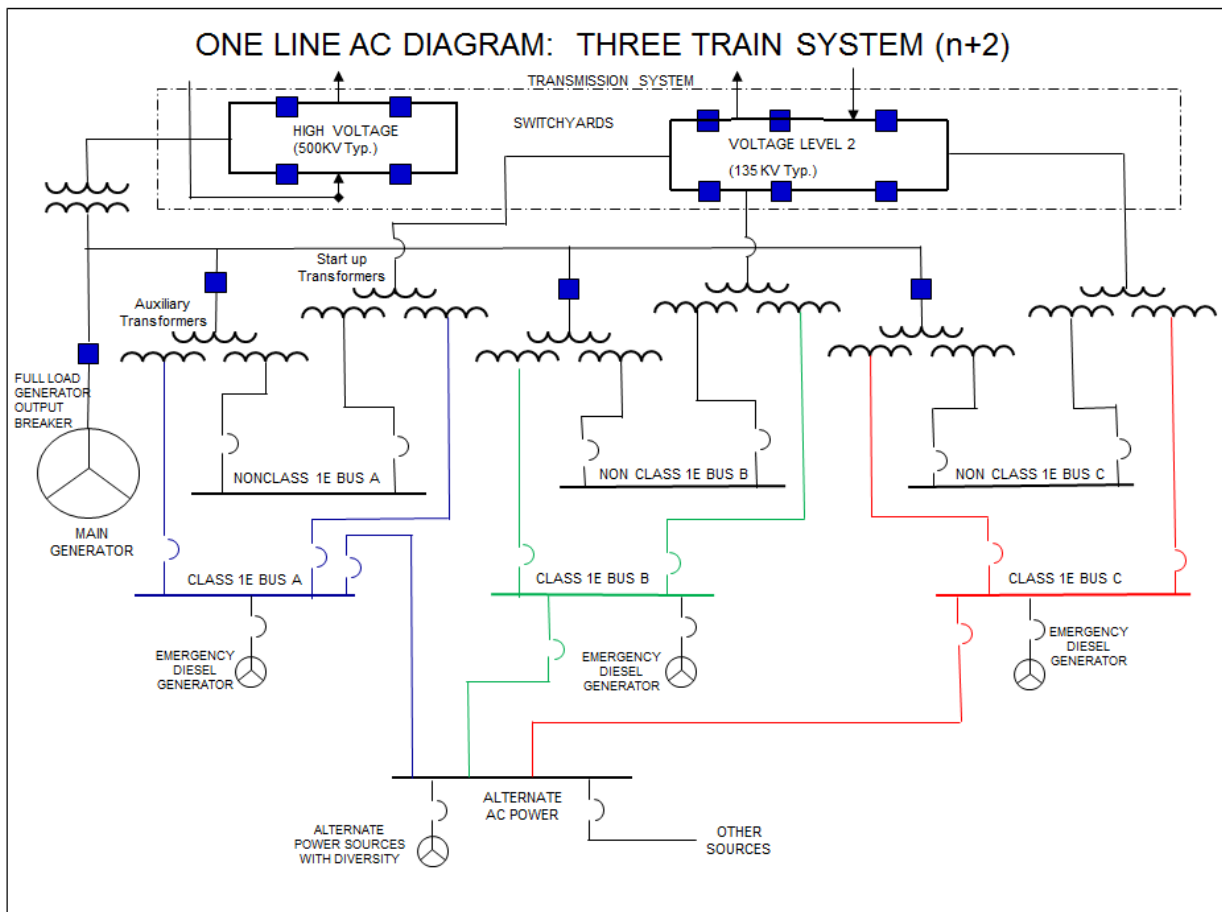
The electrical one line diagram provides certain expanded features for a rugged onsite AC power system. Some of general concepts given below are shared in IEEE standard 765⁷ while it is not stated as a requirement but as suggested approaches.

1. Generator output breaker to disconnect the plant from the grid while the support system gets uninterrupted power. It removes the need for a fast transfer to offsite power.
2. Each safety bus provided with two diverse offsite power sources without any intervening buses to advance its reliability
3. The safety buses have a dedicated emergency diesel generator, and a connection to the Alternate AC power bus with more than one source.

