Nuclear Safety
NEA/CSNI/R(2015)4/ADD1
March 2015
www.oecd-nea.org

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

ROBELSYS Workshop Proceedings
Paris, France
1-4 April 2014

Appendix 2 *(Cont'd)* **and Appendix 3**

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Unclassified **NEA/CSNI/R(2015)4/ADD1**

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/ADD1
Unclassified

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

Workshop Proceedings
Appendices 2 and 3

OECD Conference Centre, Paris, France
1-4 April 2014
Organised in co-operation with Institut de Radioprotection et de Sûreté Nucléaire

This document only exists in PDF.

JT03372213

Complete document available on OLIS in its original format

English text only

APPENDIX 2 *(Cont'd)*

PAPERS/PRESENTATIONS

SESSION FOUR

"Simulation of transients within NPP plant distribution systems"

Verification of Simulation Tools
Thierry Richard (EDF, France)

Standard Procedure for Grid Interaction Analysis
Bertil Svensson, Sture Lindhal, Daniel Karlsson (Gothia Power AB, Sweden), Jonas Jönsson, Fredrik Heyman (OKG AB, Sweden)

Electrical Dynamic Simulation Activities in Forsmark NPP
Per Lamell (Forsmarks Kraftgrupp AB, Sweden)

Introduction of Electrical System Simulation and Analysis used in Korean Nuclear Power Plants
Sang Hak Kim, Woo Sung Jeong (KEPCO, Korea)

Computer Simulation of Complex Power System Faults under Various Operating Conditions
Tanuj Khandelwal (ETAP, France), Mark Bowman (Tennessee Valley Authority, USA)

Verification of Simulation Tools

Thierry RICHARD
EDF, France

Abstract

Before qualifying a simulation tool, the requirements shall first be clearly identified, i.e.:

- What type of study needs to be carried out?
- What phenomena need to be modeled?

This phase involves writing a precise technical specification. Once the requirements are defined, the most adapted product shall be selected from the various software options available on the market.

Before using a particular version of a simulation tool to support the demonstration of nuclear safety studies, the following requirements shall be met.

- An auditable quality assurance process complying with development international standards shall be developed and maintained,
- A process of verification and validation (V & V) shall be implemented. This approach requires:
  - writing a report and/or executive summary of the V&V activities,
  - defining a validated domain (domain in which the difference between the results of the tools and those of another qualified reference is considered satisfactory for its intended use).
- Sufficient documentation shall be available,
- A detailed and formal description of the product (software version number, user configuration, other settings and parameters) in the targeted computing environment shall be available.
- Source codes corresponding to the software shall be archived appropriately.

When these requirements are fulfilled, the version of the simulation tool shall be considered qualified for a defined domain of validity, in a given computing environment.

The functional verification shall ensure that:

- the computer architecture of the tool does not include errors,
- the numerical solver correctly represents the physical mathematical model,
- equations are solved correctly.

The functional verification can be demonstrated through certification or report of Quality Assurance.

The functional validation shall allow the user to ensure that the equations correctly represent the physical phenomena in the perimeter of intended use.

The functional validation can be done by comparing simulation results with:

- actual test results,
- results obtained from other functionally validated simulation tools, supplemented if necessary by expert analysis.

The documents used for functional validation shall be properly referenced.

To ensure proper use of qualified software, a user guide shall be written.

Finally, the people carrying out studies with the software shall be adequately trained, certified and supervised. Quality audits shall be performed periodically to check the validity of the tool qualification over time as well as its proper use.

Paper

The scientific computing tools or simulation tools enable the simulation of physical phenomena requiring significant computing resources.

They consist of:

- calculation codes or solvers (for the mathematical treatment of physical equations),
- preprocessors (for data entry calculation),
- post-processors (for the exploitation of the results of calculation).

For each simulation tool, it’s important to define a main user (responsible for the use of the tool).

The objective is to have a sole expert in particular:

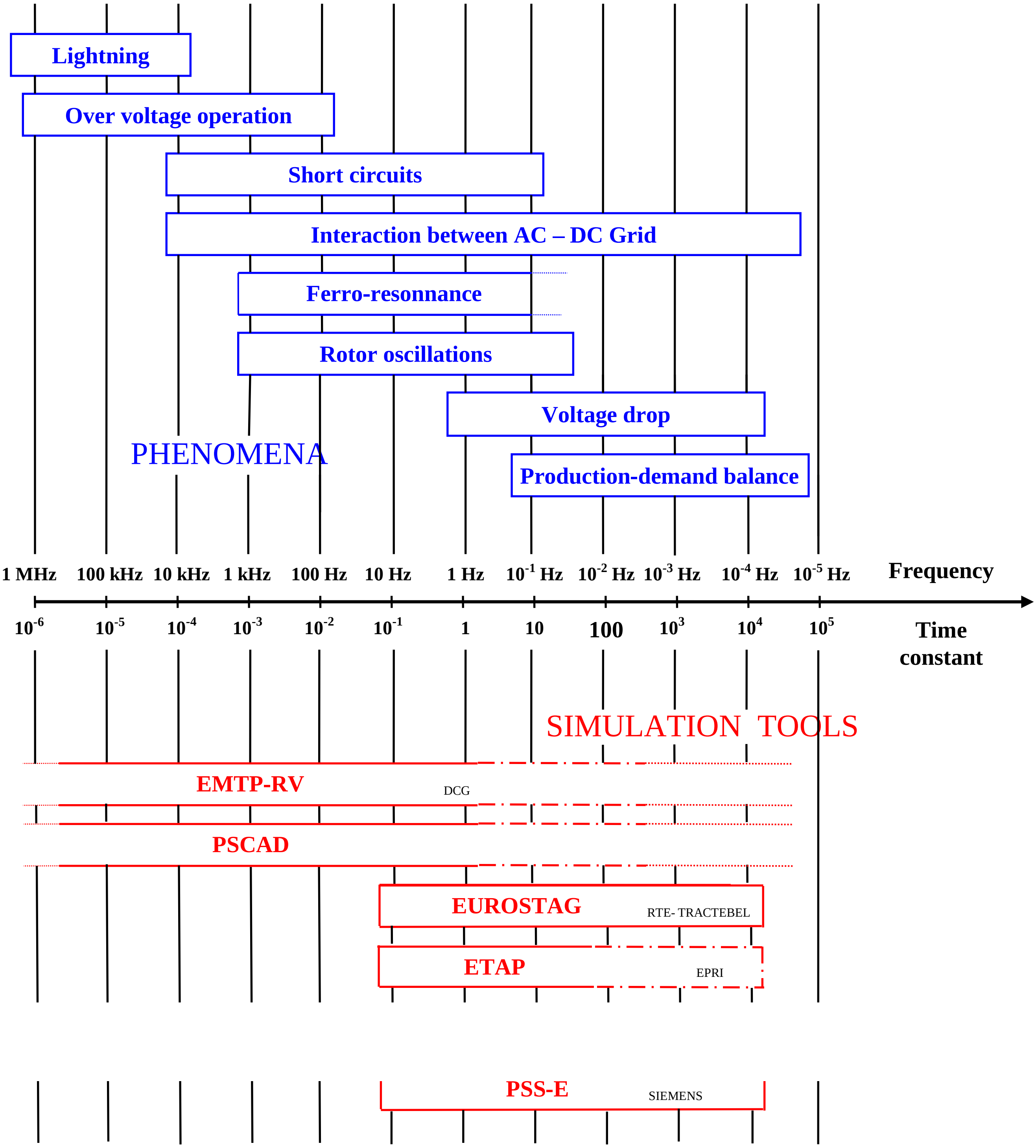
- to manage functional verifications and relationships with the developer or the seller,
- to write a user guide,
- to help and supervise less experienced users.

Before qualifying a simulation tool, the main user shall first clearly identify the requirements, i.e.:

- What type of study needs to be carried out?
- What phenomena need to be modeled?

This phase involves writing a precise technical specification. Once the requirements are defined, the most adapted product shall be selected from the various software options available on the market or be developed by a third party based on the technical specification.

A list of simulation tools allowing the study of the main electrical phenomena is proposed below.



For the simulation tools, the red dotted parts indicate that the tools can be used within these fields though they are not specifically designed for it.

For example, the reasons are that:

- the data to be used is not suitable because it is too voluminous and complex,
- the models to be used are different,
- the calculation time is too long.

Before using a particular version of a simulation tool to support the demonstration of nuclear safety studies, the following requirements shall be met (especially in case of the new development of a simulation tool):

- an auditable quality assurance process complying with development international standards shall be developed and maintained,
- a process of verification and validation (V & V) shall be implemented. This approach requires:
    - writing a report and/or executive summary of the V&V activities,
    - defining a validated domain (domain in which the difference between the results of the tools and those of another qualified reference is considered satisfactory for its intended use).
- sufficient documentation shall be available,
- a detailed and formal description of the product (software version number, user configuration, other settings and parameters) in the targeted computing environment shall be available.
- source codes corresponding to the simulation shall be archived appropriately.

When these requirements are fulfilled, the version of the simulation tool shall be considered qualified for a defined domain of validity, in a given computing environment.

When purchasing a commercial simulation tool, documentation shall be delivered by the seller. This documentation shall, at a minimum, include:

- documents relating to the design of the simulation tool,
- an operator manual.

The design documents should describe:

- the objectives and scope of the simulation tool ,
- the descriptions and explanations of physical models ,
- the descriptions and explanations of numerical methods,
- the technical databases used,
- if applicable, organizational principles of the sequence of calculations.

The operator manual should describe:

- the input data (type and size),
- how to manage and interpret the output results,
- the list of error messages,
- how models are ma de and used.

From the feedback obtained through use, the main user must complete this operator manual with recommendations. This feedback must be included in user guide note intended for inexperienced users (see here after).

The functional verification should be performed by the developer. This one shall ensure that:

- the software architecture of the tool does not include errors,
- the numerical solver correctly represents the physical mathematical model,
- equations are solved correctly.

The functional verification can be demonstrated through certification or report of Quality Assurance.

The functional validation should be performed by the main user. This one shall ensure that the equations correctly represent the physical phenomena in the perimeter of intended use.

The functional validation can be done by comparing simulation results with:

- actual test results,
- results obtained from other functionally validated simulation tools, supplemented if necessary by expert analysis.

The documents used for functional validation shall be properly referenced by the main user.

For each evolution of the simulation software or its environment, a study shall be carried out by the main user to analyze the impact of this modification. The results of this study shall classify the impact as minor or major.

- In the case of a minor impact (i.e. patch), non-regression tests shall be carried out,
- In the case of a major impact, all or part of the functional verification (by developer) and validation (by main user) process shall be repeated, according to the modifications made.

If the test results or the functional V & V process is successful then the new version shall be put into operation by the main user and the old version shall be archived and then removed from use.

To ensure proper use of qualified software, the main user shall write a user guide.

This user guide shall allow different users:

- to identify:
    - the different types of studies that should be performed with the software,
    - the models whose validity domain is consistent with the physical phenomena,
    - the necessary input data,
- to transform input data into a format recognized by the software (using spreadsheets),
- to create the necessary files to carry out the simulation,
- to achieve the same results, all other factors being equal.

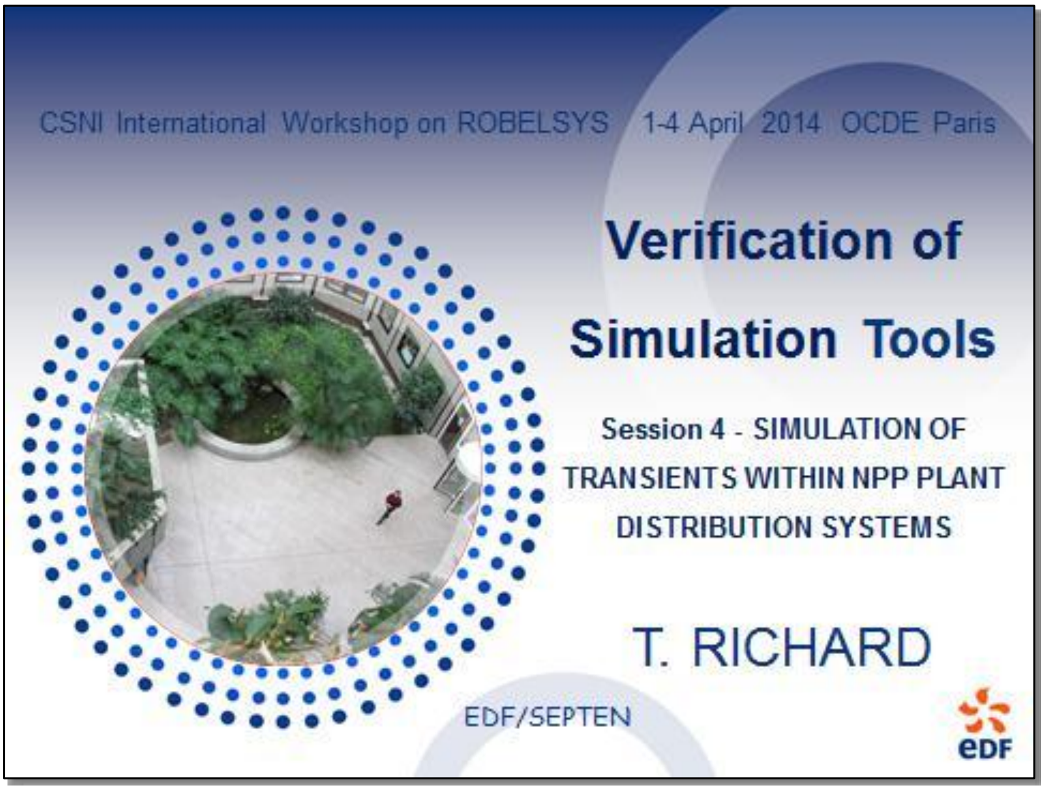
The spreadsheets shall be also quality checked by the main user.

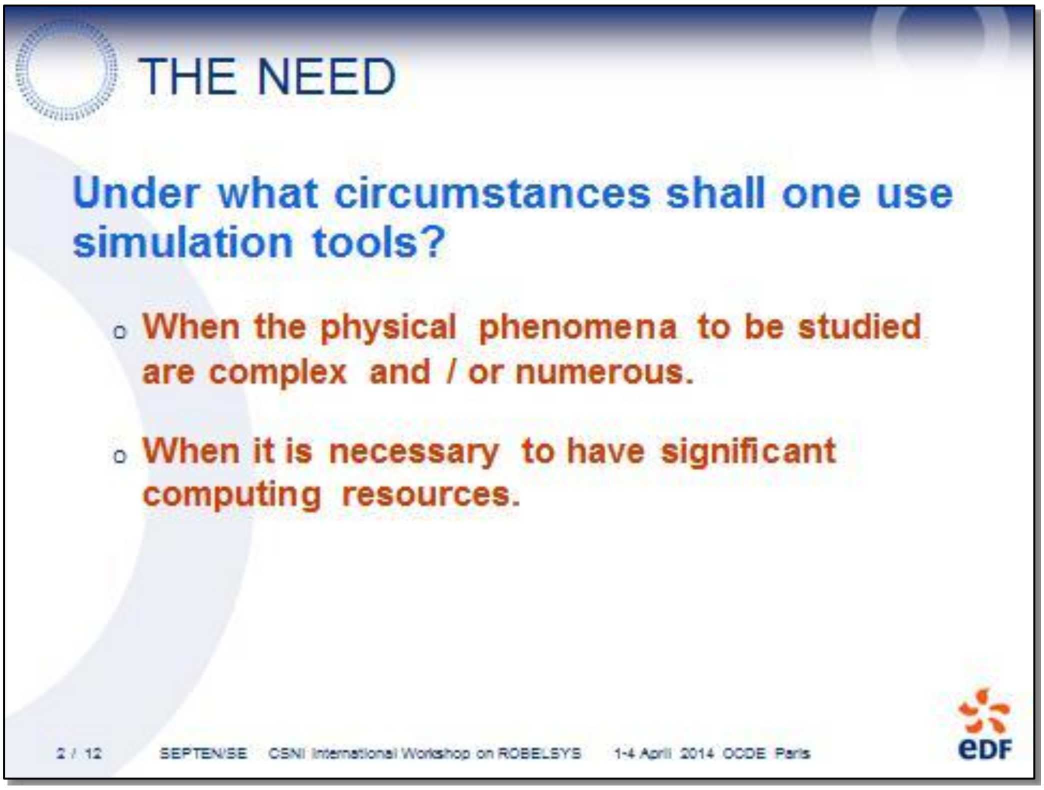
In addition to the validation aspect of the simulation tools, the user shall adjust the number of elements to be considered in the model depending on the type of study.

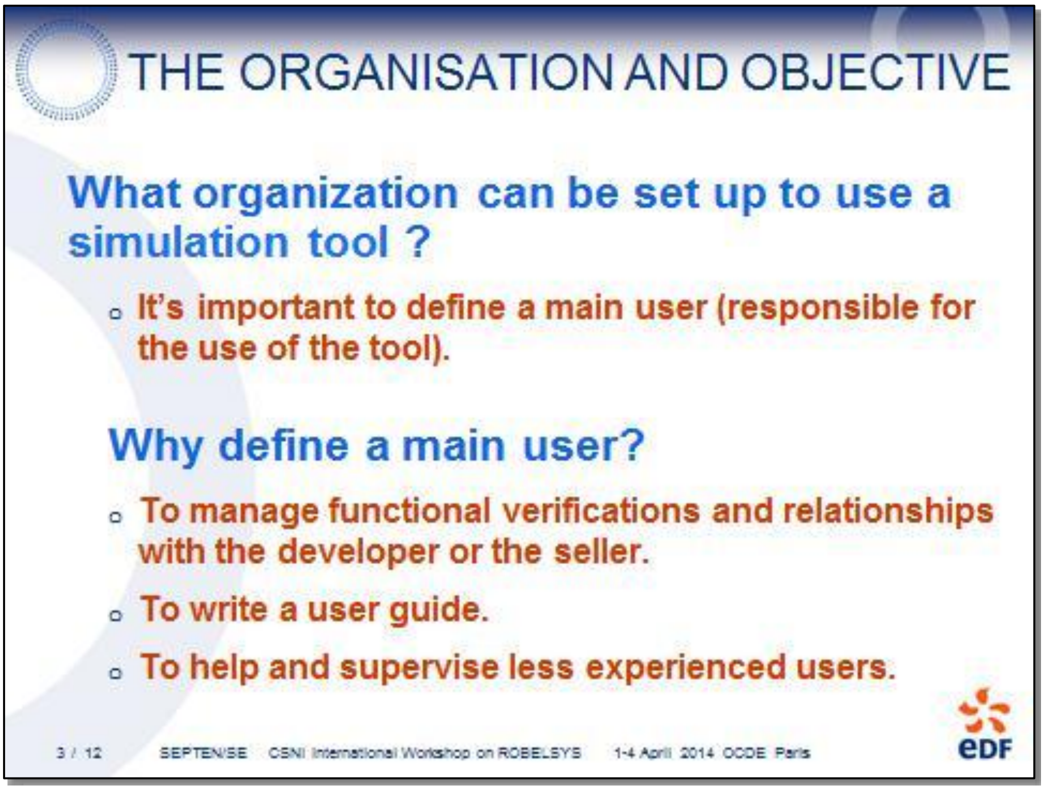
For example:

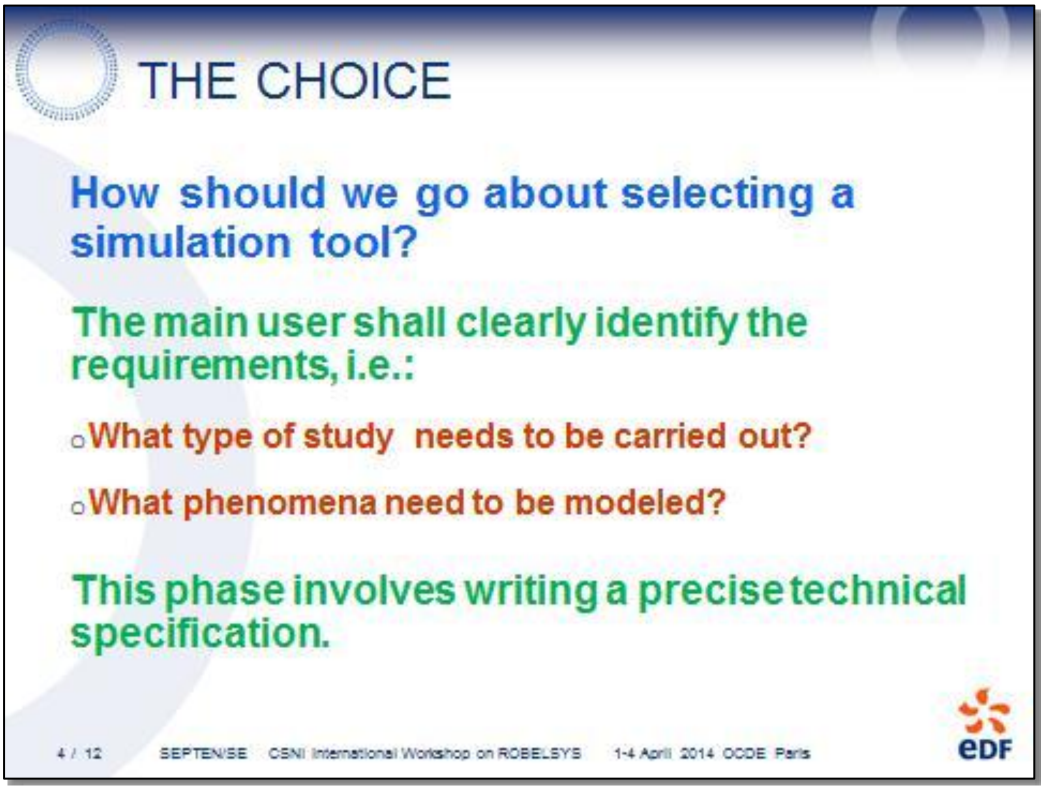
- For studies of transient behavior of auxiliaries supplied with alternative current (MV and LV):
    - all buses and transformers shall be modeled,
    - the load shall be divided according to its nature (rotating and non-rotating load),
- For transient stability studies, the model shall include:
    - the main generator with its regulators (voltage and speed),
    - the step-up transformer,
    - The HV network grid (generally represented by an equivalent model).

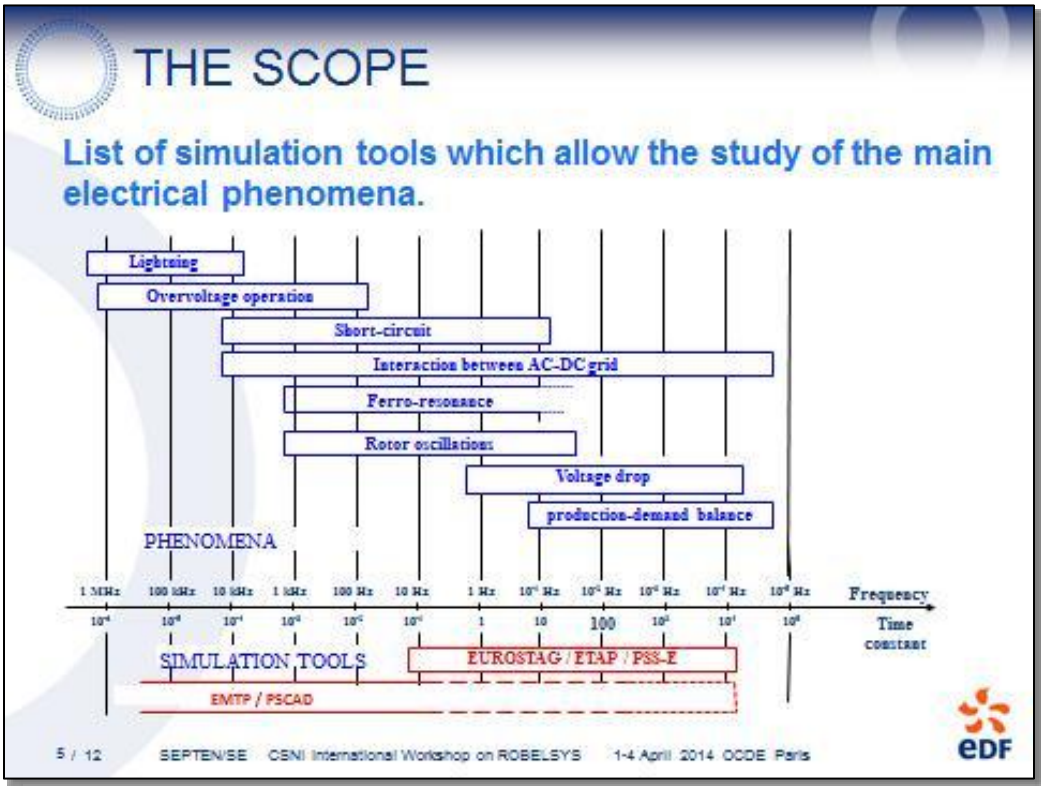
Finally, the people carrying out studies with the software shall be adequately trained, certified and supervised. Quality audits shall be performed periodically to check the validity of the tool qualification over time as well as its proper use.

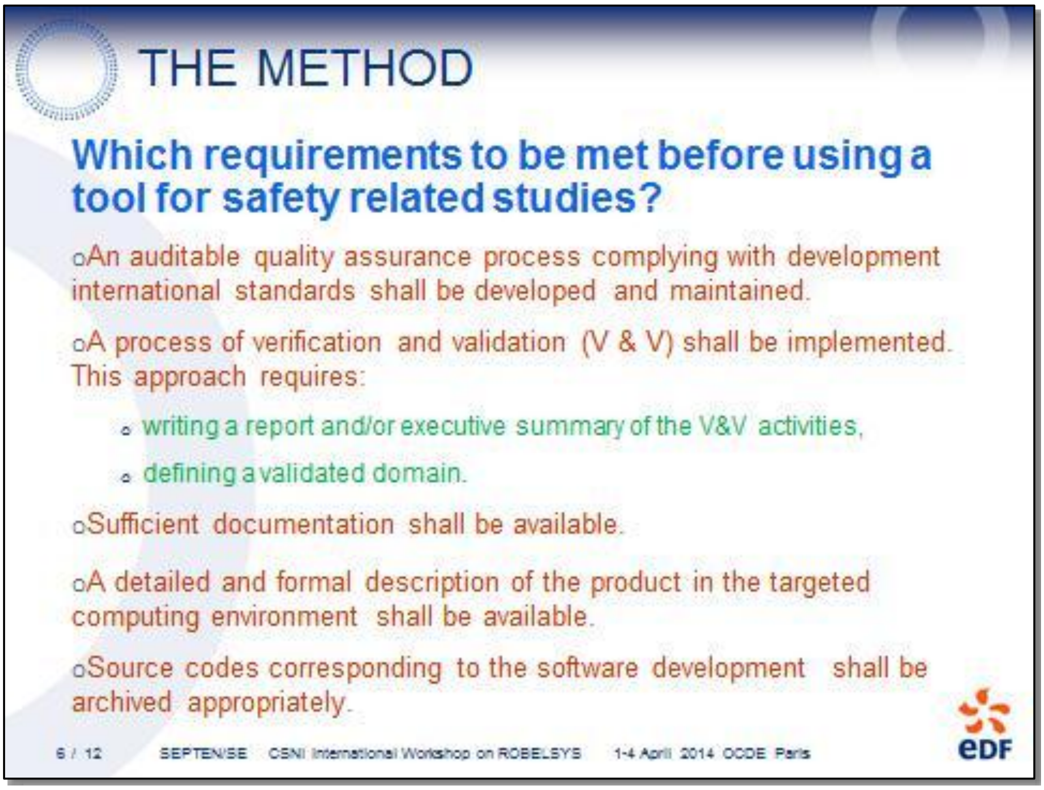

CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris
Verification of
Simulation Tools
Session 4 - SIMULATION OF
TRANSIENTS WITHIN NPP PLANT
DISTRIBUTION SYSTEMS
T. RICHARD
EDF/SEPTEN
eDF

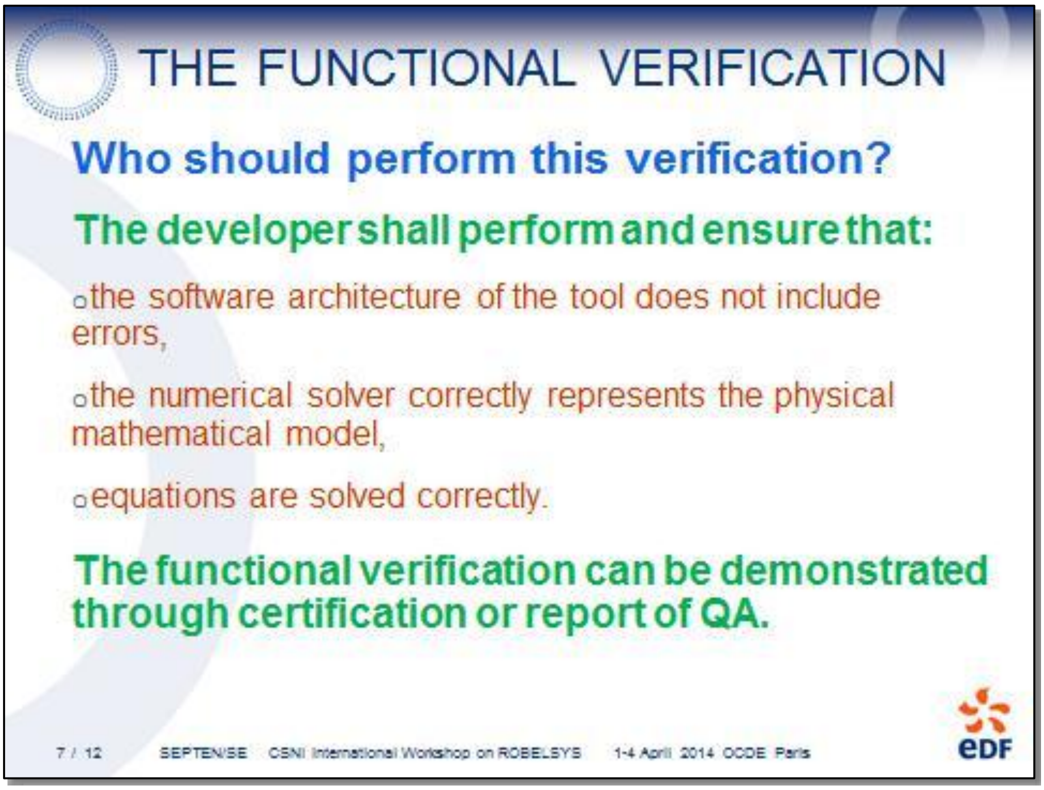

THE NEED
Under what circumstances shall one use simulation tools?
When the physical phenomena to be studied are complex and / or numerous.
When it is necessary to have significant computing resources.
2 / 12
SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris
eDF