⁵. Safety of Nuclear Power Plants: Design: No. SSR-2/1: wwwpub.iaea.org/MTCD/publications/PDF/Pub1534_web.pdf.

⁶. Design of Emergency Power Systems NS-G-1.8 : www-pub.iaea.org/MTCD/publications/PDF/Pub1188_web.pdf.

⁷. IEEE Standard for Preferred Power Supply (PPS) for Nuclear Power Generating Stations (NPGS).



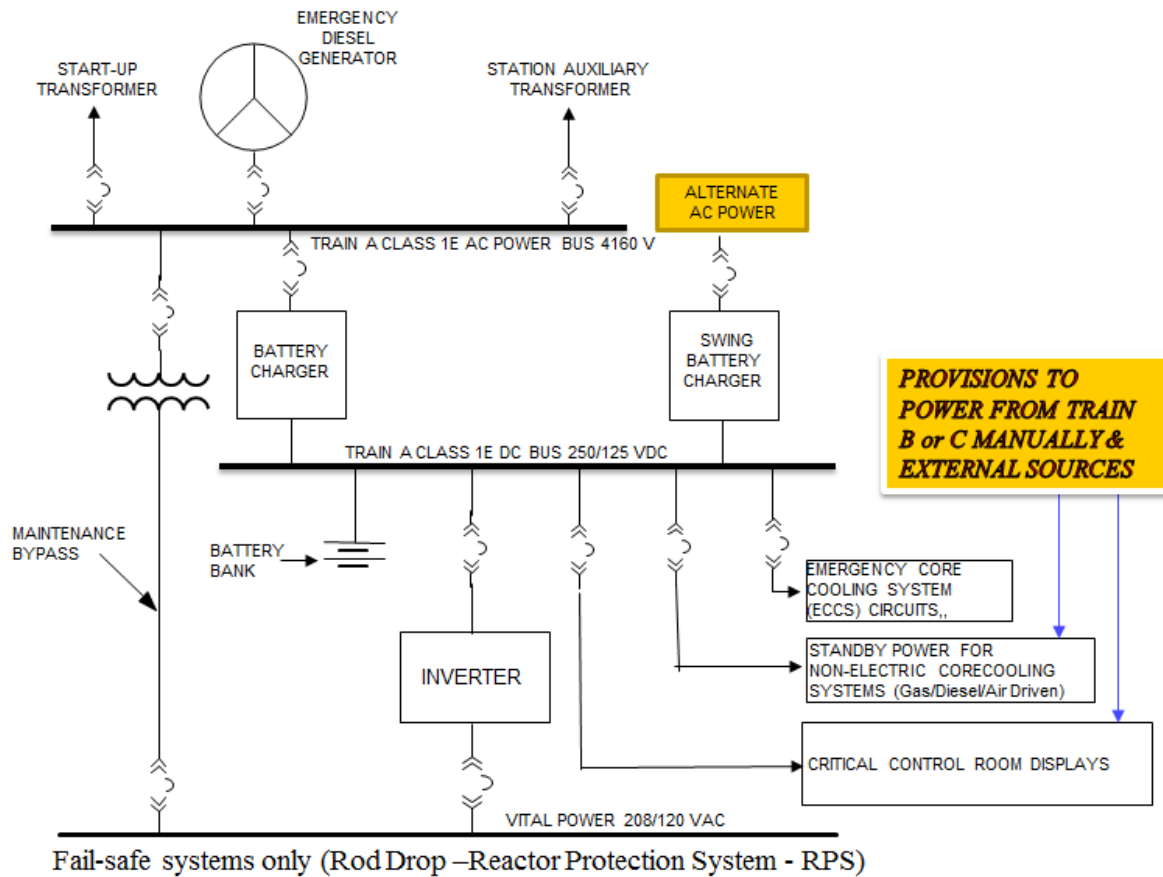
4.2 DC System

The DC bus is essential for providing electrical protection for the AC buses and switchgear. It also the motive power for the operation of breakers that power AC motor driven pumps and it is required for automatically and manually realigning available AC power sources. It powers certain critical valves under station blackout conditions until AC power is recovered. .

The onsite DC system should be designed with provisions for further increasing the availability of DC bus. Historically, a failure of DC bus is the lowest in the electrical power system. However, the non-electric cooling systems (Steam / diesel/compressed air driven injection) should make provisions for locally powering critical components when plant events lead to failures at the bus level.

The figure below provides further clarifications on how the reactor protection system and emergency core cooling could be separated to bring out independence. The power system can be powered through two off site power sources, one diesel generator, and an additional swing battery charger that could be powered from potable/ alternate power source. One or two trains of the equipment, if not all parts of the systems should be designed to withstand external events. These provisions would further improve the ruggedness of the DC power system.

DC Bus One Line Diagram (One of Three Trains)



The design should further make provisions for external powering and cross connecting of critical monitoring and control functions to deal with extreme emergencies. An additional provision is to replicate the critical controls at the remote shutdown station.

5. Conclusions

The resilience of the current nuclear industry is the result of excellent engineering and extremely trained operating staff prepared to handle anticipated challenges. The insights we have gathered from the historic events should inspire our thoughts for advancing the design into a higher plateau of robustness. The Fukushima event should inspire our endeavour to ensure nuclear safety even under extreme effects of nature's challenges.

The four elements that contribute to protecting the people and environment are the effectiveness in (1) Reactor Trip, (2) Depressurization, (3) Emergency Core Cooling, and (4) Containment Integrity. In each of these elements, defence in depth should be separately addressed. The benefits of diversity need to be recognized and implemented instead of expanding more in redundancy. Provision for a manual override with least interferences would form an added layer of diversity for emergency use.

**Advancing Ruggedness of Nuclear
Stations By Expanding
Defense in Depth in Critical Areas**
CSNI International Workshop
April 1-3, 2014 Paris, France

Thomas Koshy, Head
Nuclear Power Technology Development
Department of Nuclear Energy
Officer Of Nuclear Power Engineering Committee (IEEE)



IAEA
International Atomic Energy Agency

AGENDA

- Critical Areas for Nuclear safety
- Events History
- Potential Challenges to Overcome
- Diversity for Light water Reactors
 - Reactor Trip
 - Depressurization
 - Emergency Core Cooling
 - Containment Integrity
- AC Power Systems
- Alternate Energy Sources (Central & Local)



IAEA

T. Koshy, NPTDS/IAEA

2

Critical Areas for Nuclear Safety For Light Water Reactors

- Reactor Trip
- Depressurization
- Emergency Core Cooling
- Containment Integrity



T. Koshy, NPTDS/IAEA

3

Potential Challenges to Overcome

- External Events (beyond Design Bases)
 - Tsunami, seismic event, forest fire, flooding, malicious act, jet impact, volcano, sandstorm
- Internal Events
 - Explosion, fire, malicious act
- Plant Challenges
 - Station Black out, Irrecoverable damage to AC electric buses, Loss of control room
 - D C bus failure
 - Software lock up



T. Koshy, NPTDS/IAEA

4

Considerations for New Designs

- We need to **eliminate** the known **vulnerabilities** at a reasonable cost
- Aim for greater **availability and reliability** for safety systems and power generation
- **Defence in Depth through Redundancy** and **Diversity** are the key elements for success
- Incorporate **Defence in Depth** into all critical areas of nuclear safety



T. Koshy, NPTDS/IAEA

5

Reactor Trip Challenges & Solutions

- The Anticipated Transients with out SCRAM (10CFR 50.62)
- Solutions:
 - Diverse tripping (Additional trip solenoid for actuating the breaker trip bar) Alternate Rod Insertion/ boration - **diversity**
 - Direct-wired manually operated trip breakers with capability to operate from control room and remote shutdown area - **diversity**
 - The power supply, sensors and actuation exclusively dedicated to trip function - **redundancy**



T. Koshy, NPTDS/IAEA

6

Reason for Separating ECCS & RPS

- At North Anna, Unit 2, one diode failure caused Rx Trip & ECCS actuation.
- Consequently pressurizer overfilled, Power operated relief valve (PORV) cycled several times. Pressure relief tank rupture disk ruptured (*USNRC IN: 2009-03*)
- Safety Injection could not be reset from control room to prevent primary system going water solid
- **A single failure affected RPS & ECCS**