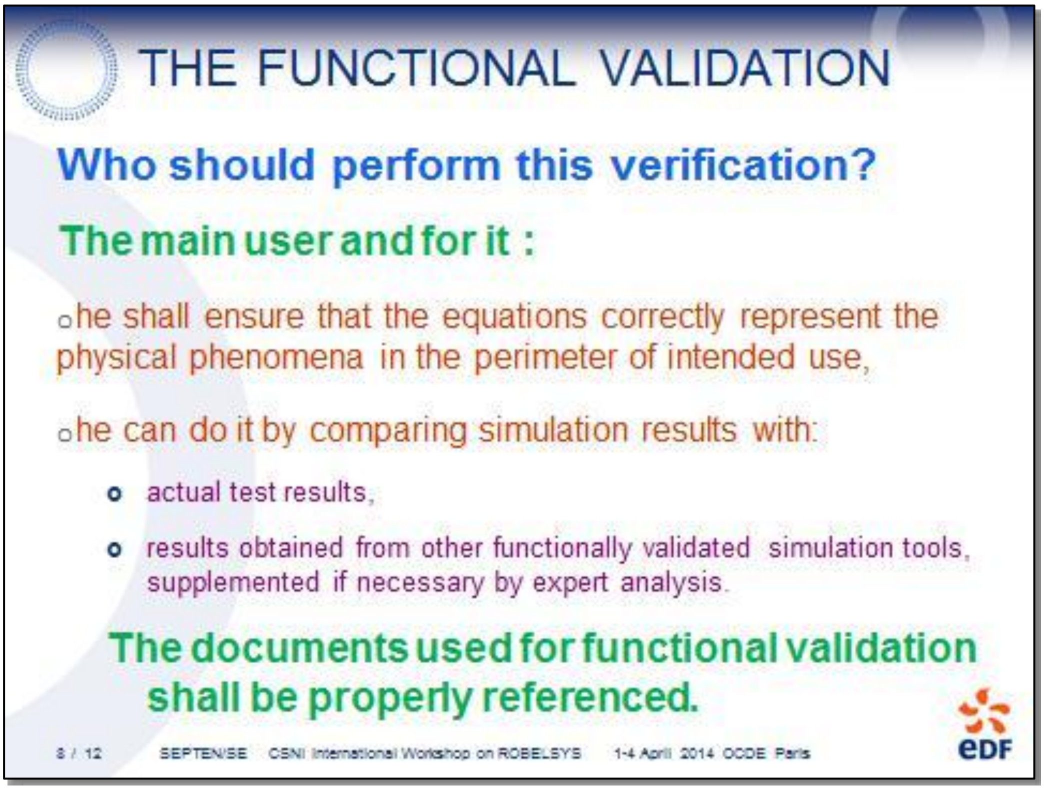

THE ORGANISATION AND OBJECTIVE
What organization can be set up to use a simulation tool ?
It's important to define a main user (responsible for the use of the tool).
Why define a main user?
To manage functional verifications and relationships with the developer or the seller.
To write a user guide.
To help and supervise less experienced users.
3 / 12
SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris
eDF


THE CHOICE
How should we go about selecting a simulation tool?
The main user shall clearly identify the requirements, i.e.:
What type of study needs to be carried out?
What phenomena need to be modeled?
This phase involves writing a precise technical specification.
4 / 12
SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris
eDF


THE SCOPE
List of simulation tools which allow the study of the main electrical phenomena.
Lightning
Overvoltage operation
Short-circuit
Interaction between AC-DC grid
Ferro-resonance
Rotor oscillations
Voltage drop
production-demand balance
PHENOMENA
1 MHz
100 kHz
10 kHz
1 kHz
100 Hz
10 Hz
1 Hz
Frequency
1
10
100
Time constant
SIMULATION TOOLS
EUROSTAG / ETAP / PSS-E
EMTP / PSCAD
5 / 12
SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris
eDF


THE METHOD
Which requirements to be met before using a tool for safety related studies?
○An auditable quality assurance process complying with development international standards shall be developed and maintained.
○A process of verification and validation (V & V) shall be implemented. This approach requires:
○ writing a report and/or executive summary of the V&V activities,
○ defining a validated domain.
○Sufficient documentation shall be available.
○A detailed and formal description of the product in the targeted computing environment shall be available.
○Source codes corresponding to the software development shall be archived appropriately.
6 / 12
SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris
eDF


THE FUNCTIONAL VERIFICATION
Who should perform this verification?
The developer shall perform and ensure that:
the software architecture of the tool does not include errors,
the numerical solver correctly represents the physical mathematical model,
equations are solved correctly.
The functional verification can be demonstrated through certification or report of QA.
7 / 12
SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris
eDF


THE FUNCTIONAL VALIDATION
Who should perform this verification?
The main user and for it :
he shall ensure that the equations correctly represent the physical phenomena in the perimeter of intended use,
he can do it by comparing simulation results with:
actual test results,
results obtained from other functionally validated simulation tools, supplemented if necessary by expert analysis.
The documents used for functional validation shall be properly referenced.
8 / 12
SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris
eDF

NEW VERSION / UPDATES

Which actions to be performed?

The main user should analyze and classify the impact as major or minor.

- In the case of minor impact (i.e. patch), the non-regression tests shall be carried out.
- In the case of major impact, all or part of the functional verification (by developer) and validation process (by main user) shall be repeated, according to the modifications made.

If the test results or the functional V & V process are successful then the new version shall be put into operation.

9 / 12 SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris eDF

GOOD USE

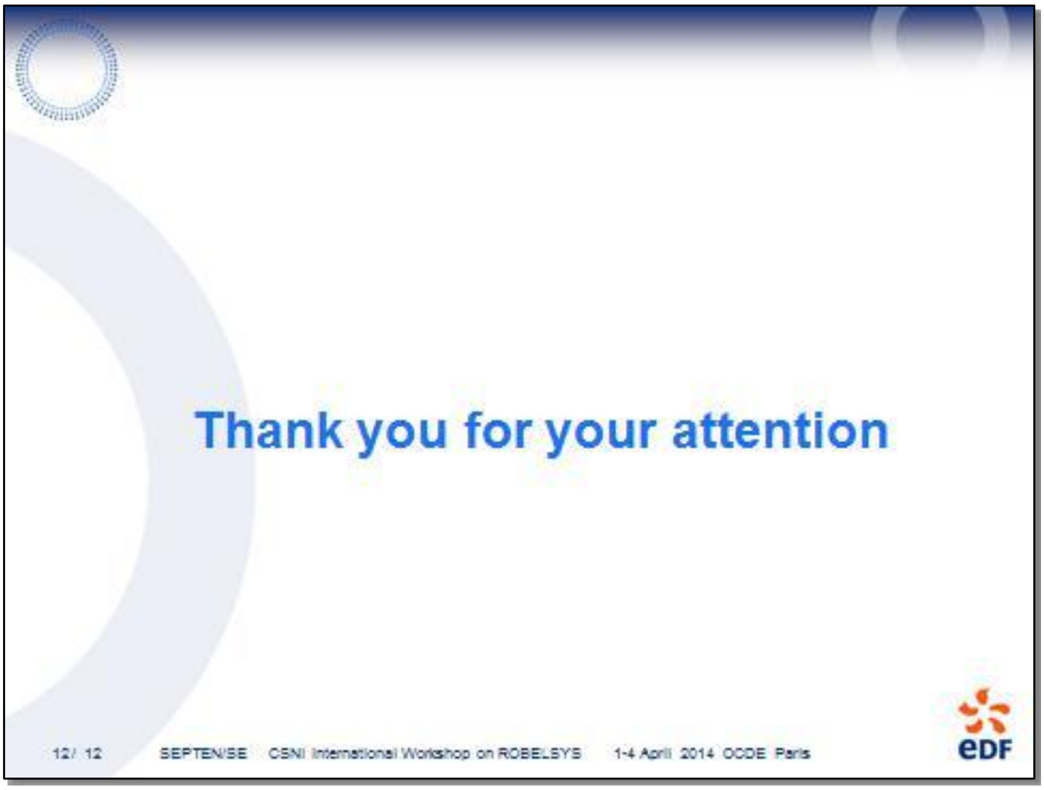
How ensure proper use of qualified tools?

The main user shall write a user guide which shall allow different users:

- to identify the:
  - different types of studies that should be performed with the software,
  - models whose validity domain are consistent with the physical phenomena,
  - necessary input data,
- to transform input data into a format recognized by the software (using spreadsheets),
- to create the necessary files to carry out the simulation,
- to achieve the same results, all other factors being equal.

10/ 12 SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris eDF


SUSTAINABILITY
How maintain the use of qualified tools?
People carrying out studies with the software shall be adequately:
o trained,
o certified,
o supervised.
Quality audits shall be performed periodically to check over the time:
o the validity of the tool qualification,
o its proper use.
11/ 12
SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris


Thank you for your attention
12/ 12
SEPTEN/SE CSNI International Workshop on ROBELSYS 1-4 April 2014 OCDE Paris

Standard Procedure for Grid Interaction Analysis

Bertil Svensson, Sture Lindahl, Daniel Karlsson
Gothia Power AB, Sweden

Jonas Jönsson, Fredrik Heyman
OKG AB, Sweden

Abstract

Grid events, simultaneously affecting all safety related auxiliary systems in a nuclear power plant, are critical and must be carefully addressed in the design, upgrading and operational processes. Up to now, the connecting grid has often been treated as either fully available or totally unavailable, and too little attention has been paid to specify the grid performance criteria. This paper deals with standard procedures for grid interaction analysis, to derive tools and criteria to handle grid events challenging the safety systems of the plant. Critical external power system events are investigated and characterised, with respect to severity and rate of occurrence. These critical events are then grouped with respect to impact on the safety systems, when a disturbance propagates into the plant. It is then important to make sure that 1) the impact of the disturbance will never reach any critical system, 2) the impact of the disturbance will be eliminated before it will hurt any critical system, or 3) the critical systems will be proven to be designed in such a way that they can withstand the impact of the disturbance, and the associated control and protection systems can withstand voltage and frequency transients associated with the disturbances. A number of representative disturbance profiles, reflecting connecting grid conditions, are therefore derived, to be used for equipment testing.

1. Introduction

The Fukushima Daiichi accident, very clearly pointed out the importance of the common cause failure in the planning and operation of auxiliary and safety systems of nuclear power plants. The connecting grid during normal operational conditions is such a common factor for many important auxiliary systems. The analysis within the nuclear power industry has for long been focused on the two very distinct conditions, the connecting grid available or the connecting grid not available. However, very little focus has been put on how to distinguish a fully reliable and healthy connecting grid from a situation where the power plant auxiliary systems have to be disconnected from the grid. The disconnection criteria must be based on the compatibility between the grid and the auxiliary equipment.

The need to enhance the analyses of grid and plant interaction is recognized in order to better define the enveloping profiles that could challenge the plant's safety systems. Simulations of dynamic behaviour outside and inside the plant as well as testing are important methods. The proposed standard procedure is based on experience from studies of the interaction between the Swedish transmission grid and the three nuclear power plants at Ringhals, Forsmark and Oskarshamn, [1]. Two different typical grid connections and auxiliary system supplies are shown in Figure 1, Oskarshamn 2 (O2) and Oskarshamn 3 (O3). For O3 the auxiliary system can also be partly supplied from the 130 kV system, as backup, and totally supplied from the 130 kV system during maintenance.

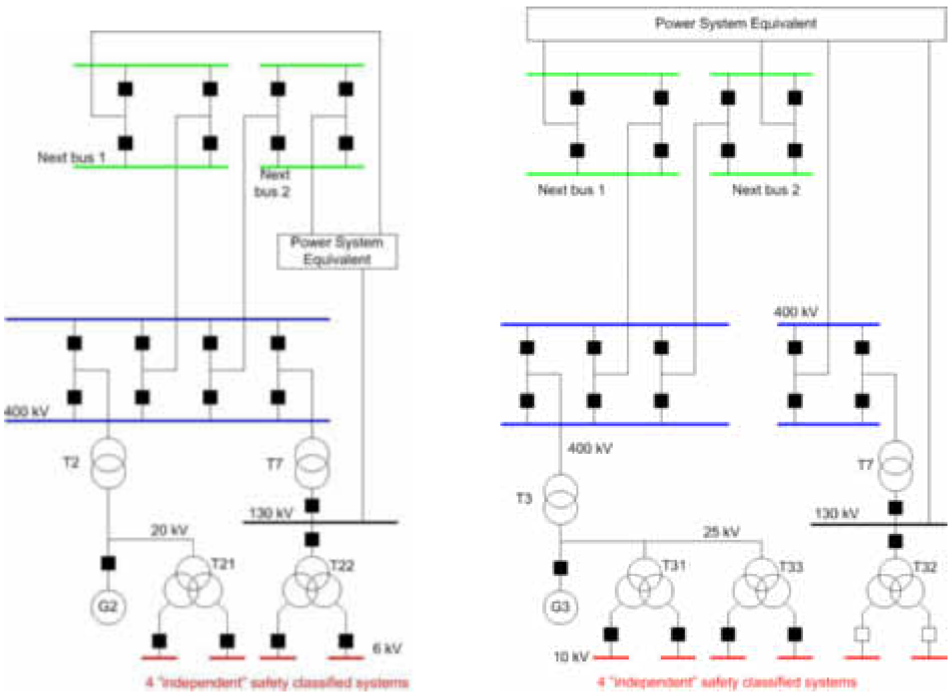


Figure 1   Typical NPP grid connection and auxiliary system supply (O2 and O3)

2. System compatibility and equipment testing

The proposed standard procedure focuses on the calculation of temporary voltages on the buses in the auxiliary power systems of the nuclear power plants caused by events in the external power system (the transmission network, the step-up transformer, and the main generator). There is a need to verify that the safety related equipment energized from the auxiliary power system can withstand the transients caused by credible events on the external power system. Equipment manufacturers are not keen to provide detailed simulation models, and testing of the physical equipment may be the only way to verify the required withstand capability. For such testing, well defined, relevant, and generally accepted, test profiles are needed. These profiles must be based on recordings of credible events and simulations of a large number of possible incidents.

The main steps for the proposed standard procedure for grid interaction analysis are listed below.

1) Collect necessary data
   a. Data for fault calculation
   b. Data for dynamic simulation
   c. Information about protection systems
   d. Transformer data
   e. Motor data
2) Derive the grid dynamic equivalent
3) Define events and blackout scenarios, and the corresponding grid disturbance profiles
4) Perform dynamic simulations of grid disturbances
5) Study the simulation results at different levels in the internal auxiliary systems
6) Specify disturbance profiles for equipment testing
7) Verify withstand capability of the equipment by full scale testing

3. Disturbance profile Method

The use of synthetic disturbance profiles has not been very common within the nuclear power area, so far. However, the use of statistics and probabilistic methods is very common, and disturbance profiles are used within other segments of the electric power sector. The most typical and well known is probably the lightning and switching impulses (IEC 60060-1), where an infinite number of possible impulses, caused by lightning or switching, are condensed into two standard profiles; one for lightning and one for switching. A distinction is made between lightning and switching impulses on the basis of the front duration. Impulses with front duration up to 20 μs are defined as lightning impulses and those with longer fronts are defined as switching impulses, see Figure 2.

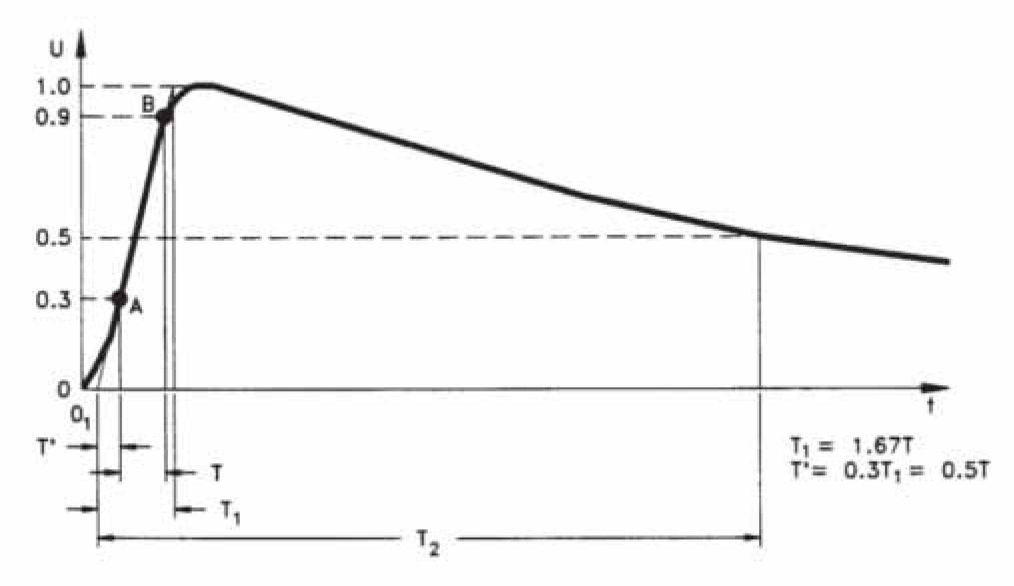


Figure 2 Standard lightning and switching impulse, according to IEC 60060-1

The standard lightning impulse is a full lightning impulse having a front time of 1.2 μs and a time to half-value of 50 μs (1.2/50 impulse). The standard switching impulse is an impulse having a time to peak of 250 μs and a time to half-value of 2500 μs (250/2500 impulse). A similar use of standardized profiles and wave shapes are also used within control and protection specification and testing (e.g. IEC 60255-26 ”Measuring relays and protection equipment – Part 26: Electromagnetic compatibility requirements”).

Disturbance profiles, with respect to voltage magnitude and/or frequency, are also used in many grid codes, especially to illustrate the fault-ride-through criteria. The fault-ride-through requirements are a bit different in different systems. The Swedish fault-ride-through requirement applicable to all nuclear units is shown in Figure 3. It has to be emphasized that the profile is not at all any power quality indication of the grid properties. It is a pure requirement, stating that the connected generating unit must be able to remain grid connected and continue its power output, as long as the voltage, on all the phases in the connected closest meshed network point, stays above the voltage profile shown in Figure 3.

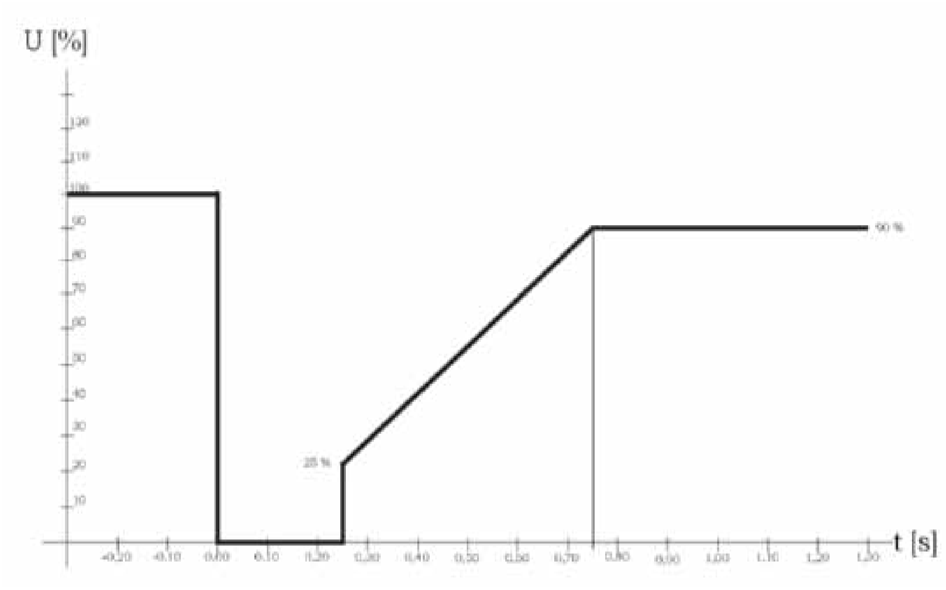


Figure 3 The Swedish grid code fault-ride-through requirement for large plants (SvKFS 2005:2)

Based on earlier experience with synthetic profiles, 13 disturbance profiles, derived for the OKG NPP, are described and evaluated, as well as their tentative impact on the auxiliary power system. In this section a number of critical grid disturbances affecting the operation of the nuclear unit auxiliary power system are analysed. The specific profile derived for a group of events, should in a “reasonable way” represent “the worst case”. Figure 4 illustrates how a number of offsite grid disturbances are grouped to be represented by one disturbance profile; 400 kV line fault with backup clearance due to breaker failure (left), and 400 kV busbar fault with backup clearance due to failure to operate of the busbar protection (right).

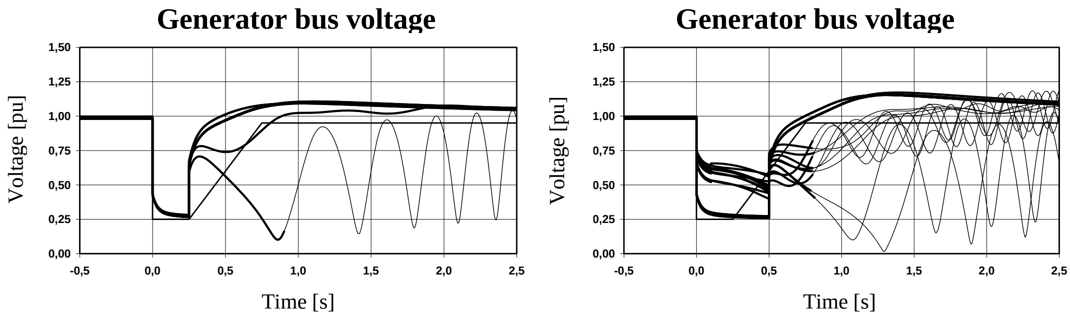


Figure 4 Different scenarios represented by one profile, line fault (left), bus fault (right)

3.1 Procedure overview

The procedure proposed is focused on the evaluation of the connecting grid conditions. As long as the auxiliary and safety systems are supplied from the connecting grid, the connecting grid is a common source. The problem is to decide when the connecting grid is not reliable and the auxiliary power system should be disconnected from the external power system, and to specify the related conditions. The procedure can be split into a number of steps:

1) Study the connecting grid, and evaluate what could happen. Here it is very important not to stop the evaluation with disturbances regarded as credible within the grid companies. Disturbance

occurrences as once every twenty year or once every hundred year are, among grid companies, regarded as extremely rare, while such incident rates within the nuclear power industry are highly frequent. The following events, affecting the conditions on the generator bus or in the grid connection point of the NPP, and thereby the auxiliary and safety system supplies, should be regarded:

a. Load rejection, i.e. disconnection of the unit and its auxiliary systems from the grid.

b. Primary shunt disturbance faults, such as short circuits and earth faults,
   - cleared by the ordinary protection system
   - cleared by the backup protection system

c. Abnormal system frequency in the connection point,
   - due to loss of generation – dynamic / static
   - due to loss of load – dynamic / static

d. Abnormal operational voltage in the connection point,
   - high voltage due to external conditions
   - low voltage due to external conditions

2) Group the events, studied in 1), with respect to the resulting voltage stress, with respect to magnitude and frequency level, structure, and duration, on the auxiliary and safety systems, into a limited number of groups.

3) Assign a synthetic, well defined, disturbance profile (voltage magnitude/frequency) for each group, according to 2).

4) Study the impact on the auxiliary and safety systems, when the disturbance profiles according to 3) are applied.

5) Derive the corresponding event rate of occurrence for each of the disturbance profile impacts derived in 4).

6) For all credible disturbances, according to the event rate of occurrence derived in 5), it has to be ensured that the equipment can either withstand the stress caused by the disturbance profile, or that the unit will be disconnected from the grid.

The work was organized in a number of packages, and each unit was studied separately (in the OKG NPP there are three units). Firstly the disturbance profiles were defined and characterized. For the OKG units 13 profiles were identified, while for other NPPs the number of disturbance profiles might be different, since the disturbance profile will be different for a unit with a static exciter, compared to a unit with a rotating exciter. When the disturbance profiles, as they appear at the unit connection point or on the generator bus, are defined, a simulation study is initiated to investigate how the applied disturbance profile propagates into the auxiliary systems. A large part of this study is to compare the disturbance profile propagation and resulting stress at different levels and points in the auxiliary system with the protection relay characteristics and settings, to really see the impact of the disturbance profile under study. For the simulation study, where a transient analysis program like PSCAD/EMTDC has to be used, the modelling of the components in the auxiliary system, such as transformers, induction machines, and power electronic converters, is extremely important, and large efforts have been made to achieve accurate models for the extreme conditions studied, such as high and low voltage magnitudes, and high and low frequencies. In parallel with the simulation study, the event rate of occurrence for each disturbance profile was calculated, as the sum of the event rates of occurrence for the group of events represented by that specific disturbance profile. For load rejection there are quite reliable statistics available. For short circuits and earth faults in the connecting grid, statistics are available for each type of power system component, and a lot of unit specific calculations have to be performed. For abnormal grid conditions with respect to frequency and voltage magnitude, often referred to as wide area disturbances, operational experience and "degree of belief" are applied.

When the stress on each voltage level in the auxiliary system, and the corresponding event rate of occurrence are determined, the stress, with respect to actions from the protection system, has to be compared to the withstand capability of the critical appliances, such as induction machines and power electronics. If shortcomings are identified, there are basically three ways to proceed, 1) to eliminate the stress on the critical level, e.g. surge arresters on higher levels to limit overvoltages, 2) enhanced protection systems to transfer to emergency diesel supply, e.g. for long duration low voltage situations to avoid induction motor stalling, and 3) to reinforce the appliance to make sure it will withstand the stress, e.g. redesign of power electronics and UPS appliances. This analysis is made separately for safety systems and for operational systems.

If severe shortcomings are identified, the unit has to be stopped to eliminate the shortcoming identified. If less severe insufficiencies or potential improvements are identified, these are listed in so called Recommendation reports, one for each unit. These recommendations are then handled within the normal plant organization and action plans for implementations are set. Finally, the improvements for increased robustness are implemented in the plant.

3.2 Load rejection

Load rejection, e.g. trip of the unit, most likely at full load and unwantedly, with the unit circuit-breaker, causes a temporary overvoltage on the generator bus. The shape, peak and duration of this overvoltage depend on the excitation system. With the automatic voltage regulator (AVR) in operation, the overvoltage will be limited to some 20-25%, while with the AVR in field current control mode, the overvoltage might reach 50%, and last for quite a long time. Load rejection, for a unit with a static exciter, is shown with and without AVR control in Figure 5.

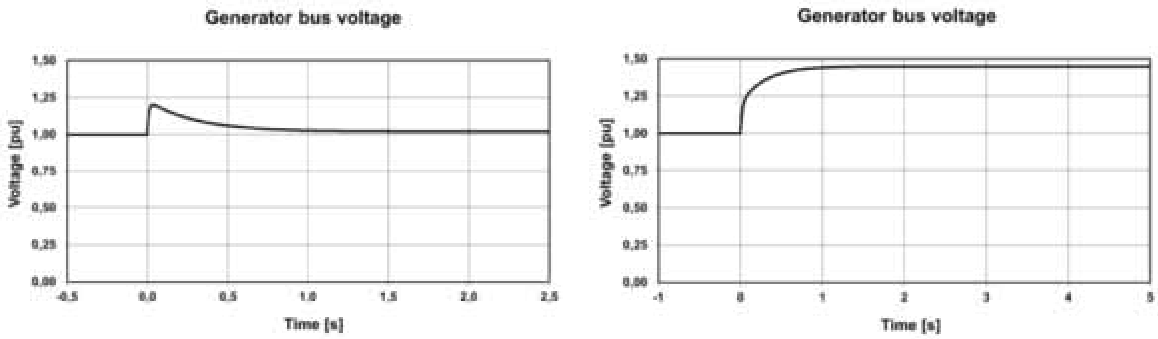


Figure 5 Generator bus voltage at load rejection with AVR (left) and with fixed field current (right)

3.3 Symmetrical and unsymmetrical short circuits in the grid

Short circuits and earth faults in the connecting grid, see Figure 1, might appear at different locations, thus triggering different fault clearing procedures. Furthermore, correctly cleared faults, as well as backup fault clearance, have to be addressed. Figure 6 shows the disturbance profile representing correctly cleared nearby short circuits. The left figure illustrates a trip of the unit circuit-breaker (100 ms), and transfer to house load operation. The disturbance profile is valid for a single bus or a double bus system with one of the busses out of operation. The right figure shows a correctly cleared (100 ms) nearby line fault, where the generator remains connected to the grid, and the voltage magnitude slowly returns to a level slightly below the pre-fault level.