IAEA

T. Koshy, NPTDS/IAEA

7

Reason for Separating ECCS & RPS

- At Forsmark, 2 UPS failures caused:
 - A reactor trip, Core Cooling Actuation (2 out of 4 trains injected water)
 - Relief valves (ADS) stuck open 28 min. (until power was recovered to vital bus)
- **Two UPS failures from a common cause** resulted in reactor trip & a LOCA (relief valve stayed open) challenging RCS recovery
 - Yankee Rowe also had a similar event when vital bus voltage declined when coasting EDG remained connected to the bus)
- Remove shared elements between ECCS & RPS to prevent common cause failures



IAEA

T. Koshy, NPTDS/IAEA

8

IEEE Std 603-2009 ANNEX A: Endorsed in USNRC 10CFR50

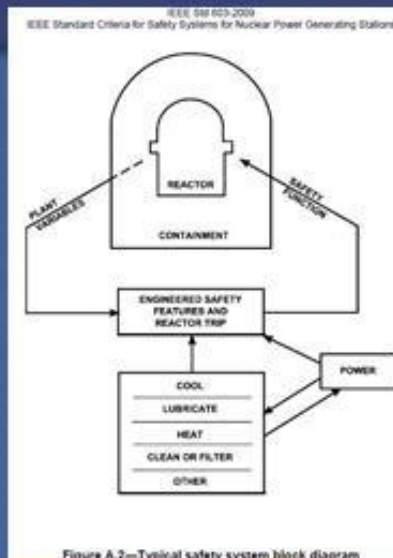


Figure A.2—Typical safety system block diagram

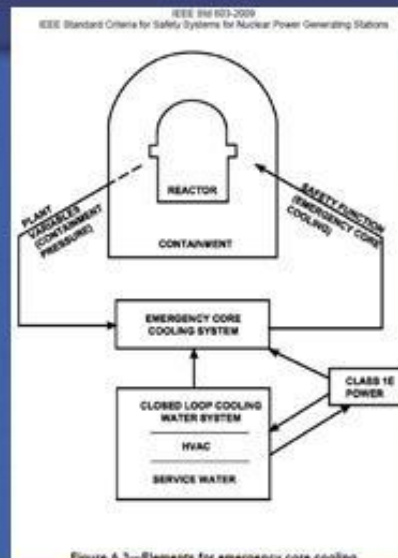


Figure A.3—Elements for emergency core cooling

Consider consequences of one or more UPS failures / loss of power etc., and conduct a thorough failure modes and effects analysis (FMEA)



T. Koshy, NPTDE/IAEA

9

Historic Events (IRS Report # 6341)

1993 Narora-1 Event

- Ejected turbine blade caused a fire and hydrogen explosion
- Complete loss of power – **station blackout for 17hrs.**
- Diesel driven fire pumps aligned to inject water into the steam generator
- No radiological impact onsite or offsite



T. Koshy, NPTDE/IAEA

10

Historic Events

2001 Maanshan

- Tropical storm caused loss of offsite power
- Both Emergency Diesel Generators (EDG) failed
- Station blackout for 2 hours
- AC safety buses became irrecoverable
- One Diesel generator was later recovered to establish core cooling



T. Koshy, NPT/IAEA

11

Historic Events (IRS report # 7788)

2006 Forsmark -1

- 400KV Switchyard work resulted in overvoltage and an under voltage transient
- 2 out of the 4 trains of vital AC power lost and the respective EDGs failed.
- Alternate AC power failed to start
- Half of the control room indications were lost
- Relief valves stayed open (LOCA?)
- Two buses that operated had the same failure susceptibility
- A near - Station Black out event



T. Koshy, NPT/IAEA

12

Historic Events

2011 Fukushima

- Tsunami caused salt water ingress into plant areas of several units
- Station Blackout for extended period
- DC controlled Steam-driven cooling system & Ice condenser operated for limited periods

2012 Byron)

SBO for 8 min. immediately following Rx Trip: close call for seal LOCA (NRC BULLETIN 2012-01)



T. Koshy, NPT/IAEA

13

Event Statistics (1997-2012) IRS reports

- Failed/Affected Systems: Emergency core cooling - 202
- Significant degradation of safety function - 284
- Degradation of containment function/integrity- 44



T. Koshy, NPT/IAEA

14

Historic Successes

- Diesel-driven fire pump helped mitigation
- DC/Battery power controlled steam-driven cooling systems:
 - Reactor core isolation cooling
 - Steam driven auxiliary feed systems
 - Steam isolation condenser / heat exchanger
- Alternate AC sources manually aligned to a fault free bus helped core cooling



T. Koshy, NPTDS/IAEA

15

Lessons from History

- Approaches to address low frequency / high consequence events - **Loss of Vital AC Power**
 - Increasing diversity in core cooling could be more effective than increasing redundancy
 - Non-electric core cooling systems (PUMPS: diesel driven, steam driven-dc controlled, compressed air-driven, pressurized accumulators etc.,)



T. Koshy, NPTDS/IAEA

16

Emergency Core Cooling System

- Core Cooling Trains sized to mitigate a large break LOCA (guillotine break of RCS cold leg)
 - Three redundant trains of 100% capacity
 - Train outage for Tech. spec. surveillance with sufficient time for a thorough maintenance / surveillance while preserving adequate protection.
- Historic approaches
 - 3 trains of 50% capacity eg. (IP 2&3); New ABWR
 - European designs with four trains of 50% capacity



TKoshy, NPTDS/IAEA

17

Diversity in Core Cooling

- Standby power for non-electric cooling systems
 - Diesel, Air, Steam driven
 - Minimum of three non-electric cooling systems protected from regional extreme environments, strategically located: each one associated with a train (*Portable for severe accident conditions*)
 - Provision to cross connect power supply manually during emergency
 - Provision for external powering from skid mounted energy sources



Capability for remote operation

T. Koshy, NPTDS/IAEA

18

Diversity in Depressurization

- Depressurization – very critical for active & passive cooling system
 - *(generally achieved using multiple valves with the same technology)*
- Solutions:
 - Incorporate minimum of two approaches (electronically fired, pilot-air operated,..)
 - Retain manual capability with DC powered valves as a back up with provisions for external powering or fully manual



Capability for remote operation.
IAEA

T. Koshy, NPTDS/IAEA

19

Diversity for Preserving Containment Integrity

- Containment is the last defense
- Need to consider severe accident
- Solutions:
 - Redundant spray headers with cooling capability
 - Reliable hardened venting and filtration
 - Hydrogen detection and control
 - External provisions (portable equipment, etc.,)
 - containment cooling
 - Supplementing water supply for cavity flooding
 - Hydrogen control



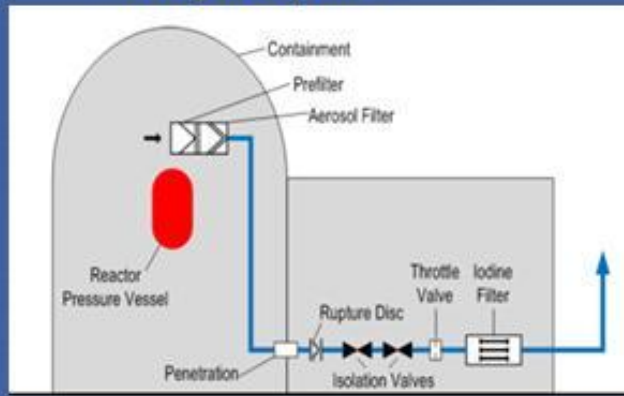
IAEA

T. Koshy, NPTDS/IAEA

20

Containment pressure & hydrogen control

CFVS – Containment Filtering Vent System



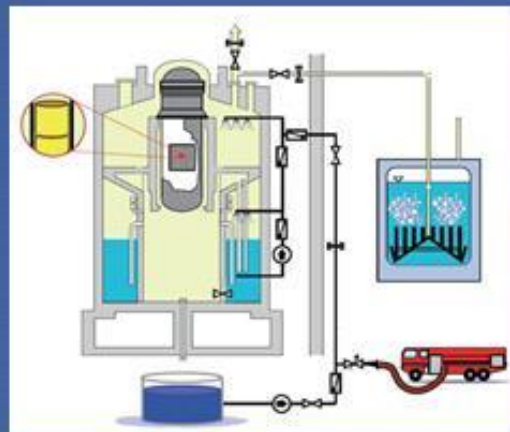
PAR – Passive Autocatalytic Re-combiners