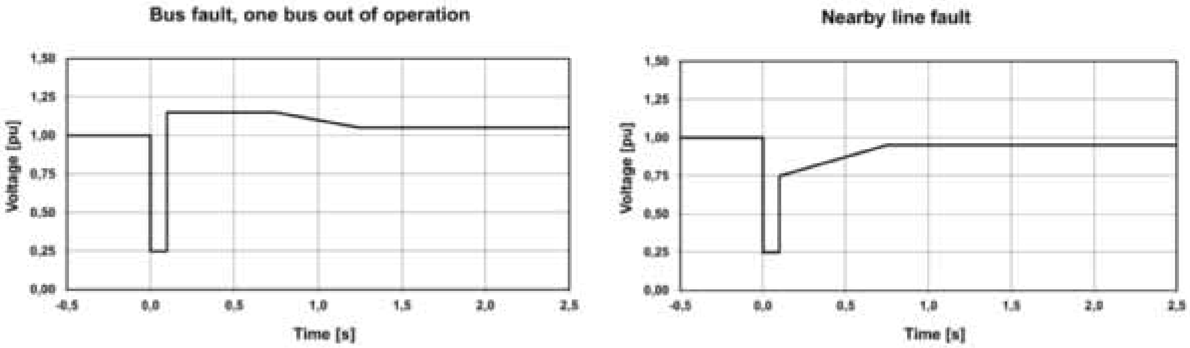


Figure 6 Correctly cleared, busbar fault, one bus out of operation (left), and nearby line fault (right)

Figure 7 shows backup fault clearance of busbar and line faults, with fault duration of 500 ms. For the busbar fault (left), one bus is out of operation, the bus protection is supposed to fail to operate and the fault is cleared by remote zone 2 distance protection, thus the long fault clearing time. Finally the unit is supposed to successfully transfer to house load operation, with a slight overshoot in voltage. For the remote end line fault (right), all telecommunication is supposed to be out of service, and the fault is cleared by the remote zone 2 distance protection, after about 500 ms. The voltage recovery is slower than for the correctly cleared fault due to the longer deceleration time for the rotating machines and the corresponding more demanding reacceleration. This fault illustrates that the fault duration might be longer than according to the fault-ride-through requirement as stated by the grid code, see Figure 3. Therefore, the generator is allowed to trip due to such a long duration fault. With double busbar protection and double communication channels, which is the present design level in the Swedish transmission system, the probability for these long fault duration times will be negligible. Thus, the circuit-breaker is the only component without redundancy.

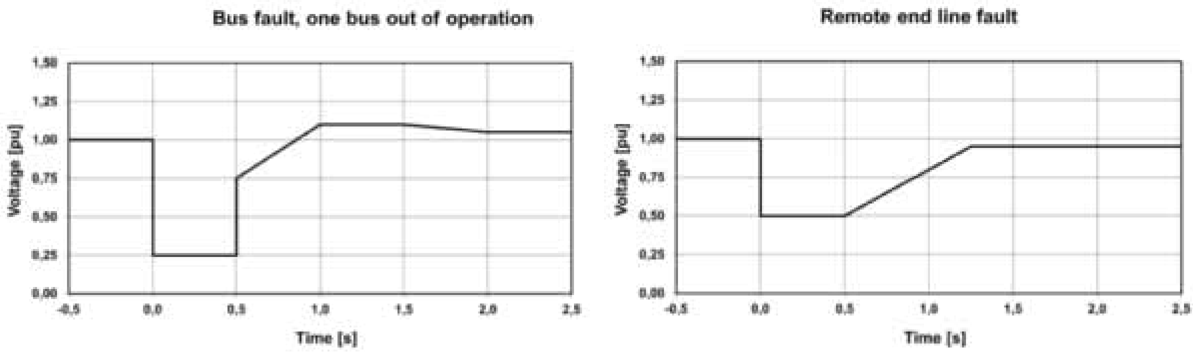


Figure 7 Backup cleared, busbar fault, one bus out of operation (left), and remote end line fault (right)

Unsymmetrical shunt faults, i.e. earth faults and two-phase faults, cause, not only a voltage dip, but also a phase shift, at the fault occurrence, and at the fault clearance. Also symmetrical faults might cause phase angle jumps. Such a phase shift might be critical for power electronic based equipment, such as switched converters or UPS devices. A nearby single phase-to-earth fault is shown in Figure 8 for backup clearance due to a breaker failure. The voltage reduction during the fault is quite moderate, while the phase angle jump, especially at the fault clearance is quite significant.

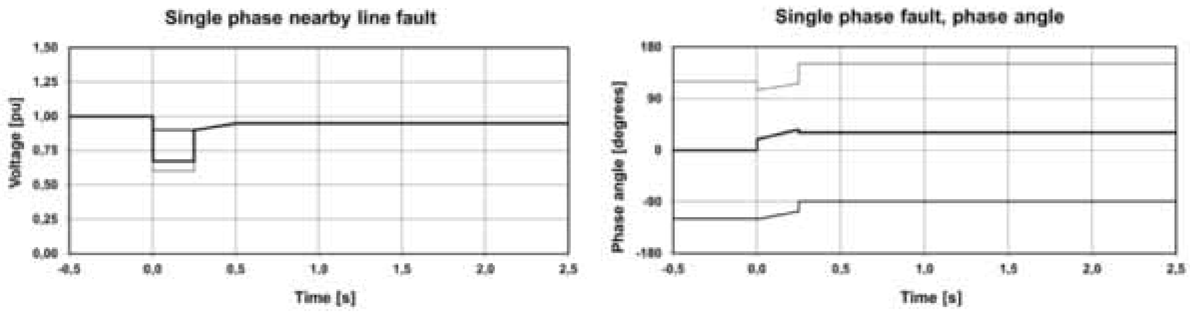


Figure 8 Single phase nearby fault with backup clearance, magnitude (left) and phase angle (right)

3.4 Loss of generation

Sudden loss of a large amount of generation (or load) causes a significant frequency dip (rise). The lowest credible frequency in the Nordic system is 47.5 Hz. If the frequency goes lower, some nuclear units have to be tripped. Frequency rises are regarded as less critical than frequency dips. In Figure 9, the frequency dip after a very large loss of generation is shown. The frequency goes almost all the way down to 47.5 Hz, and then slowly recovers to something around 49.5 Hz after about one minute. This frequency disturbance profile describes a worst case scenario, since there is a load shedding scheme in five steps starting at 48.8 Hz, and disconnecting 50% of the load by 48.0 Hz. This load shedding scheme has operated a few times in the seventies. In 1979, two steps of the load shedding scheme operated and saved the system from a blackout, see the right part of Figure 9.

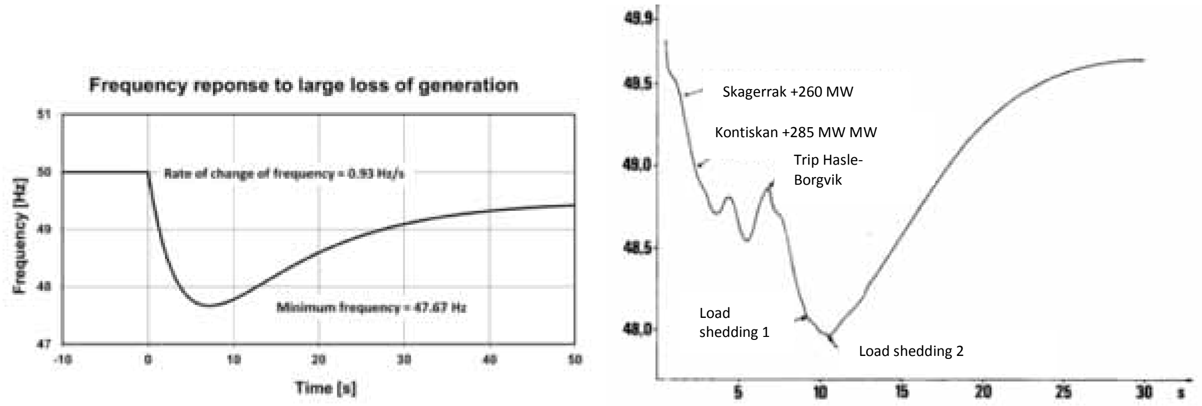


Figure 9 Frequency drop due to a large loss of generation, profile (left) and recording (right)

3.5 Voltage instability conditions

Voltage instability conditions are the most probable cause of a wide-area disturbance in the Nordic system. Blackouts have been experienced in 1983 and 2003. A voltage instability incident could be characterized as short-term or long-term, depending on the disturbance as such, but also on the point of observation. In the south end of the Swedish system there are some large generators, capable of keeping up the local voltage in case of loss of transmission capacity in the middle or north part of the country, resulting in a disturbance recognized as a slow voltage collapse (in the range of minute) in the middle of the system where the voltage depression is observed and realised, and a fast voltage collapse (in the range of seconds) in the south part, only observed at the final breakdown. Figure 10 shows the voltage magnitude and frequency profiles, for a fast or short-term voltage collapse.

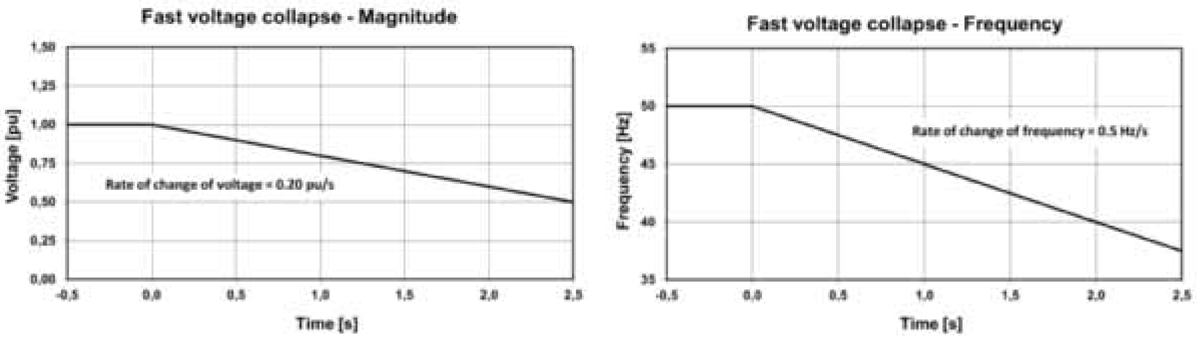


Figure 10 Short-term voltage instability, magnitude (left) and frequency (right)

The long-term voltage instability scenario is characterised by a sudden transmission capacity reduction, large enough to significantly reduce the voltage at the load end of the system, but not large enough to immediately ruin the system stability. The initial voltage reduction is typically 10 to 15%. However, the load recovery and the tap-changer control in the distribution system will partly restore the load and further reduce the transmission system voltages. After a while the voltage is so low and the current is so high that some distance protection relay picks up and trips a transmission line. Parallel paths will then be overloaded and we have a cascaded tripping, resulting in a blackout. Figure 11 shows the synthetic profiles for the voltage magnitude and frequency, for a slow or long-term voltage collapse. A more rare form of voltage instability is voltage depression, where the voltage magnitude slowly goes down to about 80%, with a corresponding increase in frequency to about 51 Hz. These conditions are very similar to the initial phase of the slow voltage collapse, but the voltage depression stops, the voltage stays low, and for some reason the voltage recovers and a collapse is avoided.

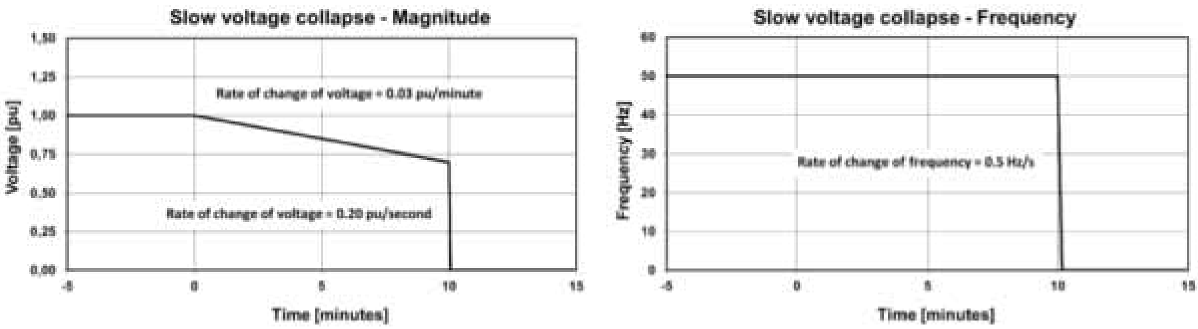


Figure 11 Long-term voltage instability, magnitude (left) and frequency (right)

4. Conclusions and future work

The proposed standard procedure for grid interaction analysis has been applied and refined in connection with analysis of the propagation of transients caused by symmetrical and unsymmetrical faults, from the external power system into the AC auxiliary power systems in three nuclear power plants in Sweden. Experience shows that analysis of steady-state performance is not sufficient. It is also necessary to verify withstand capability of the auxiliary systems for unbalanced faults. It is concluded that it is necessary to calculate the instantaneous values of currents and voltages. Based on the standard procedure presented in this paper a number of actions to improve the plant robustness, such as revised settings of voltage protection, introduction of complementary undervoltage protection, and more robust design of the auxiliary transformers, have been taken within OKG.

The present paper and work carried out so far have been focused on primary shunt faults and abnormal symmetrical conditions in the connecting grid, which need attention in order to decide if the connecting grid is to be regarded as healthy and fully reliable or if transfer to emergency diesel systems should take place. We have also learned that phase interruptions (one or two phases) on all voltage levels in the supply chain of the auxiliary systems cause operational situations hard to detect but hazardous for continued grid supplied operation. Such unsymmetrical phase interruptions are suitable for future work; identify the safe operational boarders, and methods to detect situations when the borders are violated.

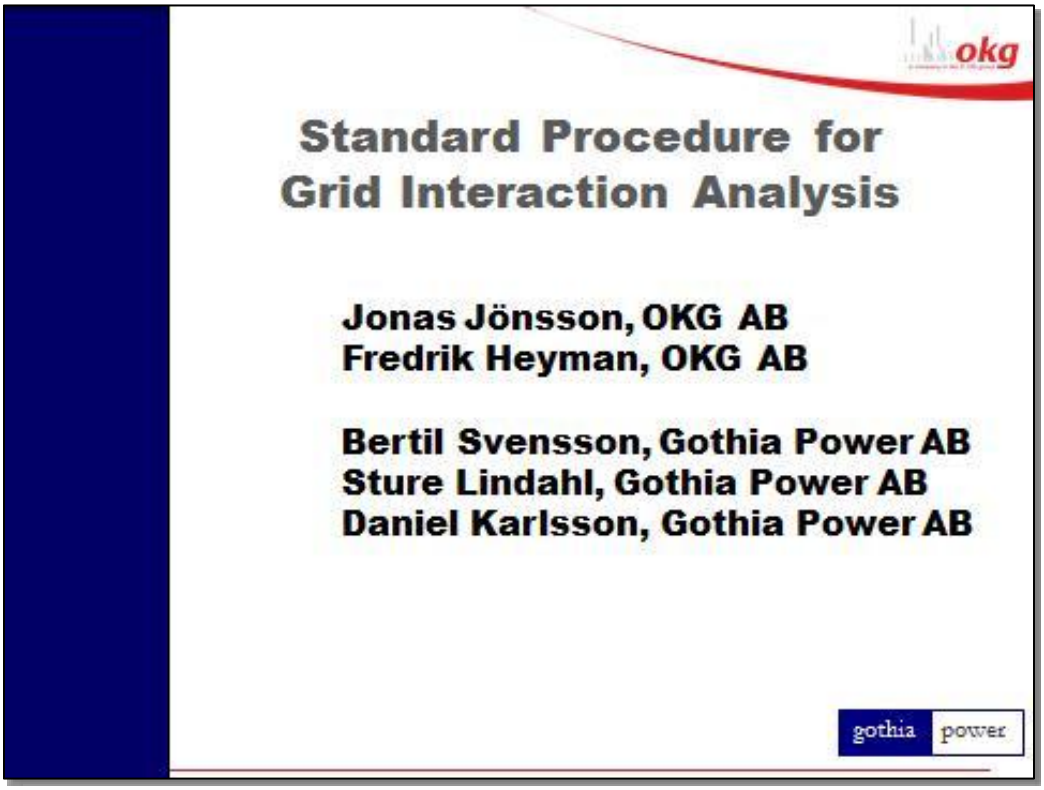
So far focus has been very much on dependability, i.e. make sure to trip for every critical situation, and not so much on security, i.e. make sure not to trip when trip is not wanted. The security issue is more related to operation and economy but unselective protection operations have caused generator tripping and dynamic instability. The dependability is more related to safety and especially the risk to subject all parts of the auxiliary system to severe voltage dips. Therefore protection schemes to increase the security, which have been focused for the transmission systems lately, will need more attention in the future for generation plants. A first attempt has been made at OKG unit 2, where a dual two out of two protection design has been implemented [2].

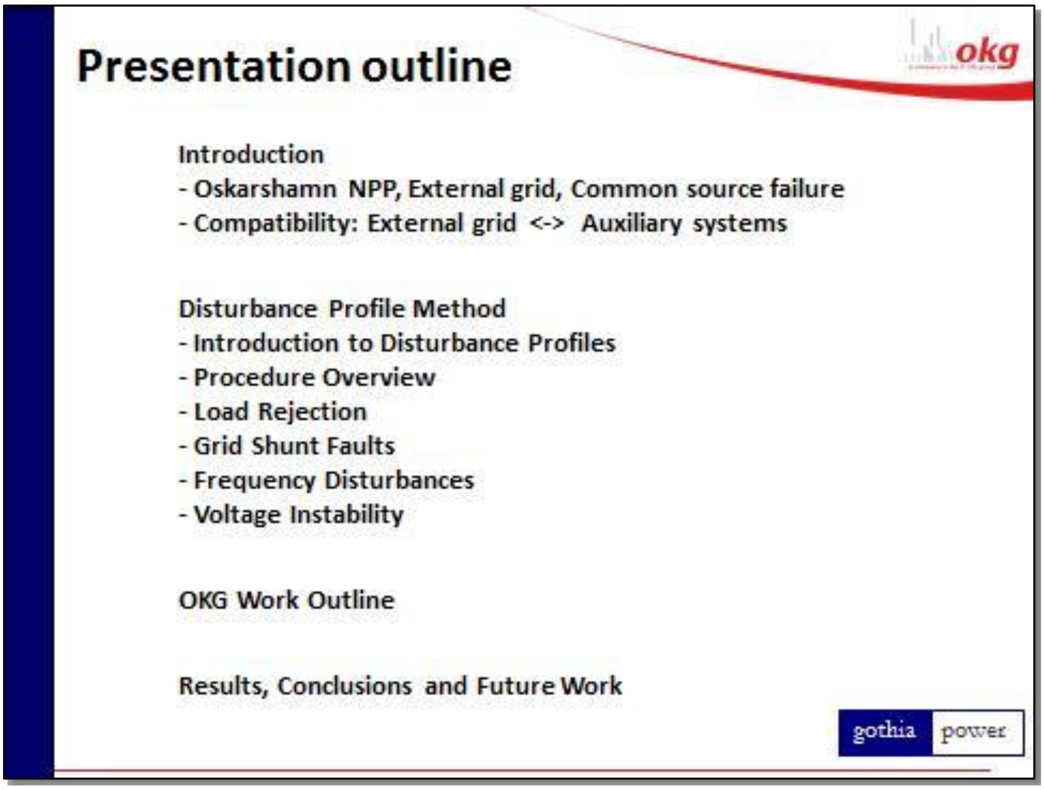
Today's protection design comprises a high level of redundancy. However, design that makes the circuit-breaker redundant is still not common. More research on design principles, costs and benefits, as well as on performance and power system design and requirements, is needed.

References

[1] Sparre, E.; "PSA-modeling of External Grid Failures Occurring Close to Nuclear Power Plants", PSAM 11/ ESREL 2012, Helsinki, Finland, June 25-29, 2012.

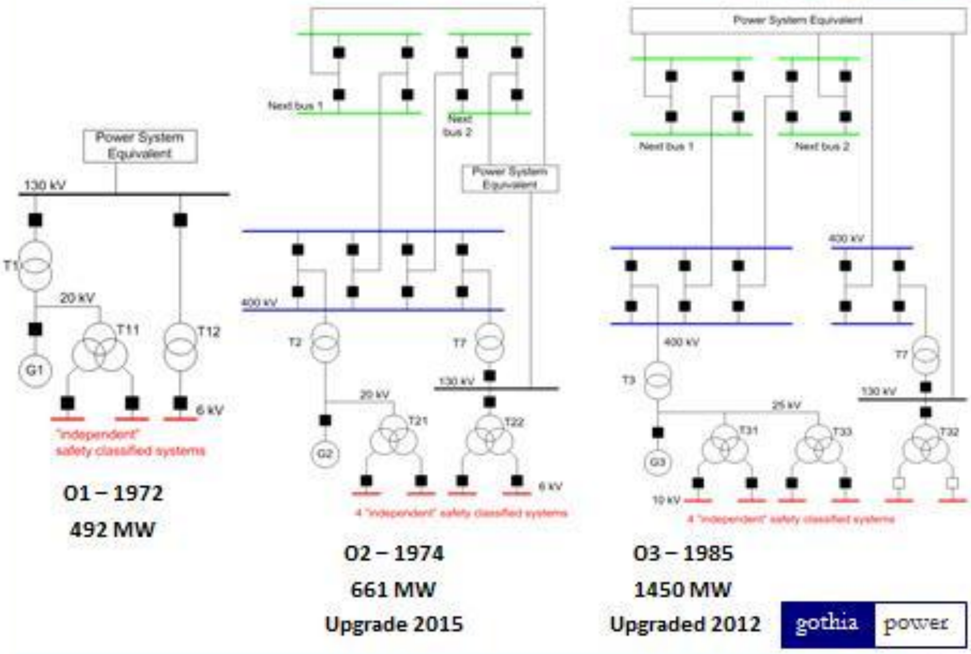
[2] Messing, L.; Lindahl, S.; Svensson, B.; "Protection system design for assurance of dependability and security", http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/c1256d32004634bac1256e19006fccc3/$file/paper_2000_06_en_protection_system_design_for_assurance_of_dependability_and_security.pdf


okg
Standard Procedure for Grid Interaction Analysis
Jonas Jönsson, OKG AB
Fredrik Heyman, OKG AB
Bertil Svensson, Gothia Power AB
Sture Lindahl, Gothia Power AB
Daniel Karlsson, Gothia Power AB
gothia power


Presentation outline
okg
Introduction
- Oskarshamn NPP, External grid, Common source failure
- Compatibility: External grid <-> Auxiliary systems
Disturbance Profile Method
- Introduction to Disturbance Profiles
- Procedure Overview
- Load Rejection
- Grid Shunt Faults
- Frequency Disturbances
- Voltage Instability
OKG Work Outline
Results, Conclusions and Future Work
gothia power

Oskarshamn NPP, Sweden

okg



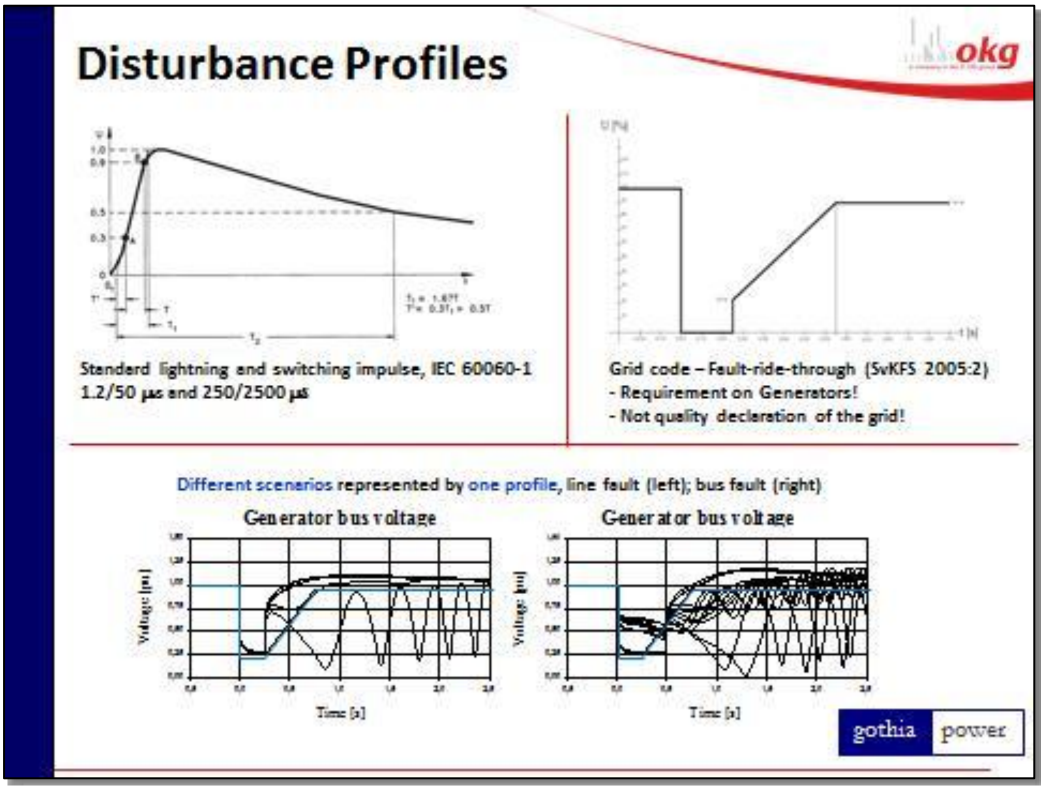
gothia power

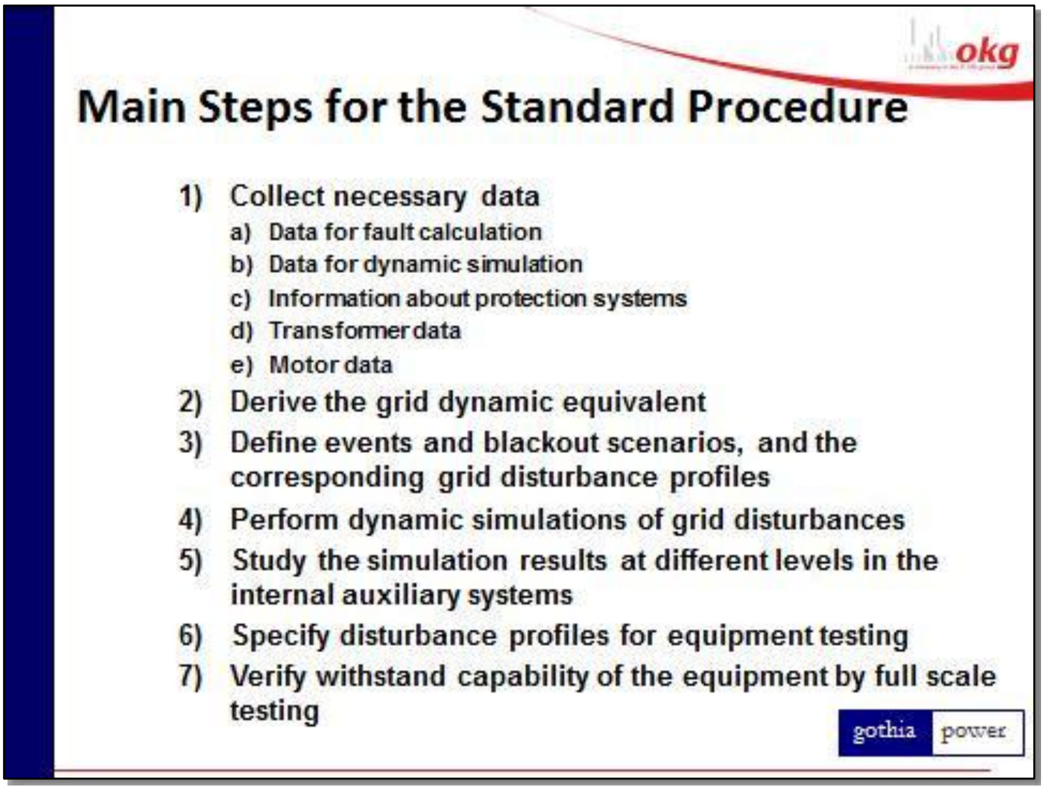
External Grid – Common Source

okg

- The Fukushima Daiichi accident, very clearly pointed out the importance of common cause failures in the planning and operation of auxiliary and safety systems of nuclear power plants.
- The connecting grid, during normal operational conditions, is such a common factor for many important auxiliary systems.
- The analysis within the nuclear power industry has for long been focused on the two very distinct conditions, the connecting grid available or the connecting grid not available.
- However, very little focus has been put on how to distinguish a fully reliable and healthy connecting grid from a situation where the power plant auxiliary systems have to be disconnected from the grid.
- The disconnection criteria must be based on the compatibility between the grid and the auxiliary equipment.

gothia power


Disturbance Profiles
okg
Standard lightning and switching impulse, IEC 60060-1
1.2/50 µs and 250/2500 µs
Grid code – Fault-ride-through (SvKFS 2005:2)
- Requirement on Generators!
- Not quality declaration of the grid!
Different scenarios represented by one profile, line fault (left); bus fault (right)
Generator bus voltage
Generator bus voltage
Voltage [pu]
Time [s]
gothia power


Main Steps for the Standard Procedure
okg
1) Collect necessary data
a) Data for fault calculation
b) Data for dynamic simulation
c) Information about protection systems
d) Transformer data
e) Motor data
2) Derive the grid dynamic equivalent
3) Define events and blackout scenarios, and the corresponding grid disturbance profiles
4) Perform dynamic simulations of grid disturbances
5) Study the simulation results at different levels in the internal auxiliary systems
6) Specify disturbance profiles for equipment testing
7) Verify withstand capability of the equipment by full scale testing
gothia power

Study Grid Disturbance Events

Study the connecting grid, and evaluate possible scenarios. The following events, affecting the conditions on the generator bus or in the grid connection point of the NPP, and thereby the auxiliary and safety system supplies, should be regarded:

- Load rejection, i.e. disconnection of the unit and its auxiliary systems from the grid.
- Primary shunt disturbance faults, such as short circuits and earth-faults,
  - cleared by the ordinary protection system
  - cleared by the backup protection system
- Abnormal system frequency in the connection point,
  - due to loss of generation – dynamic / static
  - due to loss of load – dynamic / static
- Abnormal operational voltage in the connection point,
  - high voltage due to external conditions
  - low voltage due to external conditions

gothia power

Derive the Grid Disturbance Profiles

Group the grid disturbance events studied,

with respect to the resulting voltage stress, i.e.
- magnitude and frequency level, as well as
- structure, and duration,
on the auxiliary and safety systems,

into a limited number of groups

Assign a synthetic, well defined, disturbance profile
- voltage magnitude/frequency -
for each group

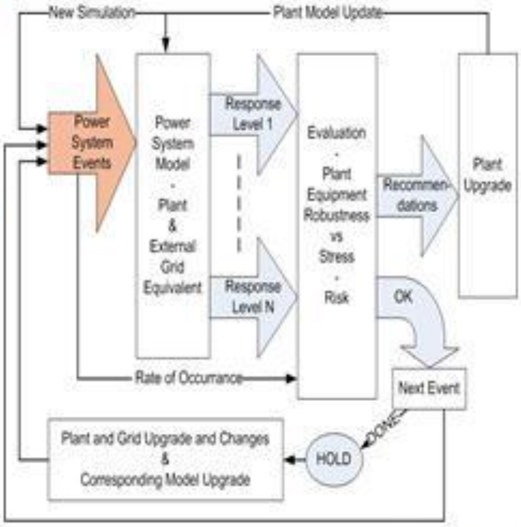
gothia power

Verify Equipment Compatibility

Study the impact on the auxiliary and safety systems, when the grid disturbance profiles are applied.