21

Severe accident Mitigation System

- Installed after accident at TMI
- Passive and filtered containment pressure release
- Passive short term pressure release at large LOCA
- Possibility to flood containment
- Recovery options in case of lost heat sink
- Mobile independent systems (e.g. for power and hydrogen recombination)
- Transition plans (SSMFS 2008:17) add capability to mitigate effects of extreme external events



Robust Power System

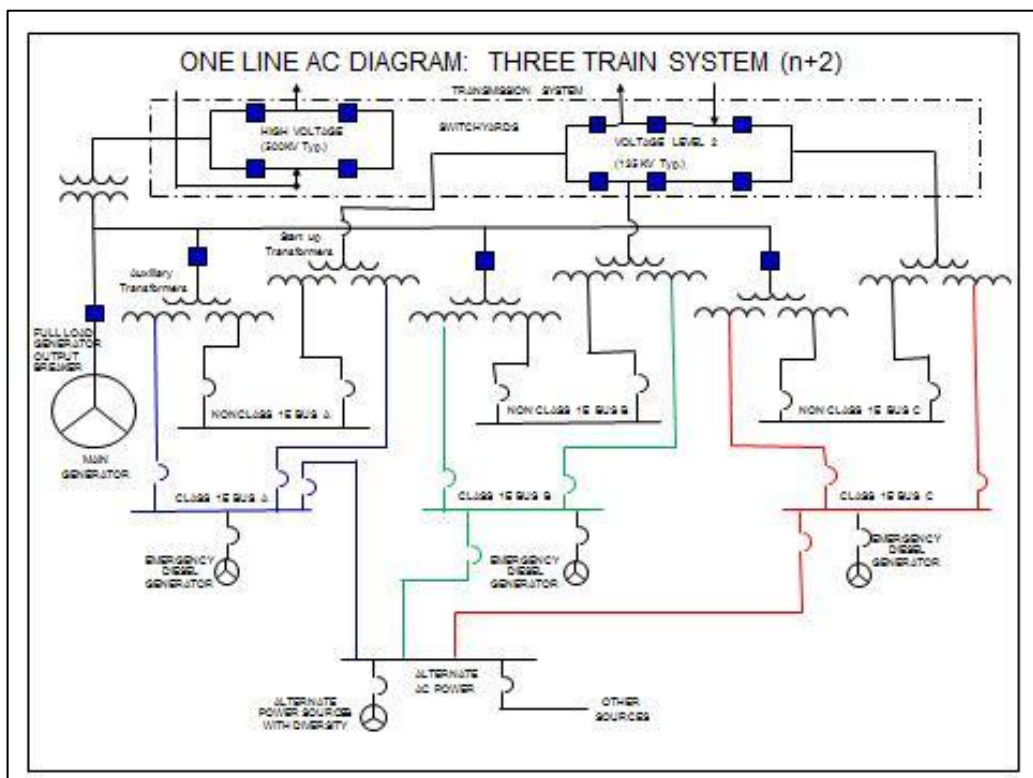
- Main Generator Output breaker
 - Prevent power interruption to onsite power systems following a generator trip (eliminates the need for fast transfer)
 - The additional cost is recovered if one plant trip is avoided
 - Two sources of offsite power made available to each safety bus for emergency and normal shutdown
 - It is desirable to upgrade the immediate switchyard providing offsite power to be built and electrically protected to a higher standard (*Fukushima lesson*)



IAEA

T. Koshy, NPT/IAEA

23



Safety Bus Line Up

- Offsite power needs to be fed directly to the safety bus without any intervening components to prevent other vulnerabilities.
- If safety bus is aligned to offsite power during normal operation, it should have another off site source for a fast transfer, and EDG power can be the third source of power (offsite power is the preferred source)
- All three phases of AC need monitoring & Protection (Byron Event: IN 2012-03), and Grid operator coordination to ensure capacity & immediate availability