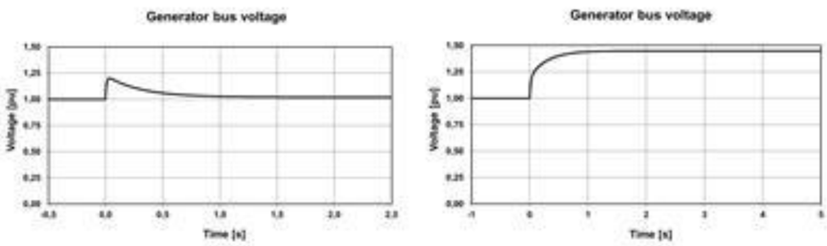
Derive the corresponding event rate of occurrence for each of the grid disturbance profile impacts.

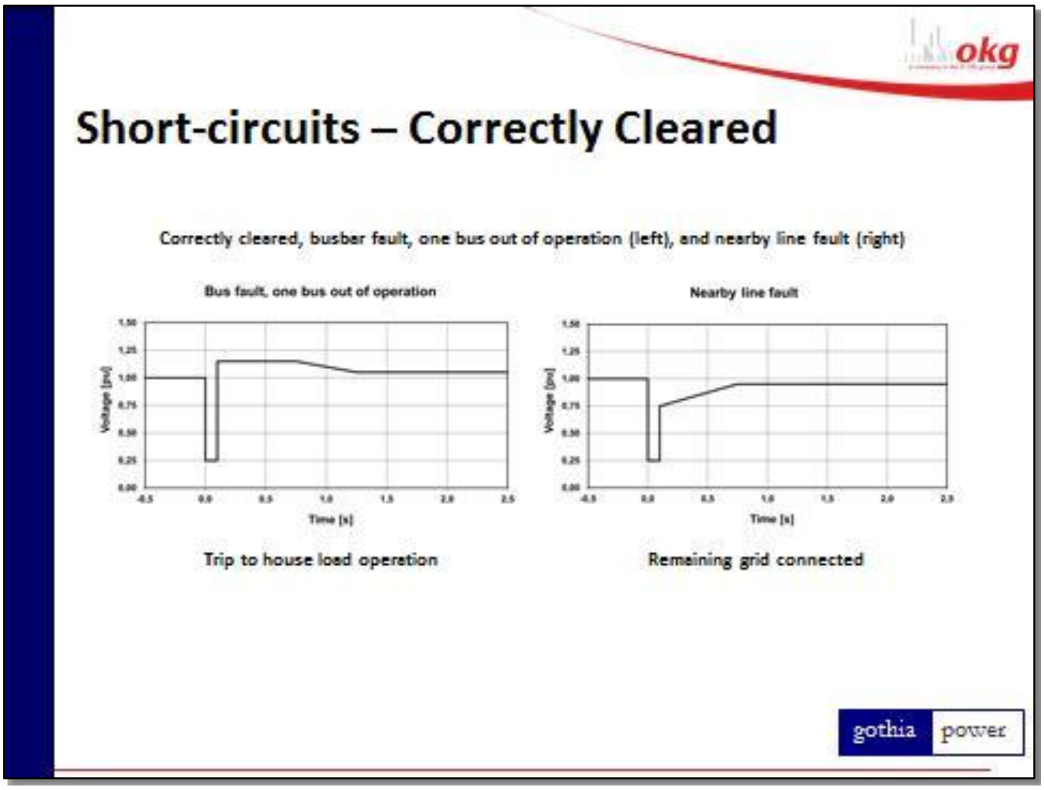
For all credible disturbances, according to the event rate of occurrence, it has to be ensured that the equipment can either withstand the stress caused by the disturbance profile, or that the unit will be disconnected from the grid.

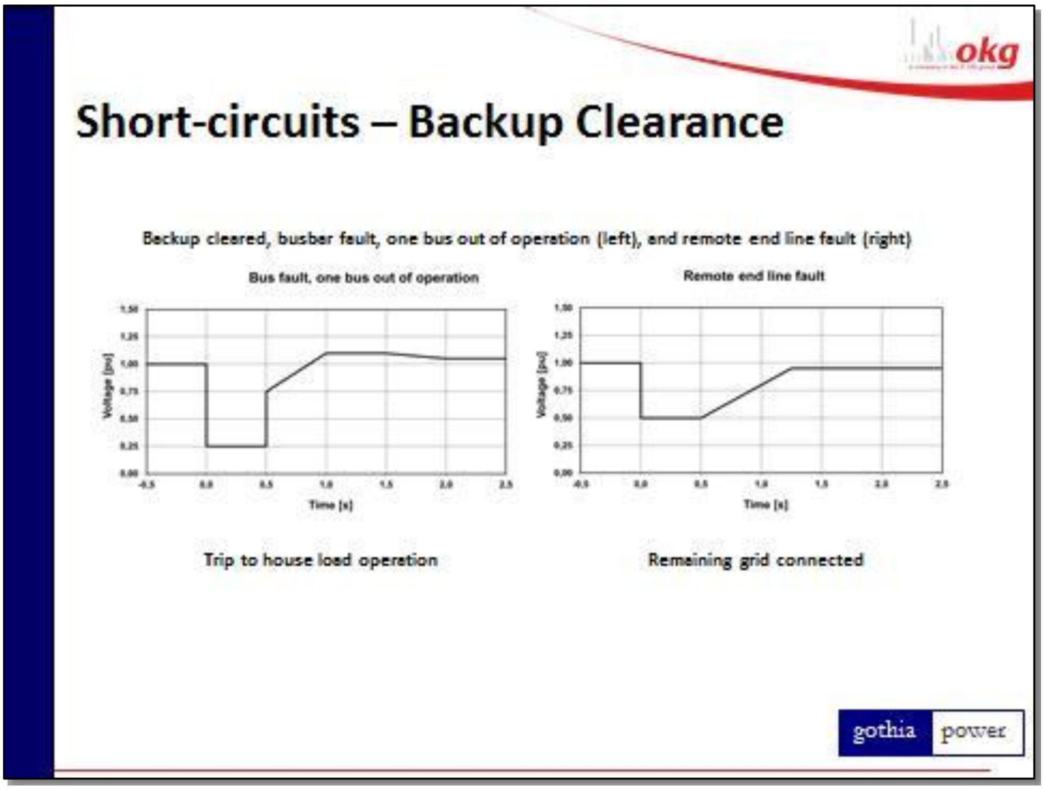


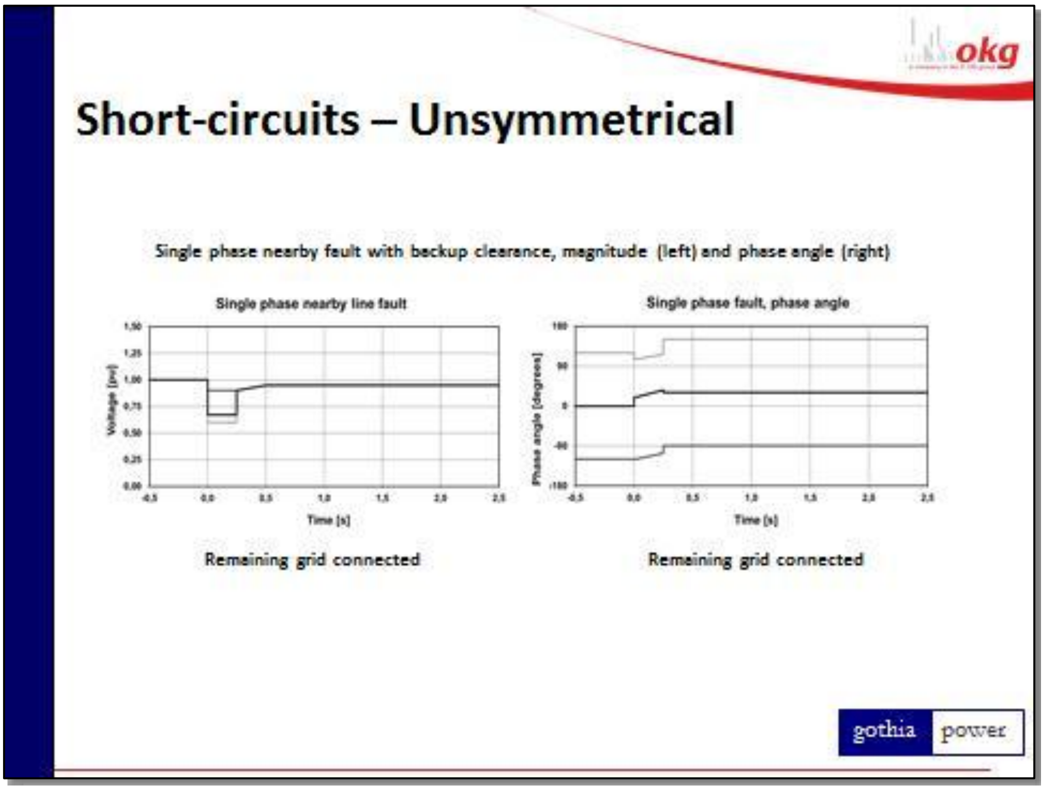
Disturbance Profiles – Load Rejection

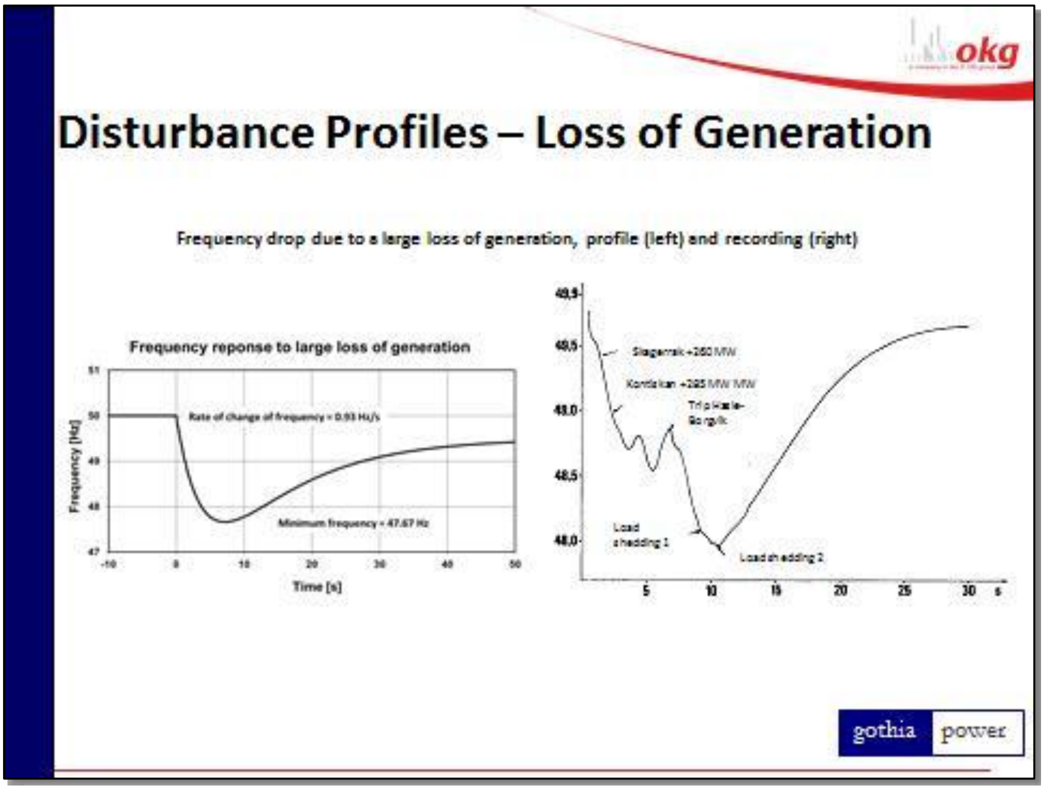
Generator bus voltage at load rejection with AVR (left) and in field current control mode (right)



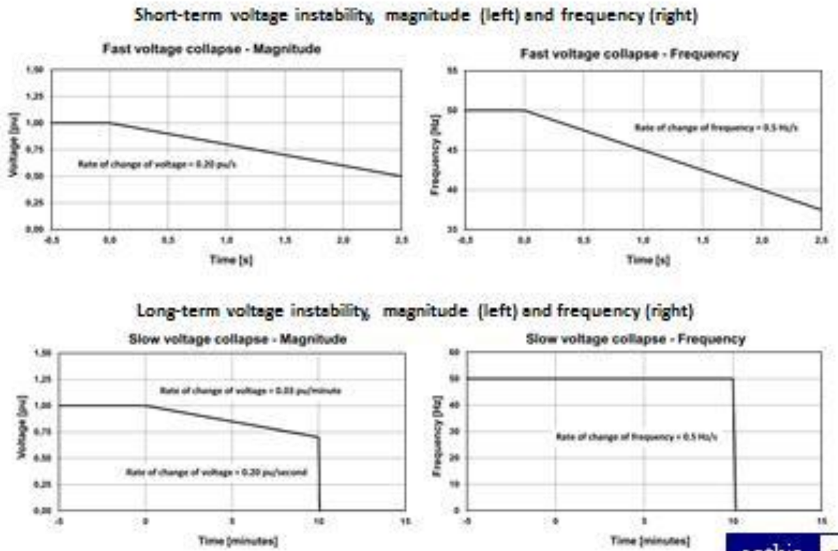

okg
Short-circuits – Correctly Cleared
Correctly cleared, busbar fault, one bus out of operation (left), and nearby line fault (right)
Bus fault, one bus out of operation
Nearby line fault
Voltage [pu]
Time [s]
Trip to house load operation
Remaining grid connected
gothia power


okg
Short-circuits – Backup Clearance
Backup cleared, busbar fault, one bus out of operation (left), and remote end line fault (right)
Bus fault, one bus out of operation
Remote end line fault
Voltage [pu]
Time [s]
Trip to house load operation
Remaining grid connected
gothia power


Short-circuits – Unsymmetrical
Single phase nearby fault with backup clearance, magnitude (left) and phase angle (right)
Single phase nearby line fault
Voltage [pu]
Time [s]
Single phase fault, phase angle
Phase angle [degrees]
Time [s]
Remaining grid connected
Remaining grid connected
gothia power

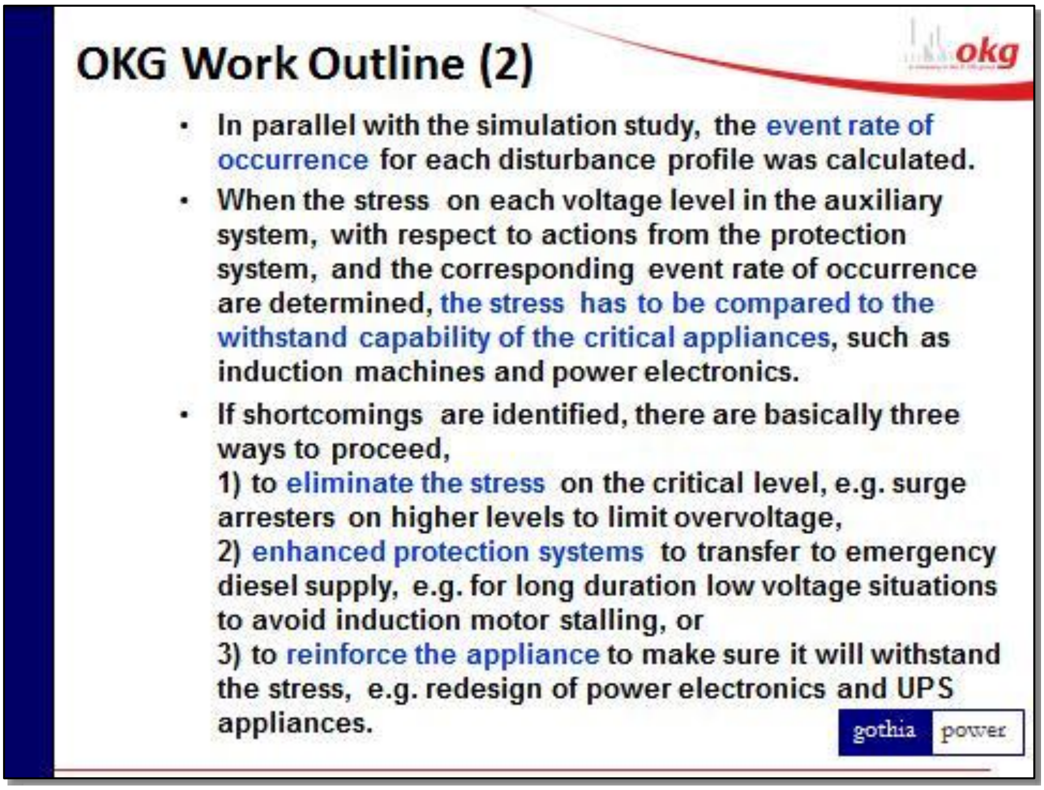

Disturbance Profiles – Loss of Generation
Frequency drop due to a large loss of generation, profile (left) and recording (right)
Frequency reponse to large loss of generation
Frequency [Hz]
Time [s]
Load
shedding 1
Load shedding 2
gothia power

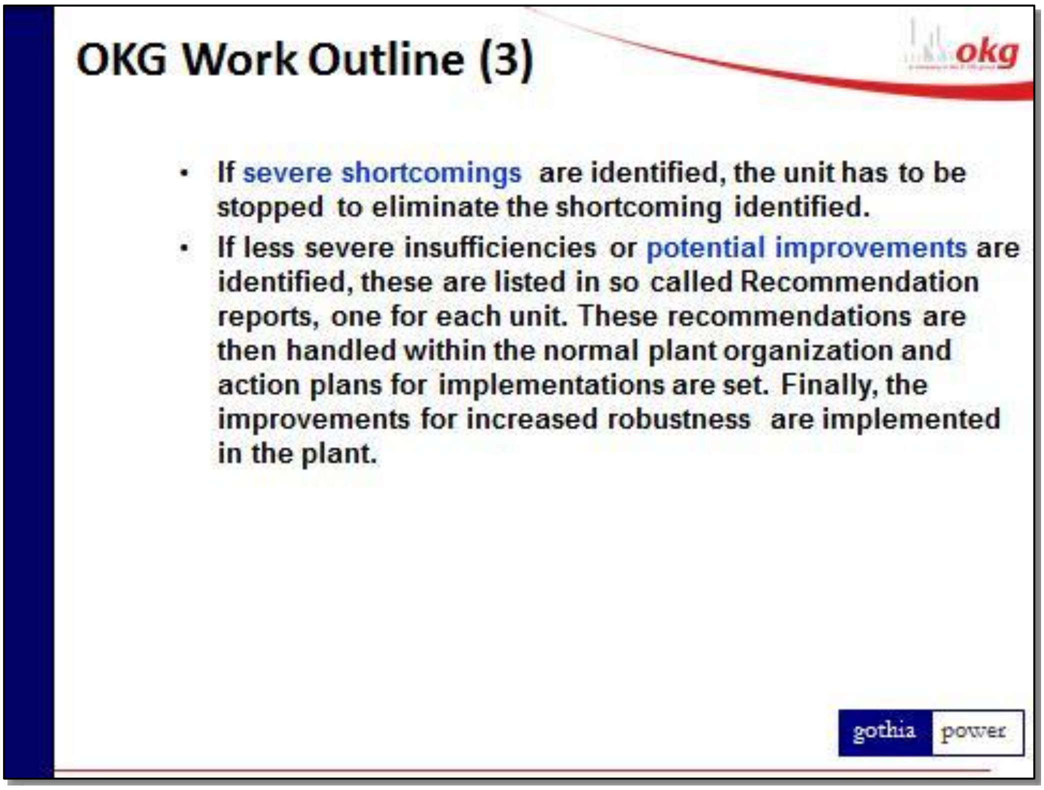
Disturbance Profiles – Voltage Instability



OKG Work Outline (1)

- Firstly the disturbance profiles were defined and characterized.
  - For the OKG units 13 profiles were identified
- Then a simulation study was initiated to investigate how the applied disturbance profiles propagate into the auxiliary systems.
  - A large part of this study is to compare each disturbance profile propagation and the resulting stress at different levels and points in the auxiliary system with the protection relay characteristics and settings, to really see the full impact of the disturbance profile under study.
- For the simulation study, a transient analysis program like PSCAD/EMTDC has to be used


OKG Work Outline (2)
okg
• In parallel with the simulation study, the event rate of occurrence for each disturbance profile was calculated.
• When the stress on each voltage level in the auxiliary system, with respect to actions from the protection system, and the corresponding event rate of occurrence are determined, the stress has to be compared to the withstand capability of the critical appliances, such as induction machines and power electronics.
• If shortcomings are identified, there are basically three ways to proceed,
1) to eliminate the stress on the critical level, e.g. surge arresters on higher levels to limit overvoltage,
2) enhanced protection systems to transfer to emergency diesel supply, e.g. for long duration low voltage situations to avoid induction motor stalling, or
3) to reinforce the appliance to make sure it will withstand the stress, e.g. redesign of power electronics and UPS appliances.
gothia power


OKG Work Outline (3)
okg
• If severe shortcomings are identified, the unit has to be stopped to eliminate the shortcoming identified.
• If less severe insufficiencies or potential improvements are identified, these are listed in so called Recommendation reports, one for each unit. These recommendations are then handled within the normal plant organization and action plans for implementations are set. Finally, the improvements for increased robustness are implemented in the plant.
gothia power

Results

- **13 disturbance profiles have been derived for Oskarshamn NPP**
- **Present plant auxiliary systems have been checked with respect to these disturbance profiles**
  - One severe shortcoming was once identified – and O3 was immediately stopped
  - Robustness improvements have been identified and implemented, such as
    - Complementary under-voltage protection
    - Revised protection settings
    - Complementary surge arrestors on the 10 kV level
    - Revised transformer design
  - Adequate robustness levels have been verified
- **New auxiliary system equipment is regularly exposed to full scale tests with respect to the disturbance profiles**

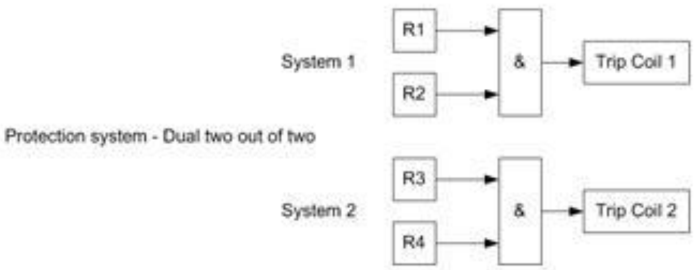
gothia power

Conclusions

Based on the standard procedure presented in this paper a number of actions to improve the plant robustness, such as

- more robust design of the auxiliary transformers,
- revised settings of voltage protection,
- introduction of complementary undervoltage protection, and
- more robust design of protection systems – “dual two out of two”,

have been taken within OKG.



gothia power

Future Work (1)

- Work carried out so far have been focused on primary shunt faults and abnormal symmetrical conditions in the connecting grid.
  - We have also learned that phase interruptions (one or two phases) on any voltage level in the supply of the auxiliary systems might cause operational situations hard to detect but hazardous for continued grid supplied operation.
  - Future work: Identify the safe operational borders, with respect to phase interruptions, and methods to detect situations when the borders are violated.
- So far focus has been very much on dependability, i.e. make sure to trip for every critical situation, and not so much on security, i.e. make sure not to trip when trip is not wanted.
  - The security issue is more related to operation and economy but unselective protection operations have caused generator tripping and dynamic instability.
  - Future work: Protection schemes to increase the security.

gothia power

Future Work (2)

- Today's protection design comprises a high level of redundancy.
  - However, design that makes the circuit-breaker redundant is still not common.
  - Future work: Research and development on design principles, costs and benefits, as well as on performance and power system design and requirements, that makes the circuit-breaker redundant.

gothia power


okg
Thank you for your attention
- Comments?
- Questions?
gothia power

Electrical Dynamic Simulation Activities in Forsmark NPP

Per Lamell
Forsmarks Kraftgrupp AB, Sweden

Abstract

The original power system analysis was done in the seventies in former ASEA AB software. For approximate twenty years no major new studies was done because of limited numbers of renewal projects. In the end of the nineties the plant started to update the selectivity planning and study of the loading of the safety busbars. The simulation and start of the development of simulation models was done in a tool named Simpow. Simpow was also an ASEA/ABB AB software developed from the program used in the seventies. To continue to work with Simpow was a decision made after doing an extensive review of on the marked available commercially software. Also at that time we start to do our first attempt building electrical simulation models of unit 1 and 2 according to the original documentation.

The development of models for the unit 1, 2 and 3 became more intensive some years after the millennium. Partly because of event July 25, 2006 and also because of the renewal of unit 1 and 2 and had subsequently been initiated for unit 3 also. Today we have initiated a conversion of our models to a new program called PowerFactory. That due to the withdrawal of support and development on SIMPOW a couple of years ago. To development relevance, accuracy and detail, models are an important issue for FKA (Forsmark Kraftgrupp AB). The model is initially created according to the plant documentation and also including requested information from the original supplier. Continued development and updates of the model is done according to the data received from the contractors via the demands according to requirements in our technical documents on different electrical components in renewal projects. The development of the model is driven by known weaknesses, depending of the type of studies and necessary data related to events.

An important part that will be described is to have a verified simulation tool and validated models. An example is that the models have been validated by making start and loading test of the safety busbars at the units and compared with the results of the simulations.

Forsmark has made studies with the developed models to support renewal projects to present the behaviour of the plant of proposed logic and to determine the specification and requirement on contracting function and also on including components. Power system simulation have also been used to analyse the different incidents that have challenged the electrical systems on the three different units, with dependence on the different initiators and causes of the disturbances to find similar weak points that can cause failure in the plants. The simulation tool is also used to study plants compliance with the authority requirements. Now after the latest event at May 30, 2013, Forsmark is working to develop a new strategy on throw to approach these studies in a more general, unconditional way. The input are review of the description how plants originally design. Review of the units relay protection design to bring out any weaknesses or inaccuracy, and compare with other plant relay protection design and study the possibilities with extended functionality of modern protection compared with the relay protection of the seventies. To find out if it is any differences in the level in the voltage, current or frequency level and duration between the result of simulation and the implemented protection scheme. Renewed evaluation of electrical related disturbance from existing experience feedback handling. Especially focusing on avoiding jeopardizes the safety function, defence in-depth regarding electrical disturbances and also on availability.

1. Events

During the last years Forsmark NPP has suffered from electrical related incidents, such as:

Forsmark 1, 25 July 2006) Loss of external power and loss of power supply from 2 of 4 diesel generators Forsmark 1, 25-07-2006 (Event Analysis Report, WANO Paris Centre, 2006-0027 revision number 01)

On July 25th, a two-phase short circuit occurred during ongoing operations in the 400 kV switchyard. The opening of a section disconnector under full load caused an arc and a short circuit. The unit circuit-breakers disconnected the plant generators, and the plant automatically inserted selected control rods for a partial scram, initiated pump runback and switched over to house load turbine power supply. Shortly after the initial event, the plant was scrammed and the containment was isolated.

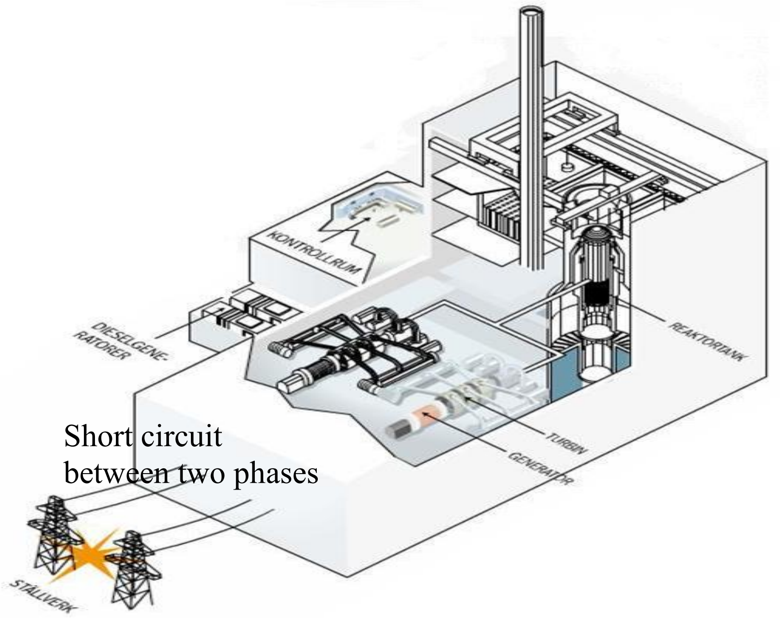


Figure 1. The fault in the switchyard.

Two out of four power supply divisions (A and B) in the internal grid (500 V, diesel backup) were without power for approximately 20 minutes. When the two 500 V diesel busbars were connected manually to the 6 kV system, all four divisions of the internal power supply system regained power, and the plant could go safely to a safe, hot shutdown state.

Shortly after the initial event, before the scram, one turbine tripped due to low hydraulic pressure in the turbine control valve system. The turbine speed fell to 2820 r/min, which should have opened the generator circuit-breaker due to low frequency (47.5 Hz). However, the breaker failed to open. A few moments later, due to further decrease in frequency, the feeder breakers between the main internal bus bars and the diesel supported 500 V bus bars disconnect.

During the electrical transient, two UPS (Uninterruptible Power Supply) units tripped. Equipment supported by the units includes the speed measurement control logics to the diesel engines, which subsequently failed to start. The loss of power resulted in loss of two auxiliary feed water pumps. Water was throughout the event pumped in at 2 x 22.5 kg/s by the two remaining auxiliary feed water pumps. During the transient, the pressure in the reactor vessel was reduced to 6 bar over a period of 30 minutes. The level in the vessel stabilized at +1.9 m over the core after 15 minutes, and was restored to the normal level after another 15 minutes.

As the two UPS-units failed (A and B), two trains of the internal 220 V system also failed. Components supported by the 220 V systems in two out of four divisions failed due to loss of power, as follows:

- Sensors, transmitters, controllers, trend and event recorders
- Indicators and supervisory facilities in the control room
- Fine motion control rod drives (all the rods were inserted by the hydraulic scram system)
- Half of the control rod drive indication was lost, i.e. therefore not providing indication of control rods fully inserted in the core
- Four out of eight reactor main circulation pump motors tripped
- Four out of eight reactor low power measuring (WRNM, Wide Range Neutron Monitors) units lost power
- The power station's internal public address and warning systems failed due to loss of power.

Lightning strike tripped all eight main circulation pumps at Forsmark 2.(Forsmark 2; 13 June 2008) Forsmark 2, 13-06-2008 (Miscellaneous Event Report, WANO Paris Centre, 2008-0128 revision number 00)

A thunderstorm over central Sweden caused a lightning strike to the main grid about 50 km from Forsmark NPP, causing a three-phase short circuit and a voltage dip to about 50 % for about 90 milliseconds. The short circuit activated the rectifiers protection relays due to that the phase angel deviated from 120 degrees with 8 degrees in more than 80 milliseconds and the rectifier tripped. When the rectifiers tripped the rotating energy stores continued to produce energy resulted in that two of the rotating energy stores to trip on undervoltage and the other two to trip on overcurrent.

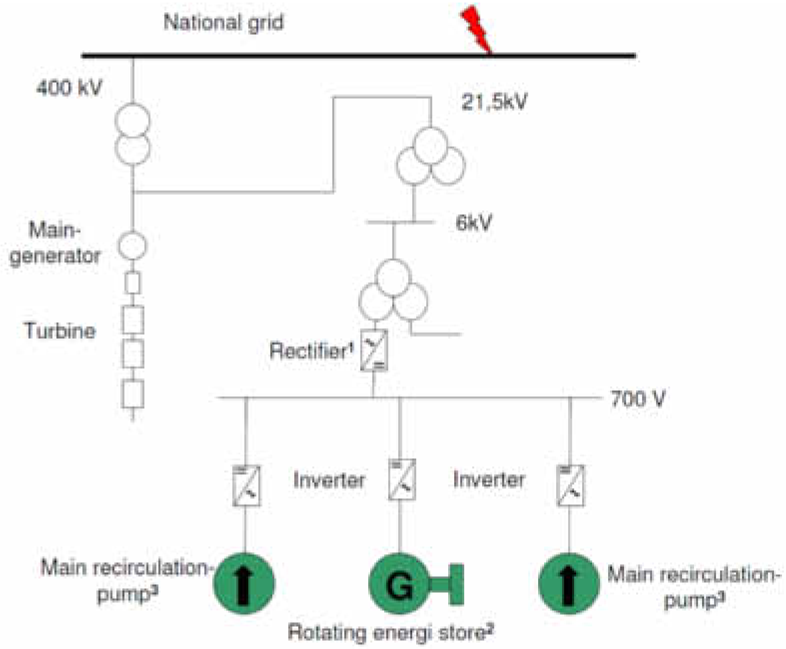


Figure 2. The lightning strike affects the frequency converter for the main recirculation pumps

This caused the main recirculation pumps to stop and run down to stop faster than anticipated in the safety analyses. With the main recirculation pumps stopped the reactor power fell to 39 % after the initial event, and the reactor power then had an increasing oscillation with amplitude of up to 10 % before a manual scram was initiated. There is no automatic main recirculation pump run down signal or an automatic scram from the reactor protection system if the rectifiers trip. With all main recirculation pumps stopped, there was a risk of thermal stratification in the RPV, and thus of uneven temperature distribution.

After assessment of the transient risks, it was decided to restart two of the main recirculation pumps. The maximum temperature difference was 18°C. The six other main recirculation pumps were restarted after the temperature in the RPV had been evened out. It was decided to shut down the reactor to the cold shut down state.

Forsmark 3 July 13, 2012 Lightning strike causing voltage transient in station AC net Forsmark 3, 13-07-2012 (WANO Event Report, WANO Paris Centre, 2012-0217 revision number 00)

During the Forsmark 3 refueling outage, operating mode cold shutdown reactor, with work underway in trains B/D (Forsmark 3 has four redundant safety trains A, B, C and D) 400 kV power supply is isolated for scheduled work and electricity is supplied from the external grid from the 70 kV mains. A lightning strike occurs in the 70 kV mains near the startup transformer.

At normal operation the station is connected to

the 400 kV off-site grid which is protected by both surge arrester and earth/shield wire at the lattice tower of the overhead line to mitigate consequences of lightning strikes. The cable and overhead line connection for unit 3 to the 70 kV switchyard and network includes several surge arresters, but the overhead line has not any earth/shield wire.

In the time of the event it is a thunder storm in the area and a lightning strike occurs in the 70 kV mains near the startup transformer.

The lightning strike apparently caused a voltage transient to propagate in the station internal net and caused damage to a number of thyristors for the battery-supplied AC net.

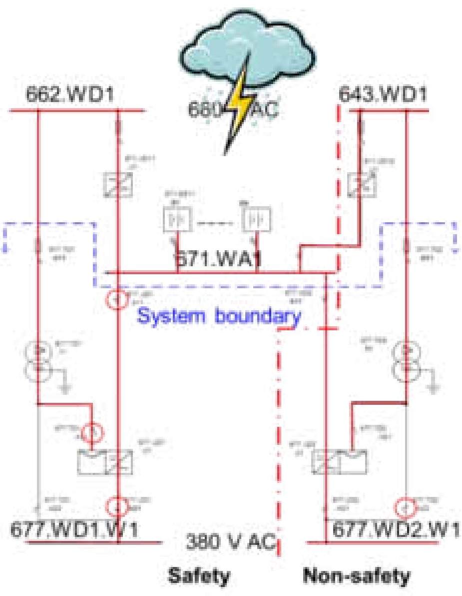


Figure 3.The affected UPS system

The event had in this case no operational consequence as the plant was in refueling mode.

Forsmark 3 May 30, 2013: Loss of two phases of the external grid during outage shutdown with loss of decay heat removal (WANO Event Report, WANO Paris Centre, 2013-0139 revision number 02)

During cold shutdown, established on 2013-05-19, the 70-kV grid was shut down for connection to new switchgear. Work was underway on the 400 kV D bus. A and B trains were ready for operation. The diesels in C and D trains were ready for operation. Relay testing was underway on the excitation system for the generator during which a spurious signal was sent to the unit breaker.

At 10:01 a.m. on May 30 an intermediate position was detected on the unit breaker indication for the E bus, due to one phase not being tripped. It was due to a loose cable in a tripping device for one of the phases. The main transformer configuration (Y/D) to the external grid resulted in discrepancy between the phases inside the plant. The operating plant components equipped with phase discrepancy protection tripped, whereupon decay heat removal was lost.

Phase discrepancy protection is actually a phase failure function in the overload protection for low voltage motors and negative sequence current protection. The diesel buses were separated manually from the external grid and energized by auxiliary diesels. The first train was ready at 10:15 a.m. and all trains were ready at 10:36 a.m. Decay heat removal was restored at 10:17 a.m.

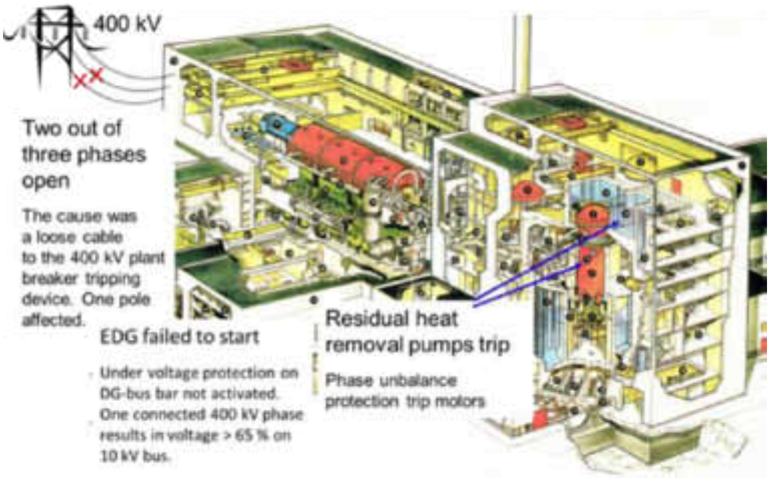


Figure 4. The event and the effect

The fuel was removed from the core and the fuel storage pool gates were open. The plant can go about one day before boiling starts. The temperature increase rate at 34°C was approximate 0.7°C/h. In conjunction with diesel start local resetting of the phase discrepancy protection for the diesel cooling water systems was required. At 10:44 a.m. the supply from the 400 kV E bus was restored. The incident is not analysed in the safety analysis report, which means that the plant is not designed to automatically handle the situation that arose. The INES classification is assessed as (1) as there was an impact on defence in-depth. Basic classification is zero and an additional factor for CCF. The incident did not have any operational consequences.

These events have an incitement to increase the efforts to make models of the plants and the off-site grid and continue to do studies.

2. Requirement

The following fundamental requirements are the base for the interpretation of the analysis of the studies:

- Swedish Radiation Safety Authority's regulation
- Keeping the integrity of the safety system and defence in-depth
- Svenska kraftnät (Swedish national grid) regulation
- Availability of the plant

It affects what studies to be performed and development of the models, and as well as how detailed the models need to be.

3. Original studies

The original simulation for unit 3 included as reference reports to the safety analysis report are as follows:

- Plant condition at grid disturbance:
  According to a special grid voltage profile: which from the beginning include an instant voltage drop on the generator busbar down to a level of 25 % for 0.25 s and then linear increase to 95 % for 0.5 s.
- Short circuit on each AC-busbar
  Feeding from auxiliary transformer and start-up transformer and an initial nominal voltage to find the maximum short-circuit currents.
- Start-up of the largest electrical machine:
  The purpose is to verify the start of the largest engine at the worst allowable ratio (0.9 p.u. voltage and at a specified short circuit power), while not interfering other motor drives with protection tripping, etc.
- Start-up sequence of the safety and non-safety busbar.

Similar studies have been done for the unit 1 and 2. These original studies have used a simulation tool from ASEA called MOSTA.

The original studies are few and can be seen as basic studies how the plant will be behave at design cases as disturbance in the off-site grid, internal short circuits and start-up sequences. In this case faults in off-site grid have been simplified to only apply to be executed as one case.

4. Activity plan

Each year is an activity plan updated to describe the planned power system simulation and analysis activities for the next three years. The activity plan presents the work done during the past year, as well as ongoing and planned activities in the areas of structuring working procedure, modelling and studies.

Because of the recent years events increased focus has been on planning a base activity which unconditionally analyses of the plant behaviour during different electricity-related incidents/disturbances, to ensure that we have models and data to assess all, or as many initial events as possible to make the plants more resilient and better protected. Basis for analysis are developed from original design philosophy to find out if some knowledge has disappeared or if it was not possible to include the functionality because of limitation in the existing technology imprinted weaknesses in the functionality or design of the systems. Also included as sources of experience and knowledge is a review of events in other plants and participations in conferences and meetings. If the result reveals weaknesses in the protection configuration, it must be evaluated if there is a need to introduce new protection equipment or if there is a need to modify existing. It is important to evaluate any changes in the protection scheme to keep selectivity.

Attempted simulations will focus primarily on studying applied events impact on safety systems, specifically on the objects connected to, and disconnection of, the safety busbar, also including defence in-depth for the non-safety system/busbar and how it is affected.

FKA have an existing tool to performing studies of electrical faults in both the internal power system in the units and off-site gridFaults caused by thunderstorms that have been assumed to have affected F3 at the event July 13, 2012 requires completely different models and tools to be studied. To study how external lightning spreading in the plant is something that will not be regularly used. This is the reason to try to develop a generic model useful for all plants and in cooperation with the other plants in Sweden.

After each study is performed, it will be evaluated if, or how, the result will affect the safety reports, either included directly or referenced via separate reports

5. Development of simulation models

When the units began modernisation in the late nineties it was as a beginning to building own competence in the area of power system simulation and analysis. Initial work was to carry out a scan of the market of different power system simulation and analysis software available. ABB's simulation tool Simpow was chosen due to proximity of support. An important factor was to have a program with the property to perform both power frequency modelling, which saves computer time, and instantaneous modelling, which gives results with more detailed time resolution. It is of importance to be able to interrupt and freeze the simulation at any time and change between the two model parameters. Also the possibility to do user defined modelling to get additional flexibility not available in the corresponding standard model. A Master Thesis was also performed which included collection of model data from existing documentation and from the original suppliers of primarily electrical machines and cables. The project also included a comparative study of the established model with a previously performed study.

The modelling of the units restarted after some years. In the meantime FKA started using contractors to performing diesel start sequence studies for the units F1 and F3 to verify the fulfilment of the loading requirement according to RG 1.9. Also some work was done to study the internal selectivity planning.

In 2005 the number of people in Forsmark working with these issues increased and working with plant modelling, was intensified with the help of the software developer. The goal was to develop a more detailed model of the Forsmark 1 unit, which later was converted to be a Forsmark 2 model. There are just some few differences between these two units. The year after FKA bought the the Oskarshamn 3 model, which is a similar unit as Forsmark 3. Oskarshamn 3 model were reviewed and converted to be a Forsmark 3 model. The models have been developed from existing documentation. When it has been a lack of model data the original suppliers, at the time of when the units was build, has been contacted to try to receive further information. The models have later been compared to the document load compilation. A document was developed by, and kept updated in connection with, the renewal projects by the system design group.

The ownership of the used software has changed and since two-three years it is not any support and development of the tool. FKA has been forced to transfer and develop models in a new tool called PowerFactory from DIgSILENT. In the market there are a variety of codes and suppliers to choose between and the choice of the code has been made strategically, especially for us in Forsmark which are few working in this area, based on a number of aspects as: competence, development, support, perseverance at the supplier, the capacity of code, number of users (total and locally), the ability to make own models, possibility to do make and change between RMS and instantaneous calculations etc.

The models have been validated by making start-up and loading test of the safety busbars at the units and compared with the results of the simulations. Further validation of the models has been done to the event of 13 June 2008 and also to the case of start-up of larger motor the feed water pump.

6. Model data

Initially developed models based on information in existing documentation. Further development of the models made by help from the original supplier. For some object e.g. electrical machines for the unit 1 and 2 similar motor size from unit 3 has been used when it has not been possible to find any original design documentation.

The work with the modelling of each unit has included very much effort to development of document including modelling and dynamic analyses requirement as:

- Modelling and Dynamic Analyses - Mandatory Information for Electrical Motor
- Modelling and Dynamic Analyses - Mandatory Information for Power Transformer
- Modelling and Dynamic Analyses - Mandatory Information for Cable
- Modelling and Dynamic Analyses - Mandatory Information for Motor Load

For some equipment that is seldom renewed as the main generators and related excitation equipment has some special requirement documents been developed. The document has been successively updated dependent on new knowledge. The requirement has also in some cases also included some extraordinary testing to get the extended data or to verify the theoretically determined model data.

The off-site grid is divided into three different parts as follows:

- Main 400 kV grid which is a physical correct model up to 3-4 switchyards away from the units. The remaining power grid is modelled as various equivalents for different parts of Sweden grid and its Nordic countries.
- The 220 kV grid is a quasi-physical model.
- The units stand-by 70 kV grid uses the TSO model as a base and includes more extended model data of the included hydro power plant and the most important the closed located gas-turbine station.

In recent years an intensive work is in progress to get into a continuously operating process to include the requirement of component data as a requirement in the contract with our suppliers to continuously update the models of the units. A major difficulty is to get a good understanding of the reason to why it is importance to develop electrical dynamic simulation models with sufficient good models to give simulation results.

A lot of effort has also been done to document the models, which is divided into different parts; one for each unit and the one for the 400 kV, 220 kV and 70 kV grid.

7. Studies

Around the millennium the focus on the studies was to verify the capacity of the diesel-generator set for the safety busbar according to RG 1.9. It has continued been an important study to make and to develop the accuracy of the modelled object in diesel supplied safety busbar, including the speed and voltage regulator of the diesel-generator set.

Network disturbances occur occasionally and are of various kinds. The nuclear power plants are designed to cope with a majority of the disturbances with which occurs with different frequencies. Further in the report some of the studies that have been made at Forsmark will be described.

After the event of 25 July 2006 a major study of disturbances in the off-site grid that can affect two or multiple trains of the internal power system was started. The incident shows that failure other than the three-phase short-circuit may affect internal power system in a negative way. The study included calculation of voltage profile in the generator busbar and internal grid e.g. the non-safety busbar in Forsmark 1, 2 and 3 at one-, two-and three-phase fault in the off-site grid.

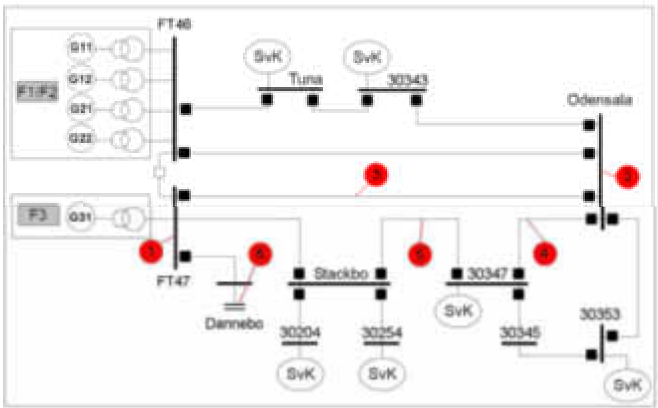


Figure 5. Location of the faults.

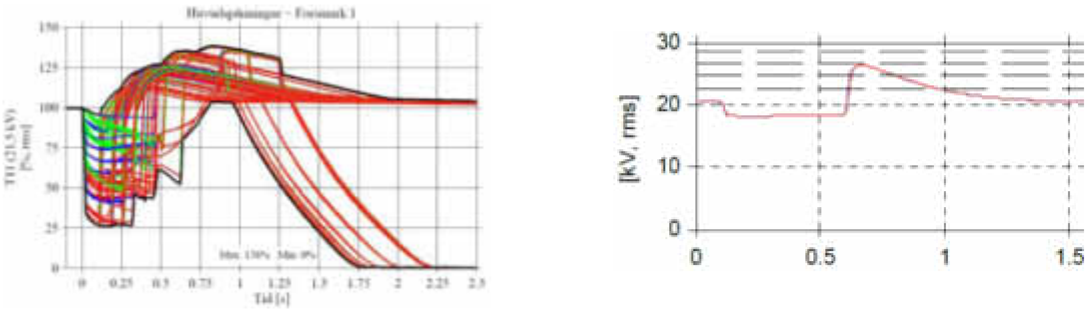


Figure 6. Generator busbar voltage at load rejection unit 1 and the remotely three-phase fault at unit 3.

One other condition that has been studied is behaviour of motors in the units at decreasing network voltage in the cases of generator not connected and generator in-service. The first case with the generator not connected is a worst case scenario and the trip times for thermal motor overload protections in the auxiliary system has been calculated. The simulation was performed with all motors connected to both the safety and non-safety busbar. The used voltage profile had a slope of -0.015 p.u./min and -0.03 p.u./min and different active power operating points. Initially the bus voltage at the safety busbar was 85 % and then it decreased to 65 % of nominal voltage for calculation of minimum delays to thermal trip with decreasing voltage. The value 85 % is because of it is the lowest voltage value according to the TSO regulation and 65 % is the voltage value at which the diesel-generator set set will receive the order to start.

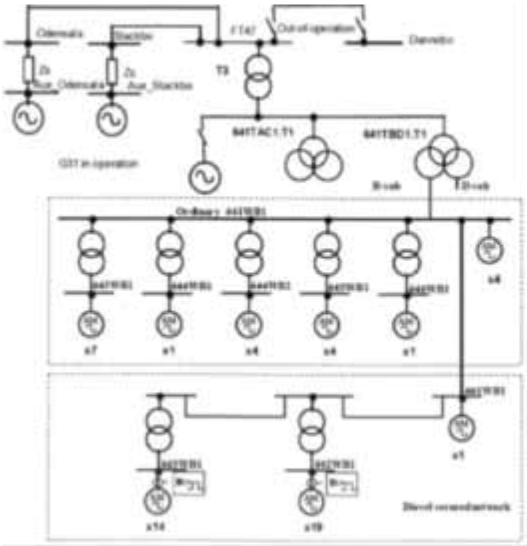


Figure 7. Principal sketch of the network modelled at slow decr. voltage.

The study shows that the shortest delay is 48.9 s for unit 3 which was the basis for the introduction of an under-voltage protection at 85 % and trip time of 10 s.

The second study which is a more realistic case deals with slowly decreasing network voltage in the 400 kV off-site grid with the generator in operation and how this can affect the auxiliary power system with special attention of the motors on the diesel feed safety busbar. Normally, when the main generator is in service, a situation with slowly decreasing network voltage should occur. The voltage on the generator busbar is kept constant up to the level of the stator and/or rotor current limiters. There may be several causes of decreasing network voltage but a high load level in combination with branch elements and production sources out of-service are often involved.

It is very difficult to predict the risk for slowly decreasing network voltage but the risk cannot be disregarded. The result is to reveal if motor thermal overload protection will start and possibly trip or asynchronous motors to stall or if it is a risk for an out-of-step condition.

At the renewal of the new switchyard at the 70 kV second source different type of studies has been done as:

- F1 - Restart of internal auxiliary power system via the 70 kV grid
- F3 - Restart of internal auxiliary power system via the 70 kV grid
- F1/F2/F3 - Restart of three blocks through 70 kV grid
- F1/F2/F3 – SBO (Station Black-Out) and restart of all three units by the 70 kV grid
- Reactive compensation in new 70 kV switchyard based on the needs of the F1, F2 and F3

The purpose of the simulation was to study necessarily short-circuit power in the 70 kV grid to restart the internal auxiliary power system. Also to develop the logic to senses when the grid starts to be weak which for unit 3 is a signal that it is necessary to limit-the non-safety start sequence? The study also include testing of the logic to restart the three unit in sequence, to cope with the transformer inrush current to not affect the relay protection in the gas turbine station connected to the 70 kV switchyard.

Last year the focus has been on open-phase condition studies. According to the event in unit 3 May 30, 2013 has a studied the cases includes that one or two breaker poles still is closed when the signal to the breaker has to trip (open all three phases). The studies that have been performed for unit 3 and similar cases have been studied for unit 1.

- Single pole failure (still closed) at 400 kV unit breaker during outage
- Single pole failure just before synchronize of the generator breaker after outage
- Single pole failure at 400 kV unit breaker at low active power from the generator
- Single pole failure at 400 kV unit breaker during normal power operation equivalent
- Two pole failure (still closed) at 400 kV unit breaker during outage
- Single pole failure (one pole does not close) of 400 kV unit breaker at synchronization after house load operation
- A case similar to Byron 2 event, with one phase open at the unit breaker and an earth fault on the generator step-up transformer side of the breaker
- Sensitivity study of the electrical machine model because we do not have any negative sequence data of the machines

There are some technical differences between unit 1 and 2 and unit 3. The first two units have each two turbin-generator trains with splitting of the switchyard with different transmission line of the off-site grid. The unit 3 has one turbin-generator train and the off-site grid has two lines from the switchyard. Precondition for the simulations has been to have reasonable low short circuit power (worst case scenario) for each study case of the external grid. Different loading condition in the internal distribution system depending on the studied case.

The conclusion so far is to include equipment that detect unbalanced condition at cold and hot shutdown reactor and at heating before synchronizing and secure that the generator quickly will be disconnected from the external grid at out-of-step condition caused by unbalanced condition. FKA has an ongoing project to include a protection for the open phase case.

The studies of the open phase condition will continued with this type of fault in the internal power system and in the 70 kV grid, when the units has it power supply from the 70 kV grid.

8. Conclusion

As has been presented in this paper, Forsmark has been working for some years to developing detailed models and carrying out studies. An experience related to the disturbances Forsmark has suffering from is that these events, based on what we know, are initially not analysed.

The future planning is focused on unconditional work with participants to find out faults that need to be analysed in order to obtain weaknesses in the units' electrical system, which can then be addressed with some form of protection function.

The models will continue to be developed depending on the modernisation of the units, and continued be more detailed, depending on what will be needed for the future studies and limited to what can be received from the contractors or subcontractors.

VATTENFALL

ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK

CSNI International workshop on
ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs
in Light of the Fukushima Daiichi Accident

OECD Conference Centre, 2 Rue André Pascal, Paris, France, 1 – 4 April 2014

WEDNESDAY, 2 APRIL 2014

1 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Larrell

Contents

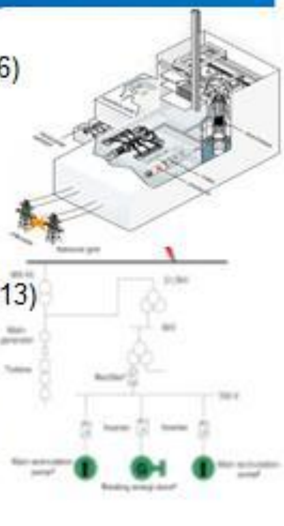
- Events
- Requirements at analysis
- Original studies
- Activity plan
- Software
- Model development, model data and validation of the model
- Presentation of made studies
- Different type of disturbance
- Questions?

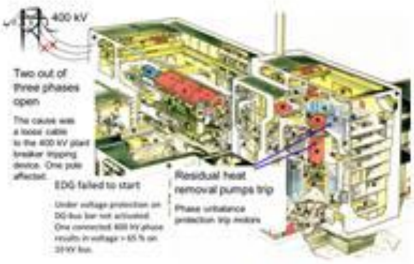
2 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Larrell

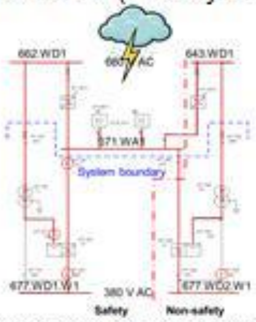
VATTENFALL

Event

- Loss of external power and loss of power supply from 2 of 4 diesel generators Forsmark 1 (25 July 2006)
- Lightning strike tripped all eight main circulation pumps at Forsmark 2 (13 June 2008)
- Lightning strike causing voltage transient in station AC net Forsmark 3, (July 2012)
- Loss of two phases of the external grid during outage shutdown with loss of decay heat removal (30 May 2013)







3 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Larrell

VATTENFALL

Requirements at analysis

- Swedish Radiation Safety Authority's regulation
- Keeping the integrity of the safety system and defence in depth
- Svenska kraftnät (Swedish national grid) regulation
- Studies for renewal project and the system and plant requirement.

4 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Larrell

VATTENFALL

Original studies, at the time of when the units was build

- Plant condition at grid disturbance:
  According to a special grid voltage profile: which from the beginning include an instant voltage drop on the generator busbar down to a level of 25 % for 0.25 s and then linear increase to 95 % for 0.5 s.
- Short circuit on each AC-busbar:
  Feeding from auxiliary transformer and start-up transformer and an initial nominal voltage to find the maximum short-circuit currents.
- Start-up of the largest electrical machine:
  The purpose is to verify the start of the largest electrical machine at the worst allowable condition (0.9 p.u. voltage and at a specified short circuit power), while not interfering other motor drives with protection tripping, etc.
- Start-up sequence of the safety and non-safety busbar.