T. Koshy, NPTDS/IAEA

25

Alternate AC Source

- Protected from anticipated external events specific to the region (seismic, flooding, hurricane, dust storm, forest fire, etc.,)
- Onsite fuel for a minimum of 7 days
- Minimum capacity to handle one full train of ECCS, one RCS / recirc. pump, and a service water pump concurrently for each unit that is supported.
- Black start capability



T. Koshy, NPTDS/IAEA

26

Alternate AC Source

- Standby power source for AAC needs to be from a minimum of two trains from a unit or one source from each unit (for multiple unit site) that is supported
- Protected, self-contained, with capability to remain on standby without any external power for 72hrs.
- Provisions for periodic full load test
- Auto-connected power sources are vulnerable to propagation of electrical failure
 - manual breaker line up after clearing the electrical fault is needed for AAC operation. (It is required for crediting it for SBO support)



IAEA

T. Koshy, NPTDS/IAEA

27

DC Power System (Typical of Three)

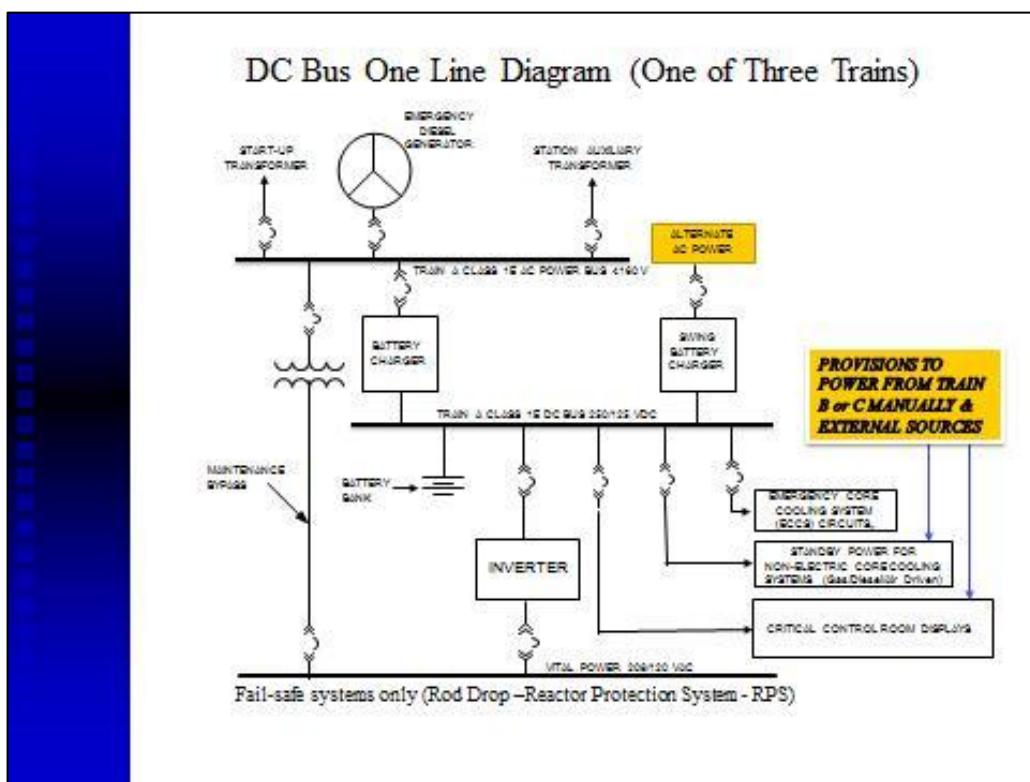
- Strategically located DC bus with two battery chargers with at least one connected to an alternate source
- DC power for ECCS actuation with its dedicated sensors and processing (Least intervening components to reduce failure modes – inverter, power supply modules etc., IEEE 603 concept)
Auctioneered power supply for increased reliability
- Reactor Protection System (RPS) powered from Vital AC (To be fail-safe such that any process signal with a logic or support system outside the acceptable band would trigger a reactor trip. IEEE 603 concepts)



IAEA

T. Koshy, NPTDS/IAEA

28



Questions ?



Thank you for your attention
t.koshy@iaea.org