5 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Larrell

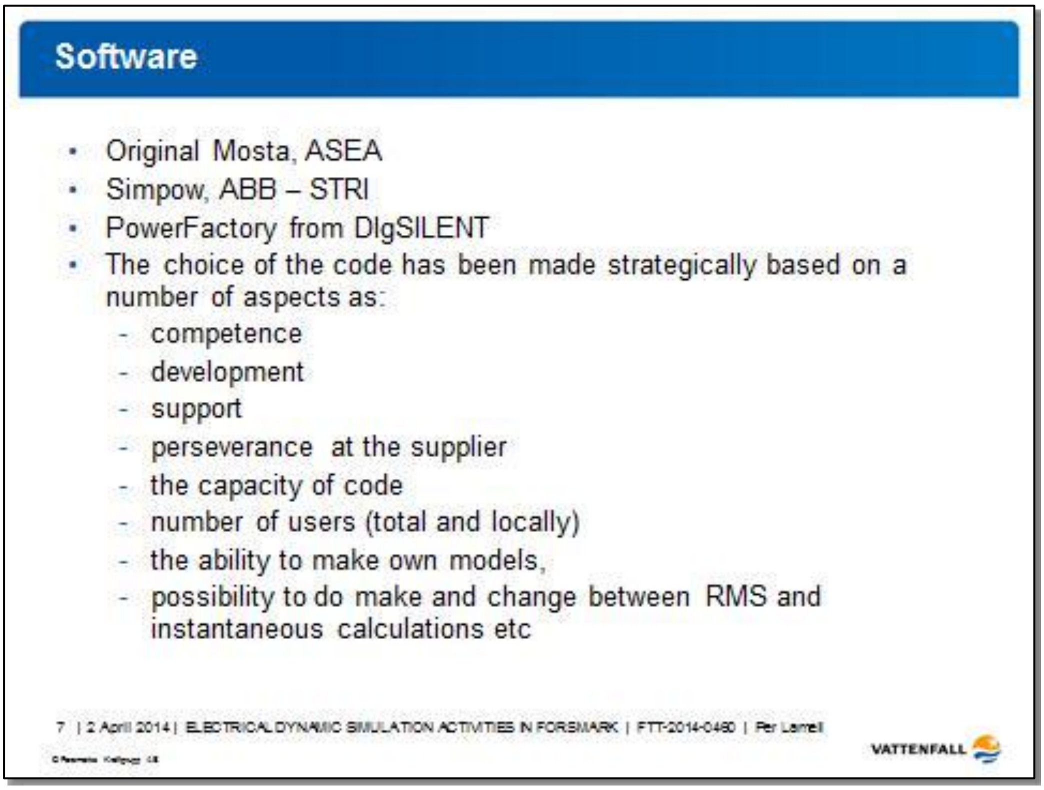
VATTENFALL

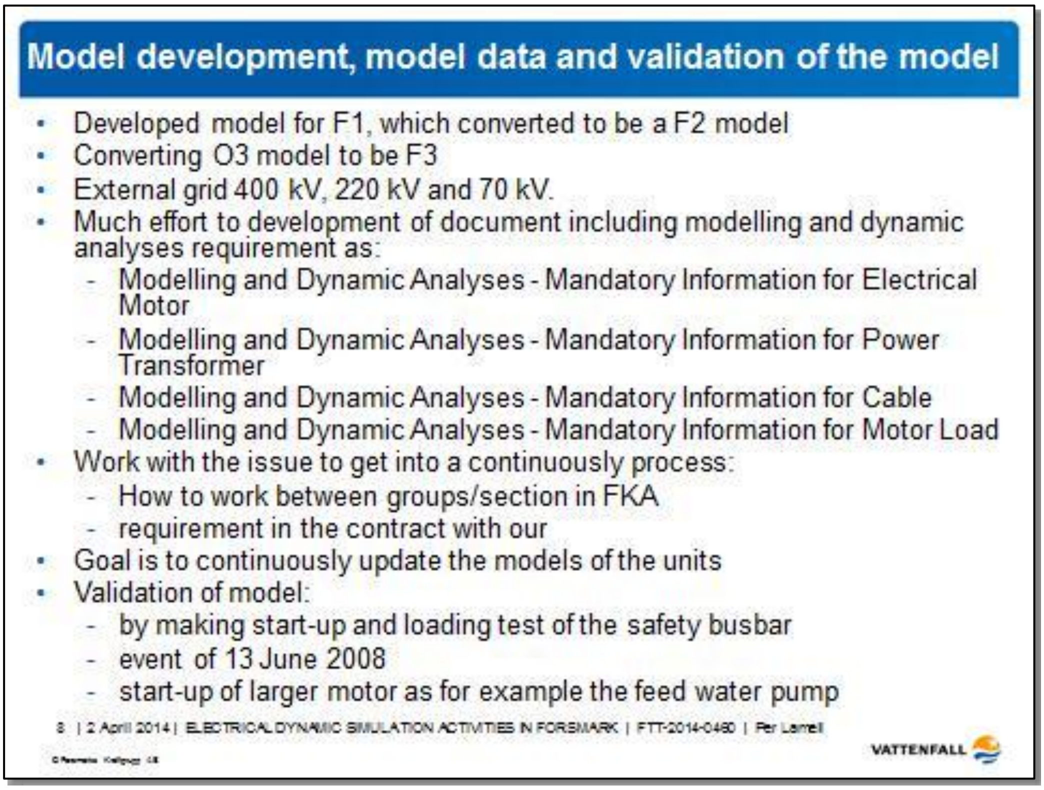
Activity plan

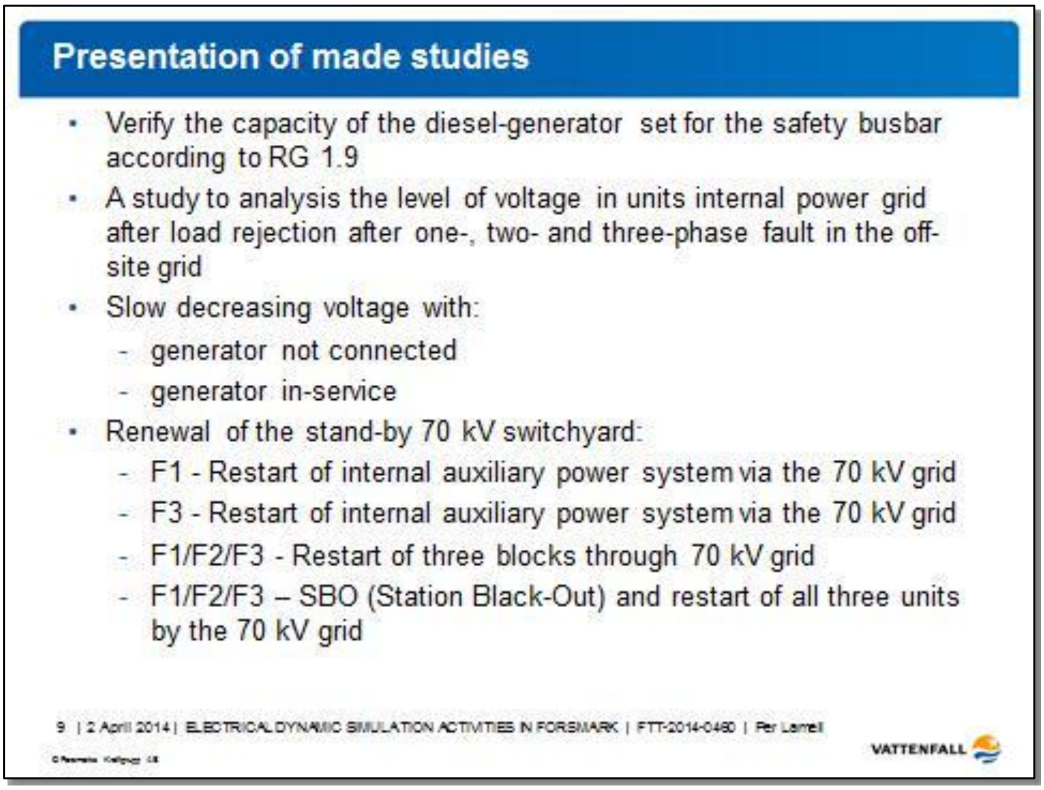
- Increased focus on unconditionally analyses of the plant behaviour during different electricity-related incidents/disturbances:
  - To make the plants more resilient and better protected.
- Basis for analysis:
  - original design philosophy to find out
    - if some knowledge has disappeared
    - if it was not possible to include the functionality because of limitation in the existing technology
  - reveal weaknesses in the functionality or design of the systems
  - renewed review of events in other plants
  - participations in conferences and meetings
- If the result reveals weaknesses evaluated:
  - need to introduce new protection equipment
  - modify existing protection configuration

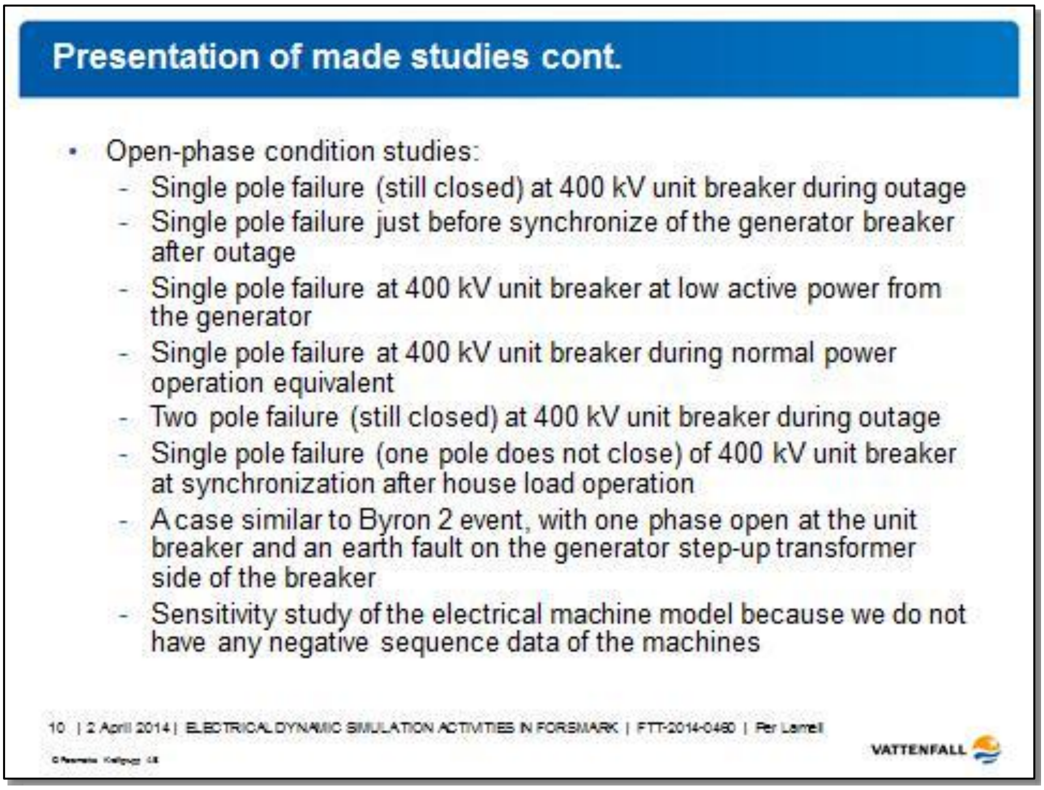
6 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Larrell

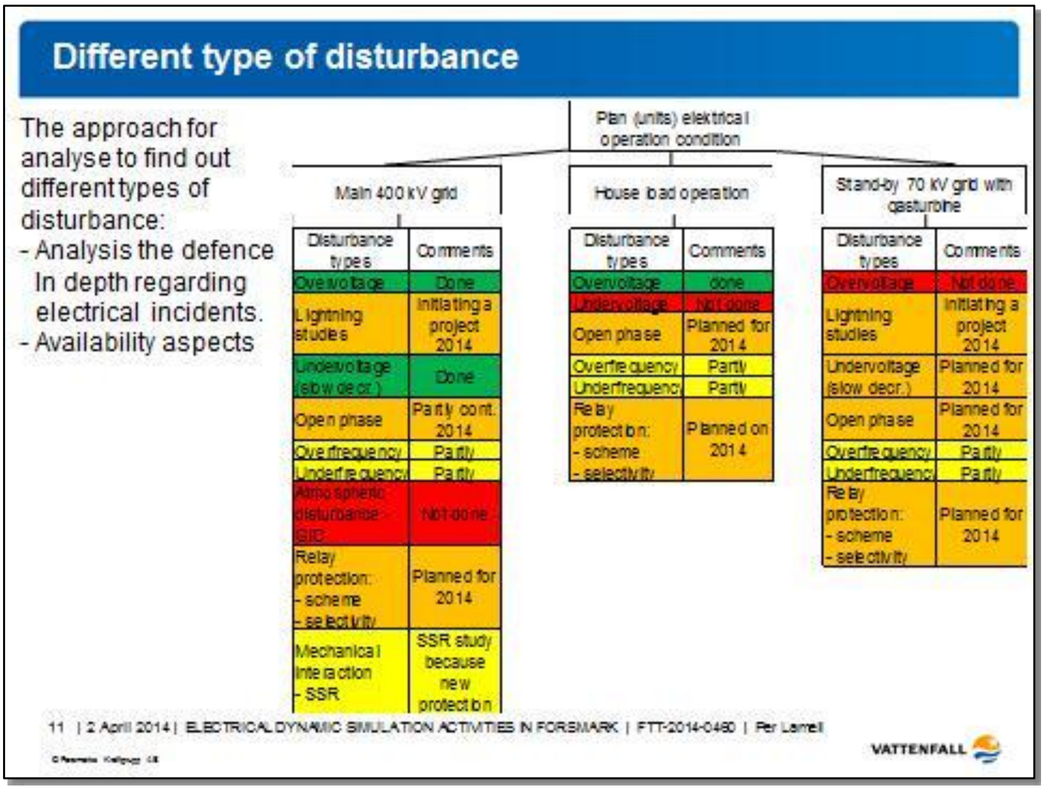
VATTENFALL

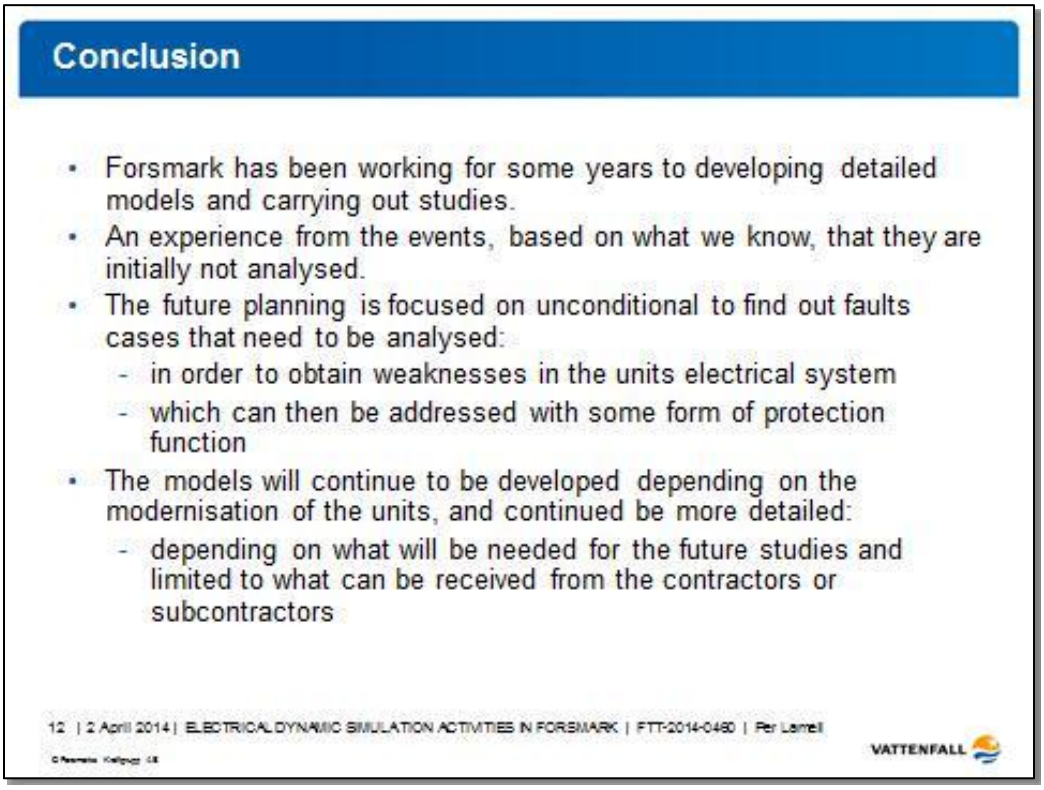

Software
Original Mosta, ASEA
Simpow, ABB – STRI
PowerFactory from DIgSILENT
The choice of the code has been made strategically based on a number of aspects as:
- competence
- development
- support
- perseverance at the supplier
- the capacity of code
- number of users (total and locally)
- the ability to make own models,
- possibility to do make and change between RMS and instantaneous calculations etc
VATTENFALL


Model development, model data and validation of the model
Developed model for F1, which converted to be a F2 model
Converting O3 model to be F3
External grid 400 kV, 220 kV and 70 kV.
Much effort to development of document including modelling and dynamic analyses requirement as:
- Modelling and Dynamic Analyses - Mandatory Information for Electrical Motor
- Modelling and Dynamic Analyses - Mandatory Information for Power Transformer
- Modelling and Dynamic Analyses - Mandatory Information for Cable
- Modelling and Dynamic Analyses - Mandatory Information for Motor Load
Work with the issue to get into a continuously process:
- How to work between groups/section in FKA
- requirement in the contract with our
Goal is to continuously update the models of the units
Validation of model:
- by making start-up and loading test of the safety busbar
- event of 13 June 2008
- start-up of larger motor as for example the feed water pump
VATTENFALL

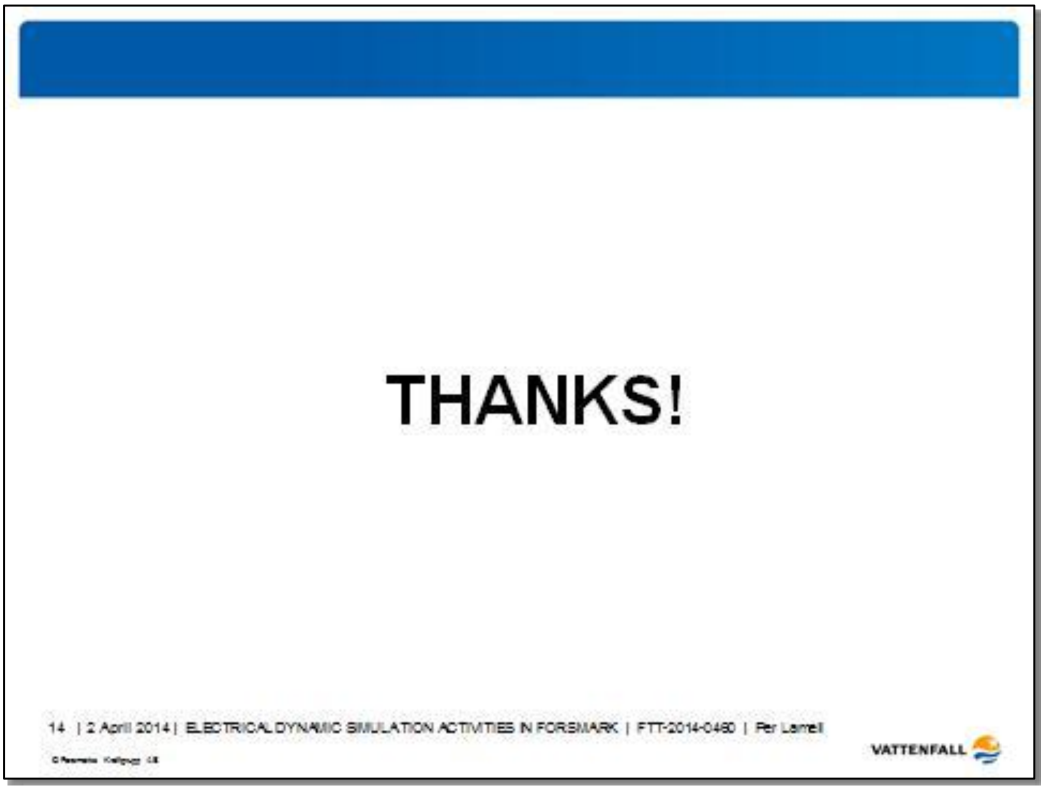

Presentation of made studies
Verify the capacity of the diesel-generator set for the safety busbar according to RG 1.9
A study to analysis the level of voltage in units internal power grid after load rejection after one-, two- and three-phase fault in the off-site grid
Slow decreasing voltage with:
- generator not connected
- generator in-service
Renewal of the stand-by 70 kV switchyard:
- F1 - Restart of internal auxiliary power system via the 70 kV grid
- F3 - Restart of internal auxiliary power system via the 70 kV grid
- F1/F2/F3 - Restart of three blocks through 70 kV grid
- F1/F2/F3 – SBO (Station Black-Out) and restart of all three units by the 70 kV grid
9 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460
VATTENFALL


Presentation of made studies cont.
Open-phase condition studies:
- Single pole failure (still closed) at 400 kV unit breaker during outage
- Single pole failure just before synchronize of the generator breaker after outage
- Single pole failure at 400 kV unit breaker at low active power from the generator
- Single pole failure at 400 kV unit breaker during normal power operation equivalent
- Two pole failure (still closed) at 400 kV unit breaker during outage
- Single pole failure (one pole does not close) of 400 kV unit breaker at synchronization after house load operation
- A case similar to Byron 2 event, with one phase open at the unit breaker and an earth fault on the generator step-up transformer side of the breaker
- Sensitivity study of the electrical machine model because we do not have any negative sequence data of the machines
10 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460
VATTENFALL


Different type of disturbance
The approach for analyse to find out different types of disturbance:
- Analysis the defence In depth regarding electrical incidents.
- Availability aspects
Plan (units) elektrical operation condition
Main 400 kV grid
Disturbance types
Comments
Overvoltage
Done
Lightning studies
Initiating a project 2014
Undervoltage (slow decr.)
Done
Open phase
Partly cont. 2014
Overfrequency
Partly
Underfrequency
Partly
Atmospheric disturbanse - GIC
Not done
Relay protection:
- scheme
- selectivity
Planned for 2014
Mechanical interaction
- SSR
SSR study because new protection
House load operation
Disturbance types
Comments
Overvoltage
done
Undervoltage
Not done
Open phase
Planned for 2014
Overfrequency
Partly
Underfrequency
Partly
Relay protection:
- scheme
- selectivity
Planned on 2014
Stand-by 70 kV grid with gasturbine
Disturbance types
Comments
Overvoltage
Not done
Lightning studies
Initiating a project 2014
Undervoltage (slow decr.)
Planned for 2014
Open phase
Planned for 2014
Overfrequency
Partly
Underfrequency
Partly
Relay protection:
- scheme
- selectivity
Planned for 2014
11 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Lamell
VATTENFALL


Conclusion
• Forsmark has been working for some years to developing detailed models and carrying out studies.
• An experience from the events, based on what we know, that they are initially not analysed.
• The future planning is focused on unconditional to find out faults cases that need to be analysed:
- in order to obtain weaknesses in the units electrical system
- which can then be addressed with some form of protection function
• The models will continue to be developed depending on the modernisation of the units, and continued be more detailed:
- depending on what will be needed for the future studies and limited to what can be received from the contractors or subcontractors
12 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Lamell
VATTENFALL


Questions?
13 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Lamell
VATTENFALL


THANKS!
14 | 2 April 2014 | ELECTRICAL DYNAMIC SIMULATION ACTIVITIES IN FORSMARK | FTT-2014-0460 | Per Lamell
VATTENFALL

Introduction of Electrical System Simulation and Analysis Used in Korean Nuclear Power Plants

Sang Hak Kim, Woo Sung Jeong

Nuclear Projects Division, KEPCO E&C
2354 Yonggudaero, Giheung-gu, Yongin-si, Gyeonggi-do, South Korea
Email: sangtop@kepco-enc.com, wsjeong@kepco-enc.com

Abstract

The purpose of this paper is to introduce the simulation methods and tools to analyze and predict the performance of the electric power distribution system for nuclear power plants (NPPs) in Korea. Electrical system design engineers are to evaluate the load flow, bus voltage profiles, short circuit levels, motor starting, and fast bus transfer under various plant operating conditions and to verify the adequacy of power distribution system for a reliable power supply to plant loads under various disturbances which could jeopardize a safe and reliable operation of nuclear power plants.

1. Introduction

The various plant operating and power supply conditions should be considered for a reliable auxiliary power system design and load allocations. The plant operating conditions have been classified to six different loading categories in power system simulation tool (Normal Operation, Plant Start-up, LOCA, Hot Standby, LOOP, and SBO). The islanded system operation with the onsite standby power supplies (e.g., emergency diesel generators and AAC diesel generators) is also evaluated. Load flow, short circuit, motor starting under all these operating conditions are simulated and evaluated for integrity of power distribution system design by use of ETAP (Electrical Transient Analyzer Program) program based on ANSI (American National Standards Institute) requirements.

2. System Configuration

2.1 Main Power (MP) System Configuration

The main power (MP) system includes essentially of the main generator, the generator circuit breaker (GCB), and the isolated phase bus (IPB). The MP system is designed to deliver generator output power to the grid interconnected with the extra high voltage switchyard (EHV SWYD) at the site through the main transformer, and to provide power supply for the plant electrical loads required for nuclear power plant operation through the unit auxiliary power transformer (UAT). This MP system is served as one of the preferred power supply (PPS) circuits.

In the event of generator circuit breaker open, the preferred power supply (PPS) circuit is still maintained since all required power supply will be fed from the grid through the main transformer and the UAT.

2.2 Auxiliary Power (AP) System Configuration

The auxiliary power (AP) system consists of subsystems: the unit auxiliary transformers (UATs), standby auxiliary transformers (SATs), 13.8 kV power system, 4.16 kV Non-Class 1E and Class 1E system, 480 V load center Non-Class 1E and Class 1E system, 480 V motor control center/low voltage Non-Class 1E and Class 1E system, diesel generators, and alternate AC power supply.

Various nominal system voltages are selected for the AP system based on the ratings of plant loads in order to ensure minimal voltage drop during the steady state and largest motor starting conditions. In nuclear power plants in Korea, the following voltage levels are typically selected for various plant loads.

- 13.8kV distribution system: Motors rated for 1,500 Hp and larger
- 4.16kV distribution system: Motors rated for 250Hp to 1,250 Hp except for the control rod drive motor generator sets
- 480V distribution system: Motors rated for 0.5Hp to 225Hp, all MOVs, lighting transformers and the control rod drive motor generator sets
- 120V distribution system: Motors rated for 0.5 Hp and below

3. Loading Category and Study Case

3.1 Loading Category

3.1.1 Plant Start-up(Category 1)

All start-up loads required for the turbine generator operation are identified and considered in this loading category. During the plant start-up stage, offsite electrical power is supplied to plant auxiliary loads via main transformer (MT) and unit auxiliary transformers (UATs) with the generator circuit breaker (GCB) open. The energy required for generator excitation system is also fed from the grid through the main transformer (MT). With all required start-up loads running, the turbine-generator can be brought up to, or near its synchronous speed so that the generator will be ready for synchronizing with the grid. Typically, an approximate 10~15% of the unit rated power are considered as plant start-up loads required for starting the unit. It is important to consider this condition especially when the power plant is remotely located from the transmission network, and the start-up power is supplied through a long and limited capacity of transmission lines. Therefore, the design engineer should coordinate with the grid operator to obtain the grid operating conditions and criteria for the transmission network.

3.1.2 Normal Operation (Category 2)

Once the turbine generator is ready for synchronizing to the grid, there are typically two ways of generator synchronizing available, i.e. automatic or manual synchronizing of generator provided by the turbine/generator control system. In automatic synchronizing, generator speed and voltage will be automatically adjusted by the turbine/generator control system so that oncoming generator can be automatically synchronized to and interconnected with the grid. In manual synchronizing, all control activities including the initiation of breaker close command should be performed by an experienced and authorized plant operator.

After the generator is connected to the grid by closing the generator circuit breaker, plant operators can gradually but smoothly increase generator output up to its rated power so that all plant loads will be fed by the generator other than by the grid.

This case models the unit at 100% load. The Normal Operation loading case is generally not as severe as the LOCA case, unless large motors are tripped on a LOCA signal. Tripping large motors on a LOCA signal is not a common design practice and is not recommended because of the impact on mechanical systems and equipment. One of the primary purposes of the Normal Operation loading case is to serve as the base loading for development of the LOCA case. A decision is required to model summer or winter HVAC loads. Alternately, two separate cases may be run to model both summer and winter HVAC loading to confirm which loading case is more severe.

3.1.3 LOCA (Loss of Coolant Accident) Condition (Category 3)

The LOCA case uses the Normal Operation loading case as a base. In this loading category, the plant operating load will be the most severe operating condition since it will further consider additional loads, which are required for supporting the LOCA condition, in addition to normal operating loads (Category 2).

Upon receipt of the LOCA signal, all required medium voltage motors will be sequentially started but all required low voltage motors will be accelerated simultaneously. Therefore, the low voltage power distribution system will consequently experience a significant voltage drop during the acceleration period of these motors following the LOCA condition. It is important to ensure that the distribution system is properly designed to mitigate this significant voltage drop within an acceptable level in the event of the LOCA.

3.1.4 Hot Standby Condition (Category 4)

In this loading category, all conditions are the same as those of normal operation (Category 2) but the generator is tripped, i.e. generator circuit breaker (GCB) is also tripped as a result of generator trip. This case simulates a bit more severe loading than that of start-up condition, and is very effective to evaluate the adequacy of SAT (Stand-by Auxiliary Transformer) rating if it is less than the UAT (Unit Auxiliary Transformer) rating.

3.1.5 Cold Shutdown Condition (Category 5)

This loading category is used to simulate the plant minimal loading condition during the unit shutdown period, and is used to analyze bus voltages to evaluate if there are any buses experiencing overvoltage, which could be detrimental effect on insulation system of electrical equipment.

The plant loads required only for supporting plant utility functions (HVAC, lighting, water supply, air supply, etc.) are modeled in this loading category. All process loads required for other loading conditions are deactivated in this loading category.

A hand calculation may be an alternative method to computer simulation, and it is a simplified evaluation with no load condition. In this alternative method, bus voltage can be calculated based on transformer voltage ratio and tap position only. Since plant minimal loads are neglected in the hand calculation, the calculated bus voltage profiles are the highest values. If these values remain within the acceptable range of electrical equipment ratings, the computer simulations are not required for a precise calculation. In Korea, this loading category is typically not modeled in the computer program.

3.1.6 LOOP (Loss of Offsite Power) Condition (Category 6)

When all offsite power is lost and House Load Operation (HLO) is failed, GCB is tripped and the normal source of power to the Class 1E auxiliary power subsystem is lost. Then the principal standby power of the emergency diesel generators are provided to the Class 1E buses.

Following the loss of voltage or prolonged degraded voltage due to a loss of power supply, the incoming breakers for the Class 1E switchgears are tripped, all the medium voltage motor loads are shed except the low voltage load centers, all Non-Class 1E bus and loads fed from the Class 1E bus will also be shed. All Non-Class 1E buses fed from the Class 1E buses will be disconnected as well. As a consequence of loss of power supply, the Class 1E emergency diesel generators (EDGs) are started.

Each Class 1E emergency diesel generator is capable of achieving the rated voltage and frequency and ready to accept loads within 20 seconds upon receipt of automatic starting command. Once the rated voltage and speed of Class 1E EDGs have been established, it is connected to the Class 1E bus in order to restore power supply to the Class 1E low voltage load centers first. Then the required medium voltage Class 1E motors are sequentially started.

For the critical Non-Class 1E loads, such as turbine-generator auxiliaries (turning gear oil pumps, turbine turning gear, and turbine-generator bearing oil lift pumps) and plant security lighting, etc., a Non-Class 1E diesel generator will automatically be started in order to restore those critical Non-Class 1E loads.

All the above scenarios are modelled in this loading category, and this category is used to simulate and evaluate the capability of the Class 1E emergency diesel generator, and Non-Class 1E diesel generator.

3.1.7 SBO (Station Blackout) Condition (Category 7)

When the Class 1E EDGs failed to start, or is unintentionally tripped during the LOOP condition, it is considered as the SBO condition, which is the worst operating condition for nuclear power plant. Once the SBO condition is detected, one common AAC diesel generator (DG) will be used for an alternative power source in order to cope with station blackout (SBO). The AAC will be available to restore power supply to the required Class 1E loads within 10 minutes in the event of the SBO condition. The AAC DG is connected to one division's loads of the Class 1E auxiliary power subsystem related to SBO coping for the selected unit. This loading category is used to simulate and evaluate the capability of AAC diesel generator.

3.2 Study Case

Based on the loading categories, six different sources can be classified as shown in figures 1 through 6. These sources and the valid load conditions are as follows:

- ○ Source 1: Main generator connected to offsite power system. It represents a valid power source for normal loading condition.
- ○ Source 2: Unit auxiliary transformers connected to offsite power system through the main transformer. It represents a valid power source for Start-up, LOCA & Hot standby loading conditions.
- ○ Source 3: Standby auxiliary transformers connected to offsite power system. It represents a valid power source for LOCA & Hot standby loading conditions.
- ○ Source 4: Class 1E emergency diesel generator. It represents a valid power source for LOOP loading condition.
- ○ Source 5: Non-1E diesel generator. It represents a valid power source for LOOP loading condition.
- ○ Source 6: AAC diesel generator. It represents a valid power source for SBO loading condition.

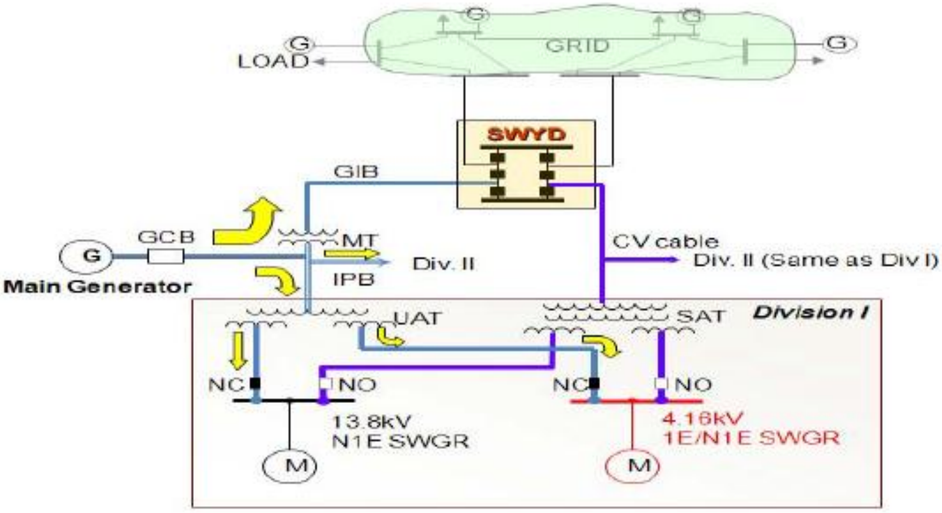


Figure 1 - Generator & Offsite Power Supply through UAT

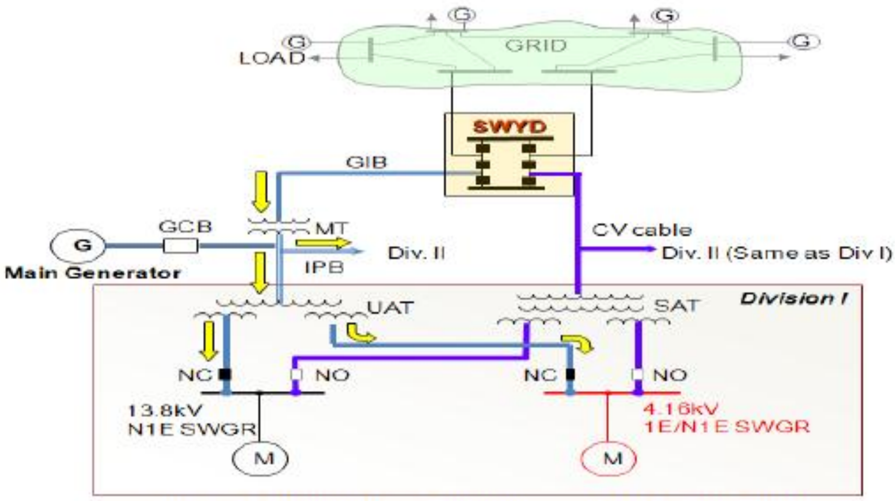


Figure 2 - Offsite Power Supply through UAT (GCB Open)

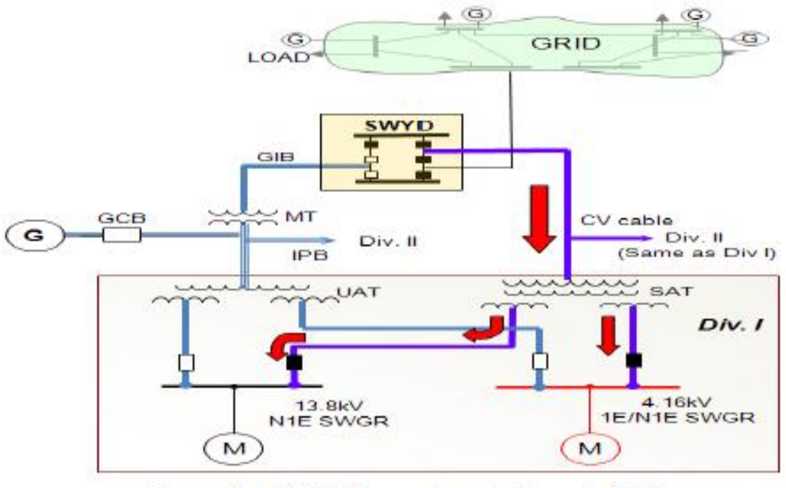


Figure 3 - Offsite Power Supply through SAT

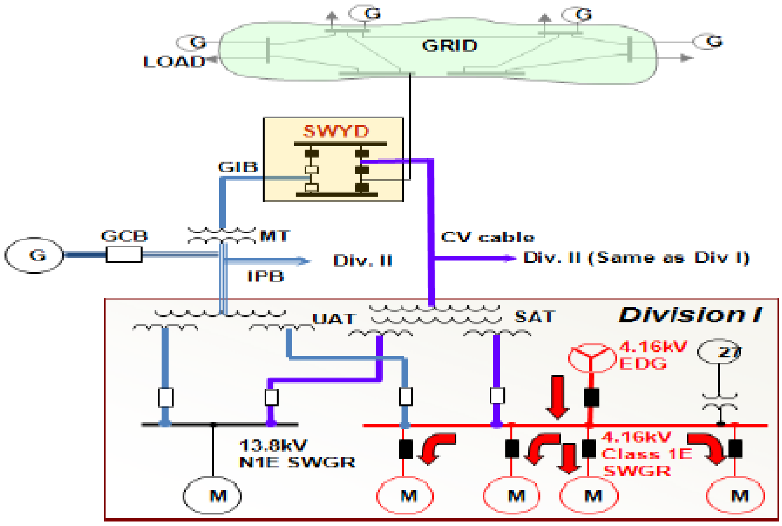


Figure 4 - Emergency Diesel Generator (LOOP)

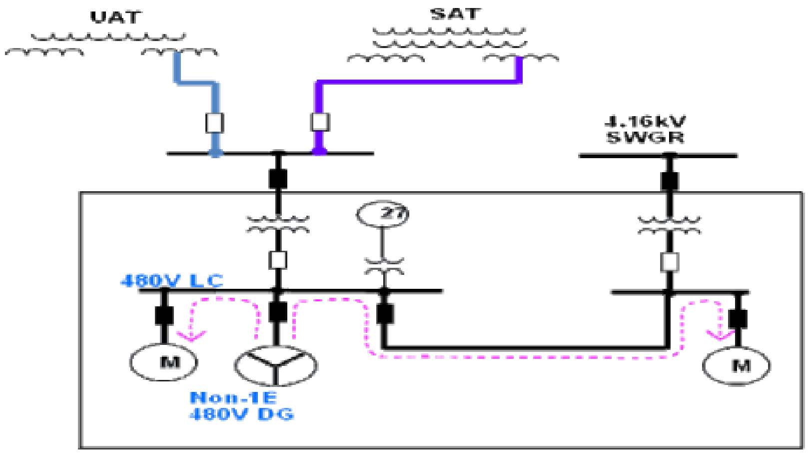


Figure 5 – Non-1E Diesel Generator (LOOP)

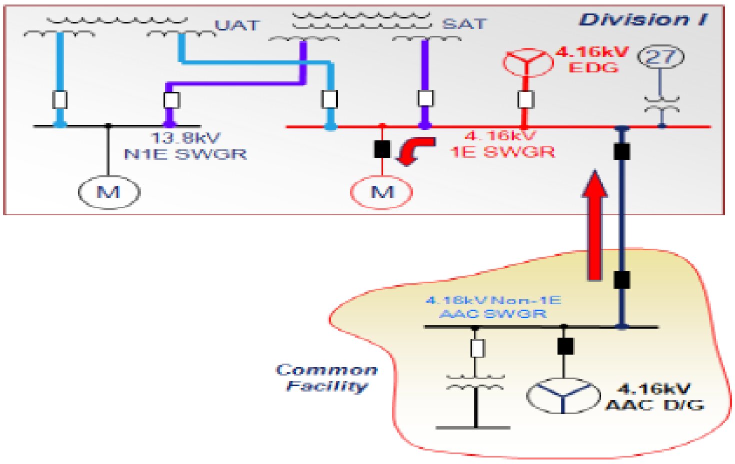


Figure 6 - AAC Diesel Generator (SBO)

3.3 Study Case Table

The various study cases can be defined by a combination of loading category and power source condition and are summarised in the following table.

Source Cond. / Load Cond.	1 (Main Gen)	2 (UAT)	3 (SAT)	4 (1E EDG)	5 (Non-1E D/G)	6 (AAC DG)
1 (Start-up)		S2L1				
2 (Normal)	S1L2					
3 (LOCA)		S2L3	S3L3			
4 (Hot Standby)		S2L4	S3L4			
6 (LOOP)				S4L6	S5L6	
7 (SBO)						S6L7

S: Study case
L: Loading Category

4. Power System Analysis

4.1 Load Flow Analysis

4.1.1 Purpose

The main purpose of load flow analysis is to simulate the bus voltage profiles, active & reactive power flows between buses as well as losses. The simulation results are used to evaluate the adequacy of plant auxiliary power distribution system design and design parameters for electrical equipment sizing under various study cases.

4.1.2 Assumption

1) The minimum and maximum operating voltages of the grid should be considered for the worst case scenarios. The minimum operating voltage of the grid (e.g. 95% of nominal voltage) is used for the worst case voltage drop and the maximum operating voltage of the grid (e.g. 105% of nominal voltage) is used for the worst case bus overvoltage calculations.
2) Maximum factory measured data is used for transformer impedance.

4.1.3 Modeling and Consideration

We should focus on the minimum and maximum loading conditions of the auxiliary power system. The maximum loading is used to analyze undervoltage conditions, and the minimum loading is used to analyze overvoltage conditions. The normal operation (Category 2, Source 1) and LOCA (Category 3, Source 2 or 3) conditions are generally considered as the maximum loading while cold shutdown (Category 5, Source 2 or 3) condition is considered as the minimum loading. However, a hand calculation is generally performed for the worst case overvoltage calculation by assuming no load condition.

4.1.4 Acceptance Criteria

1) All distribution bus voltages should be maintained between 0.9 p.u. and 1.1 p.u. under all study cases.
2) The calculated loading on the transformer and buses should not exceed the rated capacities.
3) The calculated kW and kVAR loading on the diesel generator and AAC DG should remain within the active and reactive power capability limits.

4.2 Short Circuit Current Analysis

4.2.1 Purpose

The purpose of the short circuit current calculation is to determine prospective fault current magnitudes at various locations throughout the system. Electrical equipment and system should be able to withstand the thermal and mechanical stresses induced by the short circuit current although protective devices should isolate faults at a given location. The results of short circuit current analysis are used to determine the short circuit ratings of electric equipment.

4.2.2 Assumption

1) Voltage factor: A 105% of pre-fault voltage is applied for the maximum short circuit current calculations unless otherwise noted by the grid and/or the plant operator.
2) Minimum factory measured data is used for transformer impedance.

4.2.3 Modeling

4.2.3.1 Grid & Generator Modeling

The grid and generator are the most important inputs for the short circuit current calculations since these are major sources of short circuit current contribution to a fault location. Therefore, the required inputs for short circuit current calculations must be obtained from the grid and generator manufacturer respectively. Typical data required for short circuit current calculations are as follows:

Grid – 3 Phase short circuit capacity and X/R ratio
Generation – generator rating, impedances, and X/R ratio

4.2.3.2 Motor Modeling

Motors are the second major sources of short circuit current contribution to a fault location. Therefore, all medium and low voltage motors are modelled individually in the simulation program based on the information provided by motor suppliers. Typical data required for induction motors are the rated power, voltage, and %LRC (Locked Rotor Current). ETAP uses ANSI C37.010[1] standard multiplying factors for calculating the positive sequence short-circuit impedances.

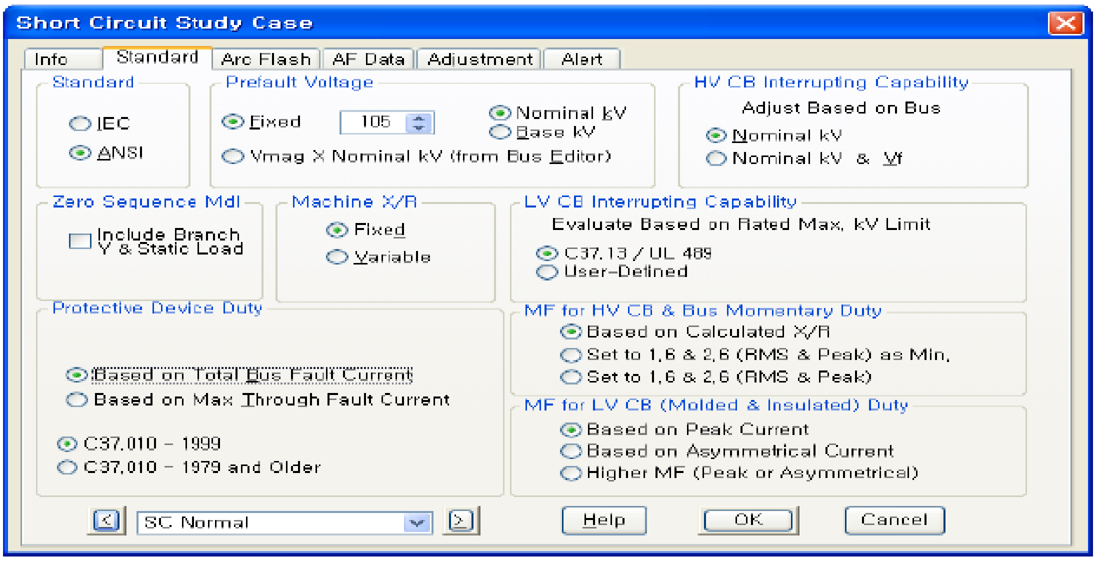
---

[1] IEEE Std C37.010, *IEEE Application Guide for AC High-Voltage Circuit Breakers Rated on a Symmetrical Current Basis Recommended Practice for Industrial and Commercial Power Systems Analysis, 1999(R2005)*

4.2.3.3 Lumped Load Modeling

Average %LRC (Locked Rotor Current) and % motor load in lumped load kVA are required for calculations. The procedure for calculating positive sequence short circuit impedance is the same as that of individual motor modeling.

4.2.4 Short Circuit Study Case



1) Prefault Voltage and Protective Device Duty

Apply 105% of nominal voltage for the maximum short circuit current calculation. Calculation results are based on 'Total Bus Fault Current' option since this option is to calculate and summate all contribution currents to a fault location for a conservative design.

2) MF for HV CB & Bus Momentary Duty

With "based on calculated X/R" option selected, the multiplication factors used to compute the asymmetrical and peak duty for high-voltage circuit breakers and high-voltage buses are based on calculated system X/R ratio.

3) MF for LV (Molded & Insulated) Duty

All LV circuit breakers used in Korean NPPs are classified as the unfused breaker type. So, "Based on Peak Current" option is selected to calculate multiplication factor (MF) based on the peak current, which is the same method used for calculating MF for an unfused low voltage power circuit breaker.

4.2.5 Consideration

It is important to assume and define the most severe case for short circuit current calculations. During the plant normal operation condition, the Class 1E emergency DG is not synchronized to the system. But, the periodic load-run test is required for the Class 1E EDG to ensure its intended functions in accordance with IEEE during the plant operation in service. In such that case, the Class 1E EDG under load-run test, which means synchronized to plant power distribution system, will provide an additional short circuit contribution current throughout the system. It will increase the system short circuit current levels and should be considered as the most severe condition for the short circuit current calculations. Therefore, Category 2 and Source 1 condition with the Class 1E EDG (Emergency diesel generator) should be considered in the calculations.

4.2.6 Acceptance Criteria

1) Results of short circuit current calculations should not exceed the momentary and interrupting ratings of medium voltage and low voltage circuit breakers.
2) The short circuit rating of buses should not be less than the prospective fault currents.

4.3 Motor Starting Analysis

4.3.1 Purpose

Large induction motors draw six (6) or seven (7) times their full load currents from their power supply under starting conditions, which may last up to several seconds. One of the resulting effects of this current surge is a voltage drop in the network which may disturb the normal operation of other loads, flickering of lights, contactors dropping out and voltage sensitive equipment malfunctioning. The purpose of motor starting calculations is to ensure that the voltage profile of the electrical network remains within the specified limits and that the motor can be accelerated to its rated speed.

4.3.2 Assumptions

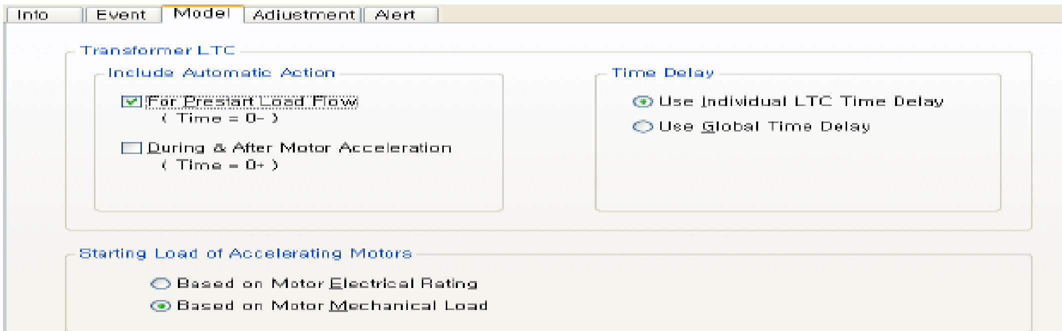
1) The minimum grid operating voltage should be taken into consideration. It should be assumed to be 95% of system nominal voltage unless otherwise noted by the grid and/or plant operator.
2) Maximum factory measured data is used for transformer impedance.

4.3.3 Modeling

There are two types of motor starting calculations: Dynamic Motor Acceleration and Static Motor Starting. In the Dynamic Motor Acceleration calculation, the entire process of acceleration is shown. This method is used to analyse fast bus transfer. In the Static Motor Starting method, the starting motors are modeled by locked-rotor current. This model is used to confirm voltage at the moment of starting and after finishing motor starting.

In Korean NPP design, the Static Motor Starting method is generally carried out for the early stage of power distribution system design since the dynamic motor starting method requires extensive motor information to be provided by motor supplier. Therefore, the dynamic motor modeling is typically applied to the fast bus transfer study.

4.3.4 Motor Starting Study Case



1) Transformer LTC
   It is assumed OLTC(on load tap changer) is not operated during starting time. If "For Prestart Load Flow" option is selected, voltage regulation actions reflected only prestart loading conditions.

2) Starting Load of Accelerating Motors
   "Based on Motor Mechanical load" option is selected for dynamic motor starting method because actual load torque based on rated output is used. In this option the load curve will be applied as it is without any adjustments.

4.3.5 Consideration

Generally, a starting of the largest motor will result in the most severe voltage drops on the distribution power system. Therefore, it is considered if the largest motor can start successfully, it is reasonably acceptable to assume that other smaller motors will also start successfully. Normal (Category 2, Source 1) and start-up (Category 1, Source 2 or 3) conditions are typically used for motor starting study.

In the event of the LOCA condition, a group of low voltage motors are started simultaneously upon receipt of LOCA signal. The associated low voltage power distribution system will experience the most significant voltage drops with the low voltage motors starting. Therefore, this condition is also essential to demonstrate that power distribution system is adequately designed for successful motor starting so that all motors can perform their safety functions coping with the LOCA condition.

4.3.6 Acceptance Criteria

The minimum required motor terminal voltage for Non-Class 1E motors and the Class 1E motors should not be less than 80% and 75% of motor rated voltage respectively.

4.4 Fast Bus Transfer Analysis

4.4.1 Purpose

For nuclear power plants in Korea, the main purpose of the motor bus transfer is to transfer the Class 1E motor loads from one power source to an alternate power source in order to maintain continuous power supply for the Class 1E motor loads without power interruptions. Therefore, a fast bus transfer scheme is typically employed at nuclear power plants in Korea.

During the fast bus transfer process, there would be high risk of excessive shaft torque which could cause mechanical damages and/or increase the shaft fatigues resulting in motor lifetime reduction. Therefore, the fast bus transfer study is to simulate and evaluate the effect of loss of normal power source (fed from the UAT) and see if the fast bus transfer is electrically feasible to an alternate power source (fed from the SAT) for the Class 1E motor bus, and to determine if ANSI C50.41[2] criteria can be satisfied. If fast bus transfer fails and residual voltage is below 30% of rated voltage, residual voltage transfer is conducted.

---

[2] IEEE Std C50.41, *American National Standard for Polyphase Induction Motors for Power Generating Stations, 2000*

4.4.2 Assumptions

1) The system voltage angle and pu V/Hz are assumed as zero (0) degree and a 1 p.u. respectively for conservative results for the resultant pu V/Hz.
2) Any faults on the Class 1E motor bus (Switchgear/MCC) shall not initiate the fast bus transfer process.
3) For breaker opening and closing time, the minimum incomer opening time and the maximum alternative incomer closing time should be used for conservative calculations of the worst case out of phase condition.
4) Assume there is a fault on the primary and/or secondary windings of the UAT so that the fast bus transfer scheme can start bus transfer process to an alternate power source (i.e. SAT.)

4.4.3 Modeling and Consideration

1) All medium voltage motors are individually modelled in equivalent circuit representing stator and rotor windings, and load torque characteristics are modelled in the simulation program. This information should be provided by the suppliers for a precise model.
2) Plant normal operation loading and configuration (Category 2, Source 1) are considered for the fast bus transfer study.

4.4.4 Acceptance Criteria

1) Fast transfer occurs within a time period of 10 cycles or less.
2) The maximum phase angle between the motor residual V/Hz vector and the system equivalent V/Hz vector does not exceed 90 degrees.
3) The resultant V/Hz between the motor residual V/Hz phasor and the incoming source V/Hz phasor at the instant of transfer completion does not exceed 1.33 pu V/Hz on the motor rated voltage and frequency basis.
4) Class 1E motors should be able to re-accelerate to its rated speed as a result of the fast bus transfer process.
5) During the fast bus transfer processing, any nuisance operations of protective relaying system should be avoided. If it would be unavoidable, proper changes to relay settings should be recommended.

5. Conclusions and Recommendations

This paper has introduced typical studies for power distribution system design applied to nuclear power plants in Korea. In addition, protective relay coordination study, power system harmonic analysis, DC short circuit current study and transient stability, etc. are also carried out during the detail engineering phase although those studies are not presented in this paper. Throughout various power system studies, power distribution system is adequately designed for a reliable and safe operation of nuclear power plants.

During design and engineering phase, it is often difficult to obtain a final confirmed data, i.e. tested values for critical equipment parameters such as final transformer impedance, etc., for power system and equipment modeling required for simulation and analysis. Therefore, as-built calculations with the final tested values are very important step to ensure adequacy of power distribution system design.

Once the as-built calculations are carried out, the next step is to verify simulation results and all assumptions used in power systems studies in comparison with the actual measurement in the field prior to commencing initial full-power reactor operation. The recommended procedures for field verification and test are well elaborated in NUREG-0800 BTP 8-6[3], "Adequacy of Station Electric Distribution System Voltages. "

Throughout all above steps, a reliable and safe design of electrical power distribution system will be eventually ensured for nuclear power plant operation.

References

1) IEEE Std 399, "Recommended Practice for Industrial and Commercial Power Systems Analysis," 1997.

2) IEEE Std C37.010, "Application Guide for AC High-Voltage Circuit Breakers Rated on a Symmetrical Current Basis," 1999(R2005).

3) IEEE Std C50.41, "Standard for Polyphase Induction Motors for Power Generating Stations," 2000.

4) NUREG-0800, BTP 8-6, "Adequacy of Station Electric Distribution System Voltages," 2007.

5) 10 CFR 50, Appendix A, "General Design Criteria for Nuclear Power Plant."

6) Regulatory Guide 1.93, "Availability of Electric Power Sources, 2012."

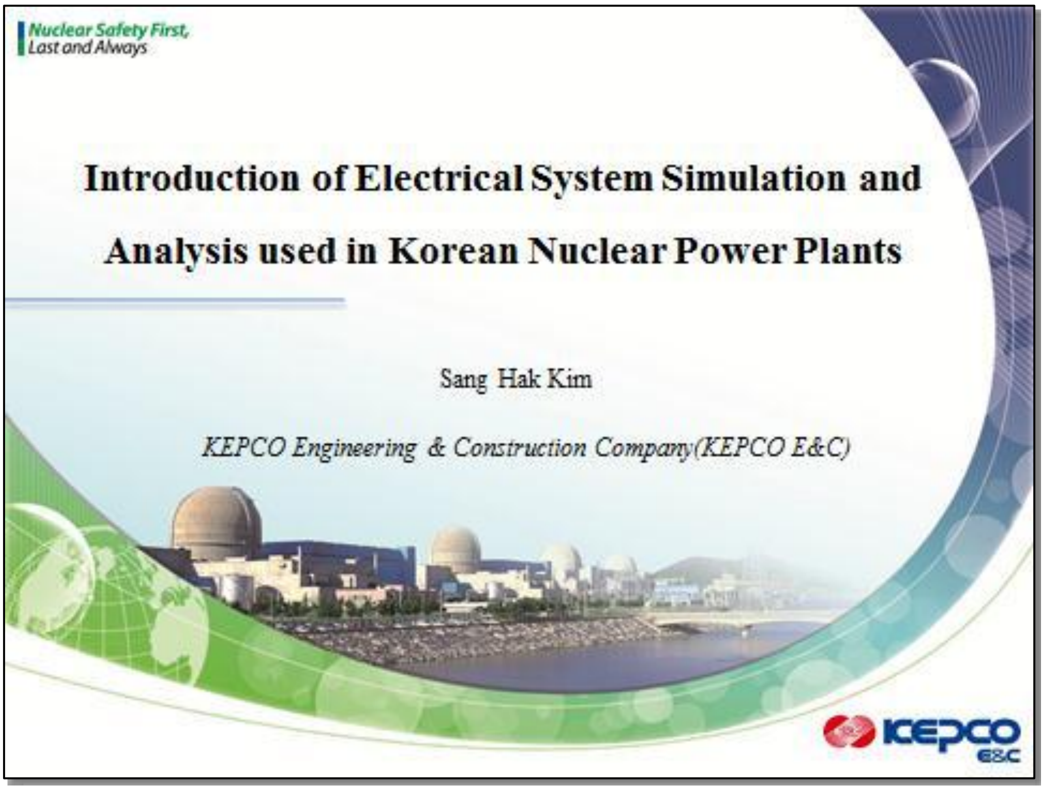
7) Regulatory Guide 1.32, "Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants," 2004.

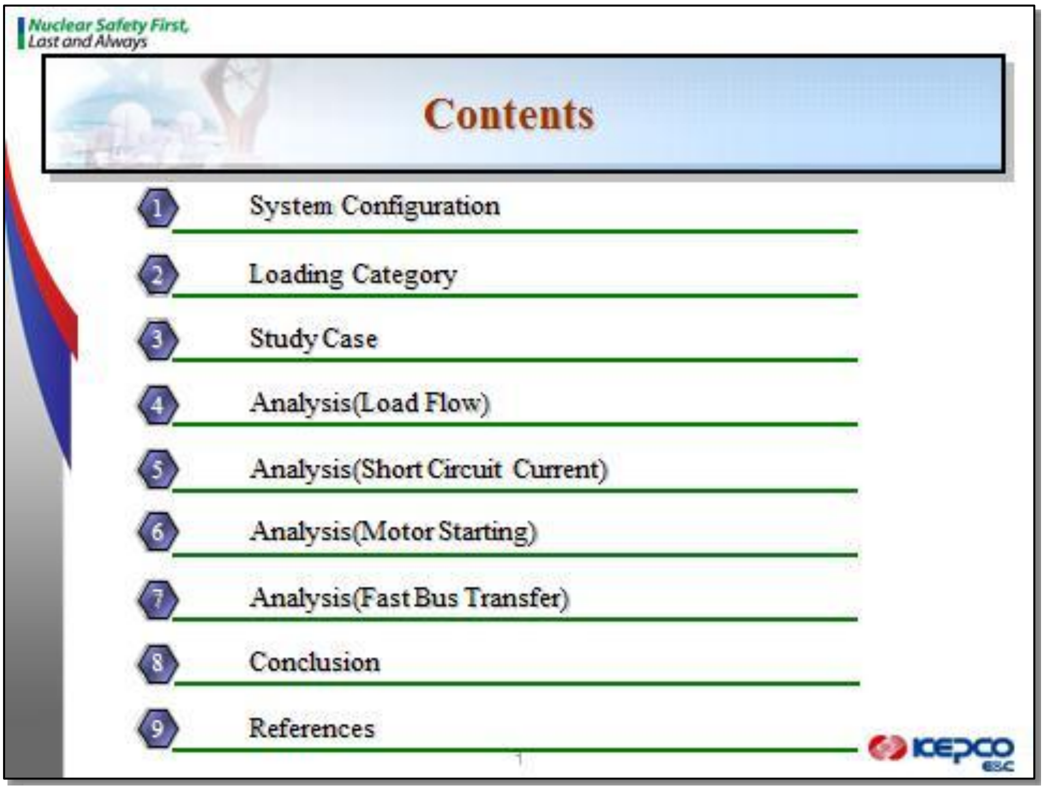
8) Regulatory Guide 1.155, "Station Blackout," 2012.

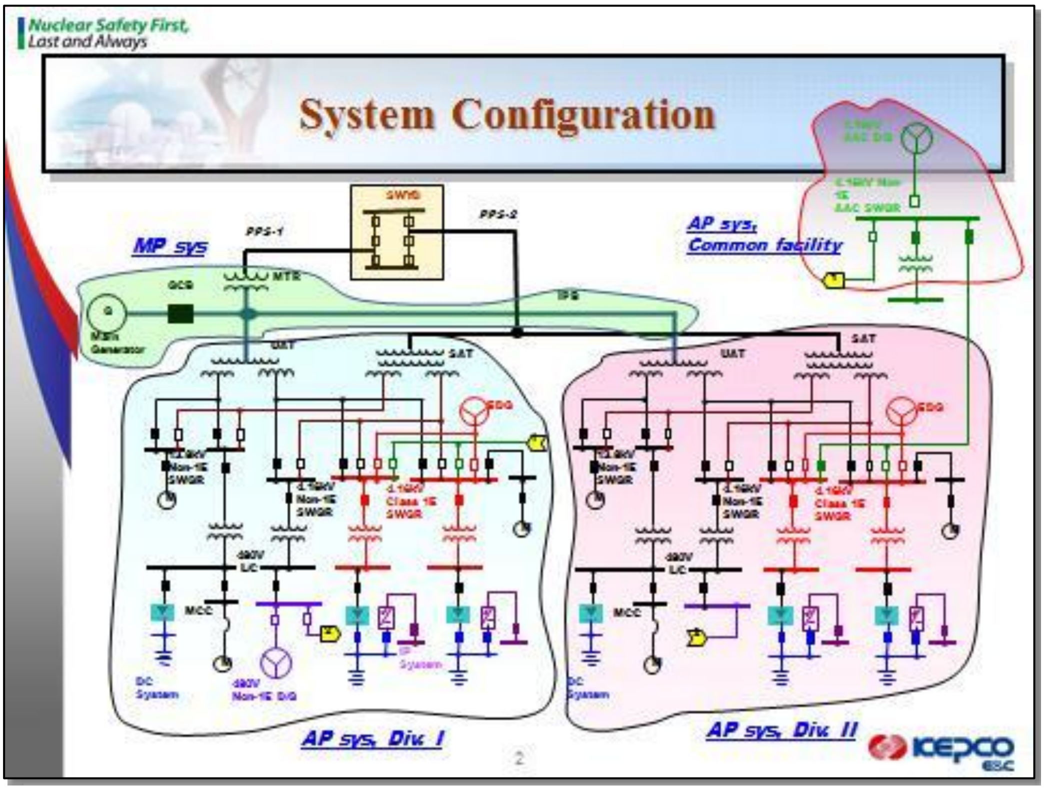
9) IEEE Std 765, "Standard for Preferred Power Supply(PPS) for Nuclear Power Generating Stations," 2006.

10) IEEE Std 741, "Criteria for Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations," 2007.

[3] NUREG-0800 BTP 8-6, *Adequacy of Station Electric Distribution System Voltages , 2007*


Nuclear Safety First,
Last and Always
Introduction of Electrical System Simulation and
Analysis used in Korean Nuclear Power Plants
Sang Hak Kim
KEPCO Engineering & Construction Company(KEPCO E&C)
KEPCO
E&C


Nuclear Safety First,
Last and Always
Contents
1 System Configuration
2 Loading Category
3 Study Case
4 Analysis(Load Flow)
5 Analysis(Short Circuit Current)
6 Analysis(Motor Starting)
7 Analysis(Fast Bus Transfer)
8 Conclusion
9 References
1
KEPCO
E&C



Nuclear Safety First,
Last and Always

System Configuration

- **Offsite Power System**

  Switchyard system is designed as interface facility between the nuclear power plant and transmission system, and provide a functions as follows;

  - Sends a power plant output to the transmission system
  - Provides a offsite power to plant auxiliary loads

- **Onsite Power System**

  Onsite power system consists of Main Power (MP), Auxiliary Power (AP), DC/IP and Emergency Power Sources, and provides a function as follows;

  - To provide a reliable power to plant auxiliary loads
  - To provide a emergency power for safe shutdown

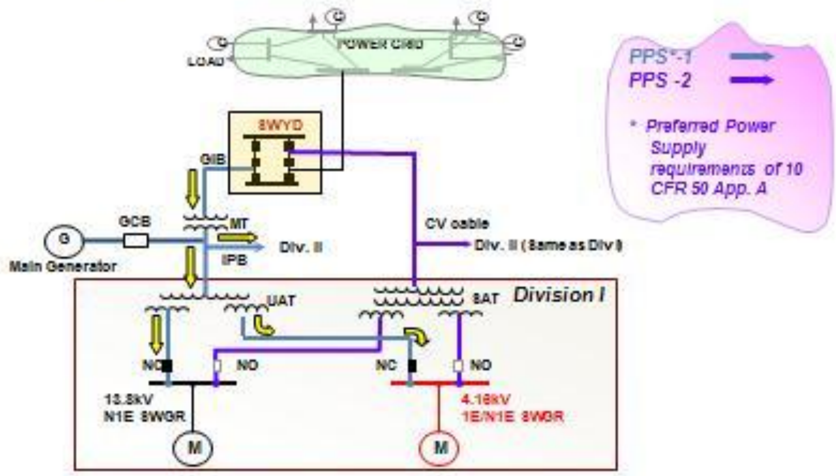
3

KEPCO E&C

Nuclear Safety First, Last and Always

Loading Category(Plant Start-up)

- Plant Start-up (Category 1)



4

KEPCO E&C

Nuclear Safety First, Last and Always

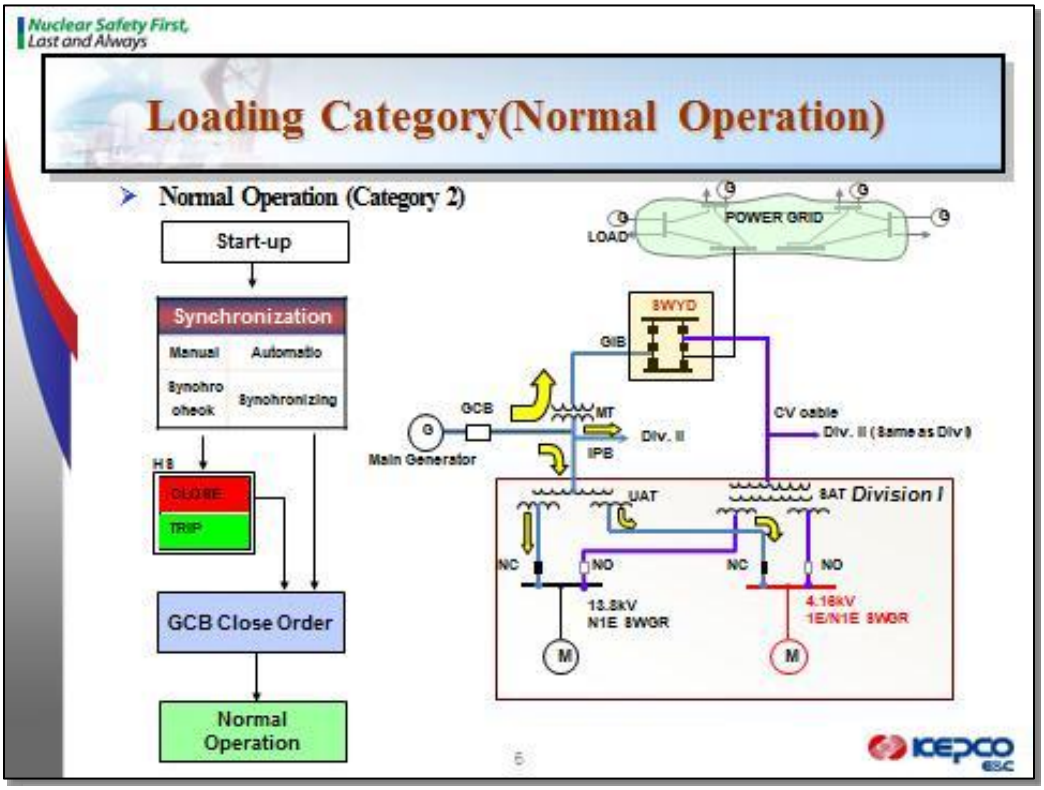
Loading Category(Plant Start-up)

- Plant Start-up (Category 1)

  The start-up operating condition is considered important especially when the power plant is at a remote location and the start-up power is supplied through a long and limited capacity transmission lines. The design engineer should have the client's accurate operating criteria for the transmission network.

5

KEPCO E&C



Nuclear Safety First, Last and Always

Loading Category(Normal Operation)

- Normal Operation (Category 2)
  - This case models the unit at 100% loading.
  - This loading case is generally not as severe as the LOCA case, unless large motors are tripped on a LOCA signal. Tripping large motors on a LOCA signal is not a common design practice.
  - One of the primary purposes of the Normal Operation loading case is to serve as the base loading for development of the LOCA case.
  - Two separate cases may be run to model both summer and winter HVAC loading to confirm which loading case is more severe.

7

KEPCO E&C

Nuclear Safety First, Last and Always

Loading Category(LOCA)

- **LOCA(Loss of Coolant Accident) Condition(Category 3)**
  - The LOCA case uses the Normal Operation loading case as a base.
  - This case generally models the most severe loading on the auxiliary power system.
  - Upon receipt of the LOCA signal, all required medium voltage motors will be sequentially started.
  - All required low voltage motors will be accelerated simultaneously.
  - The low voltage power distribution system can experience significant voltage drops during the motor acceleration period for these motors.

8

Nuclear Safety First, Last and Always

Loading Category(Hot Standby)

- **Hot Standby Condition(Category 4)**
  - This loading case models the loading immediately after a unit trip.
  - The Hot Standby loading case uses the Normal Operation loading case as a base.
  - In many instances, this case can be a more severe case than Start Up.

9

Nuclear Safety First, Last and Always

Loading Category(Cold Shutdown)

- **Cold Shutdown Condition(Category 5)**
  - This case models the lightest expected loading for the unit during times when the unit is shutdown. It is used to evaluate bus voltages to confirm that no equipment experiences overvoltage conditions.
  - Only those loads required to support plant utility functions (HVAC, lighting, water supply, air supply, etc.) are modeled as "on" for the Cold Shutdown loading case.
  - A hand calculation can be used for a simplified version of this case. All loads are assumed off, and the calculation confirms that no buses are overvoltaged based on transformer turns ratios and tap position only.

    If voltage remain within the acceptable range of electrical equipment ratings, the computer simulations are not required.

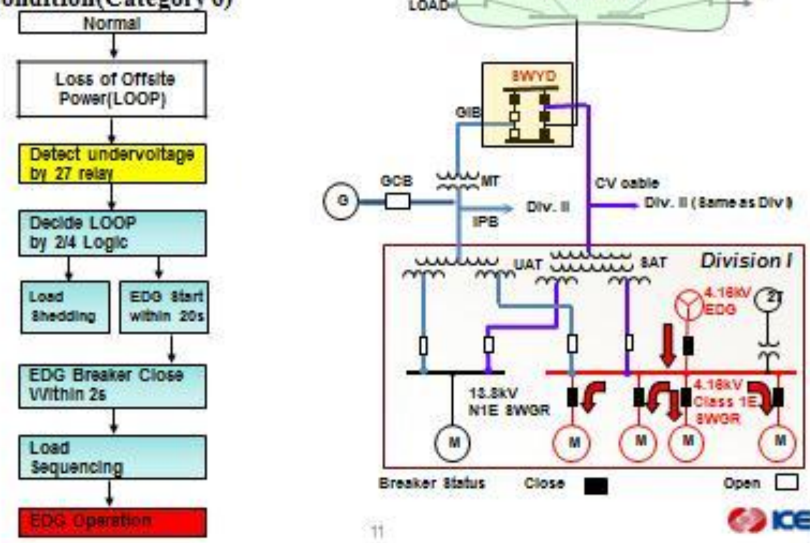
10

KEPCO E&C

Nuclear Safety First, Last and Always

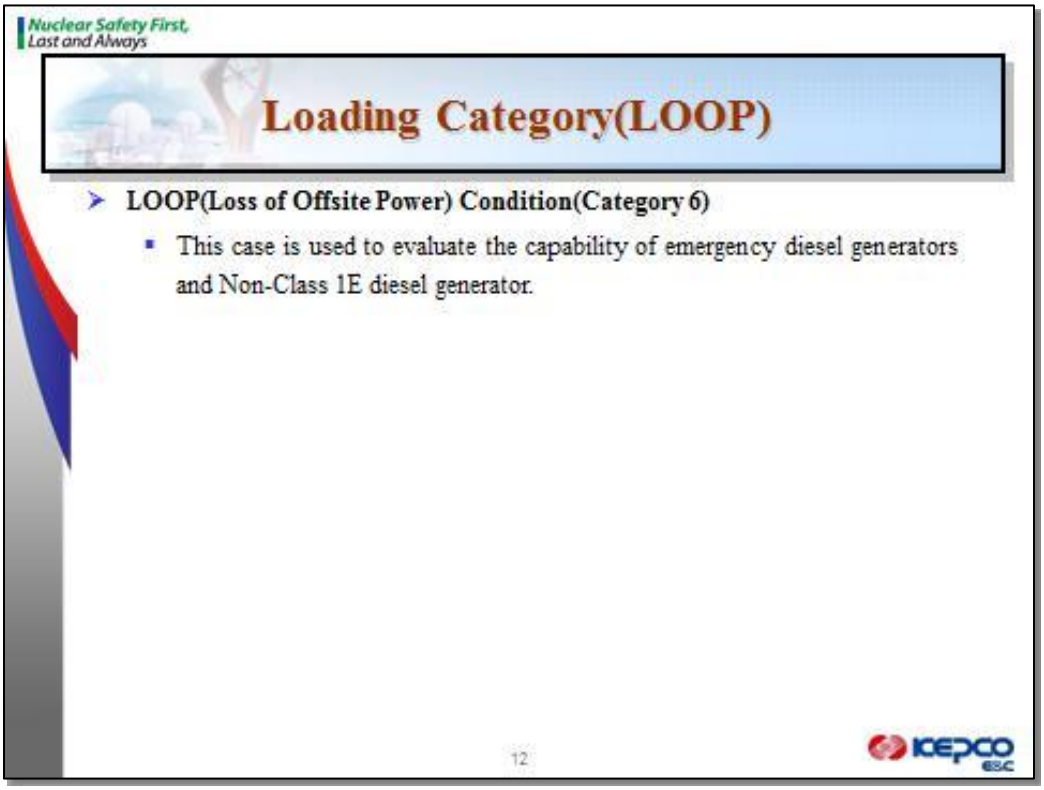
Loading Category(LOOP)

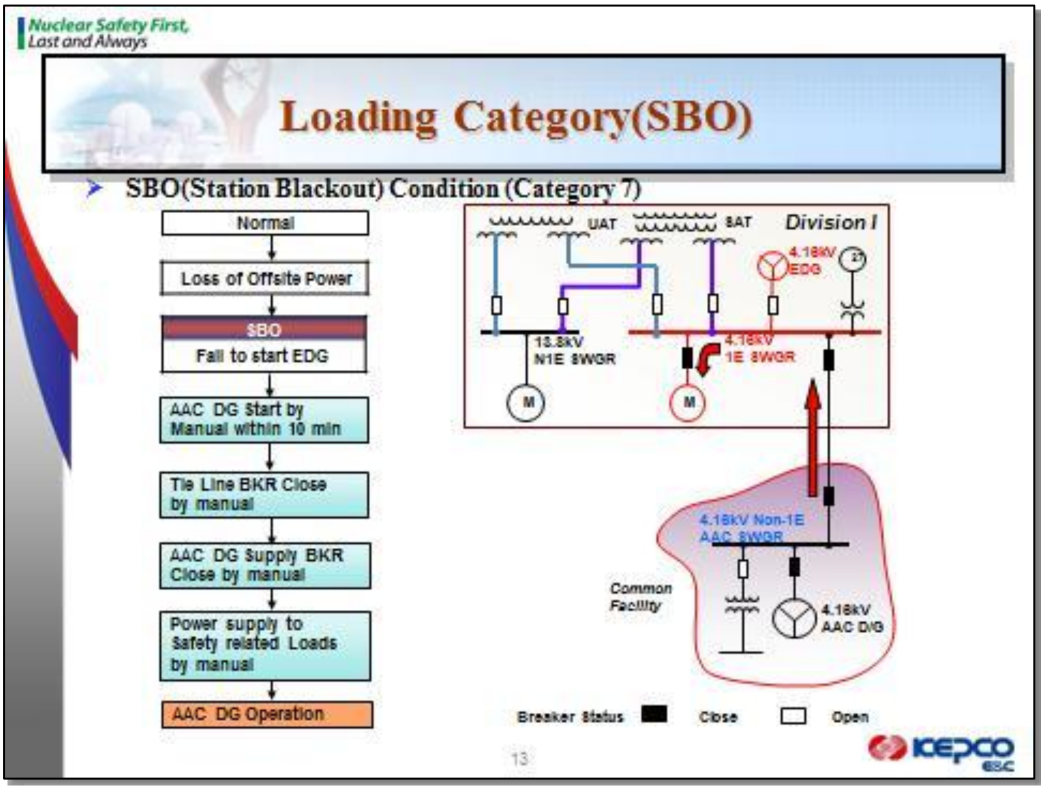
- **LOOP(Loss of Offsite Power) Condition(Category 6)**



11

KEPCO E&C


Nuclear Safety First, Last and Always
Loading Category(LOOP)
LOOP(Loss of Offsite Power) Condition(Category 6)
This case is used to evaluate the capability of emergency diesel generators and Non-Class 1E diesel generator.
12


Nuclear Safety First, Last and Always
Loading Category(SBO)
SBO(Station Blackout) Condition (Category 7)
Normal
Loss of Offsite Power
SBO
Fail to start EDG
AAC DG Start by Manual within 10 min
Tie Line BKR Close by manual
AAC DG Supply BKR Close by manual
Power supply to Safety related Loads by manual
AAC DG Operation
UAT
SAT
Division I
4.16kV EDG
13.8kV N1E SWGR
4.16kV 1E SWGR
M
4.16kV Non-1E AAC SWGR
Common Facility
4.16kV AAC D/G
Breaker Status
Close
Open
13

Nuclear Safety First, Last and Always

Loading Category(SBO)

- **SBO(Station Blackout) Condition (Category 7)**
  - This case is used to evaluate the capability of AAC diesel generator.

14

KEPCO E&C

Nuclear Safety First, Last and Always

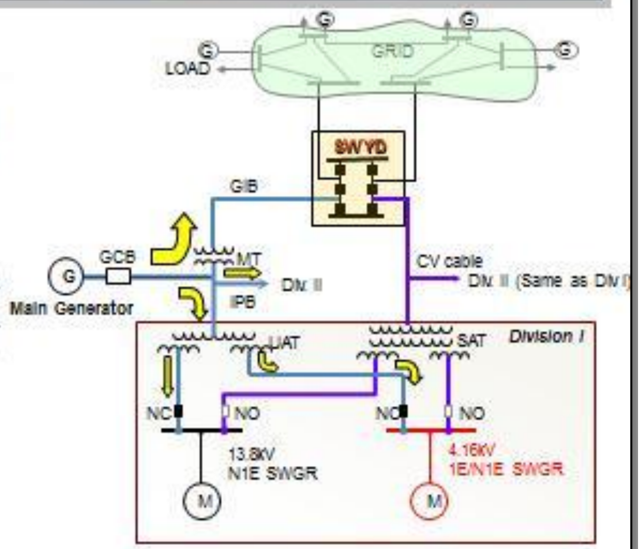
Study Case

- **Study Case**

Based on loading category six different sources can be classified These sources are follows:

- Source 1

  Main generator connected to offsite power system. This source is valid for normal loading condition.



15

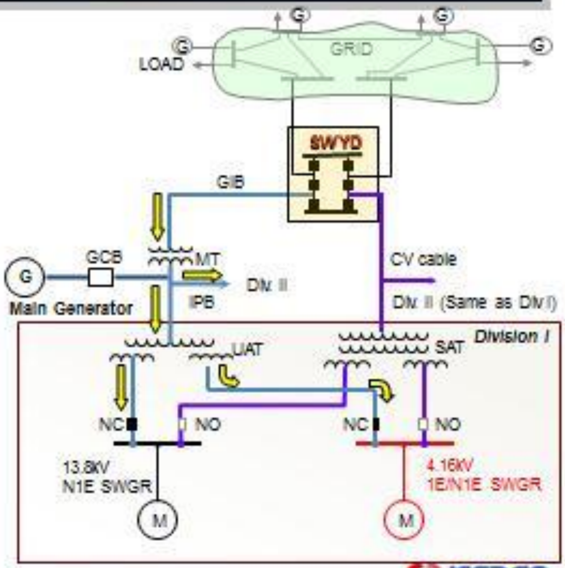
KEPCO E&C

Nuclear Safety First, Last and Always

Study Case

- Source 2

Unit auxiliary transformers connected to offsite power system through the main transformer (back feeding). This source is valid for Start-up, LOCA & Hot standby loading conditions.



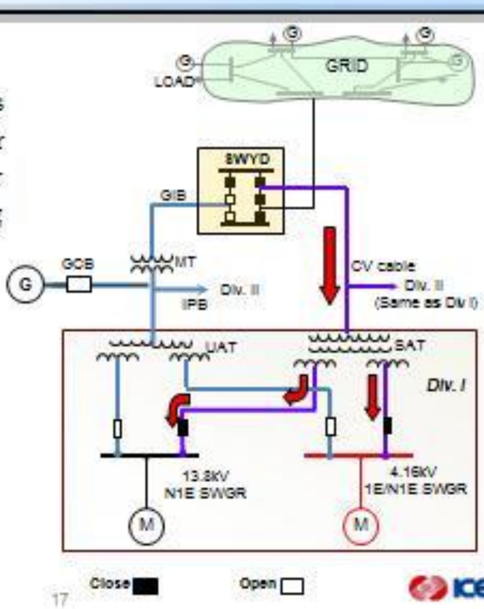
16 KEPCO E&C

Nuclear Safety First, Last and Always

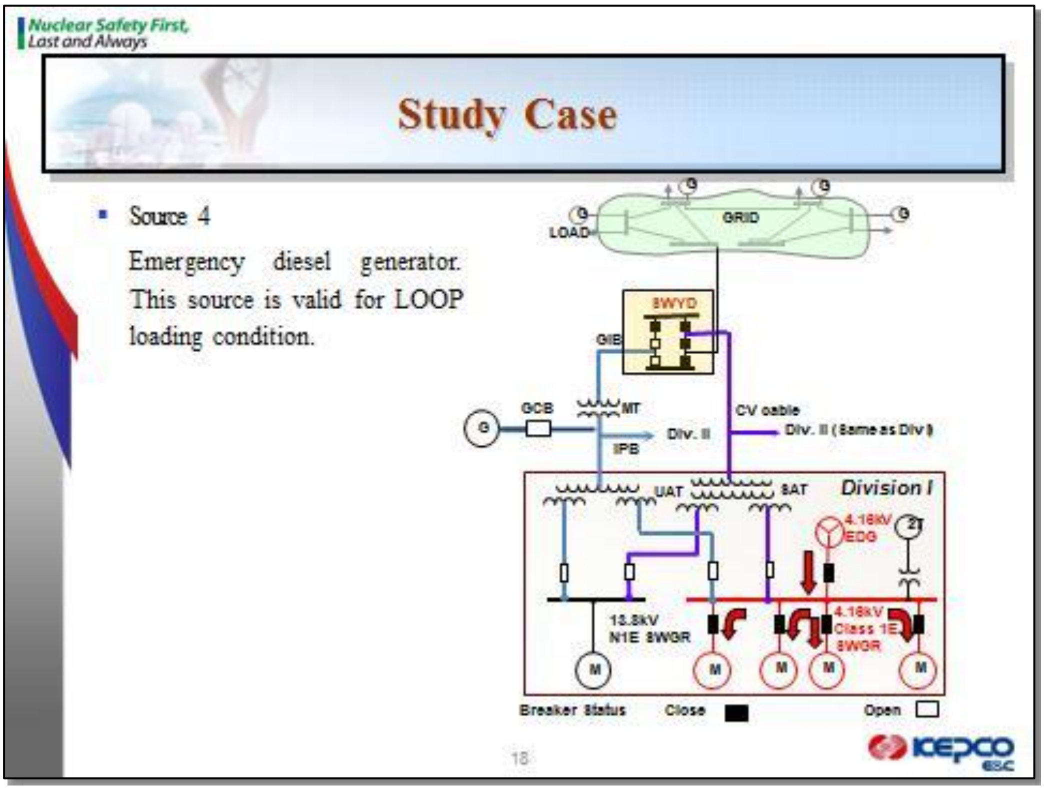
Study Case

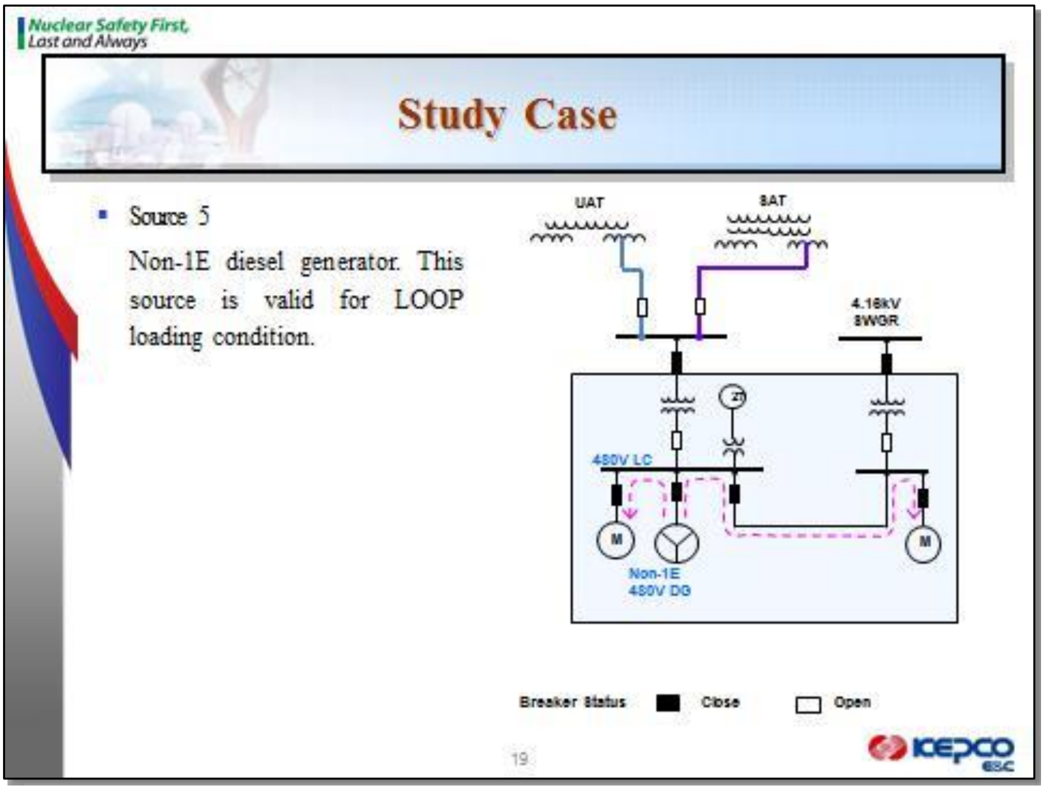
- Source 3

Standby auxiliary transformers connected to offsite power system. This source is valid for LOCA & Hot standby loading conditions.



17 KEPCO E&C


Nuclear Safety First,
Last and Always
Study Case
Source 4
Emergency diesel generator. This source is valid for LOOP loading condition.
LOAD
GRID
SWYD
GIB
GCB
MT
IPB
Div. II
CV cable
Div. II (Same as Div I)
UAT
SAT
Division I
4.16kV EDG
27
13.8kV N1E SWGR
4.16kV Class 1E SWGR
M
Breaker Status
Close
Open
18
KEPCO E&C

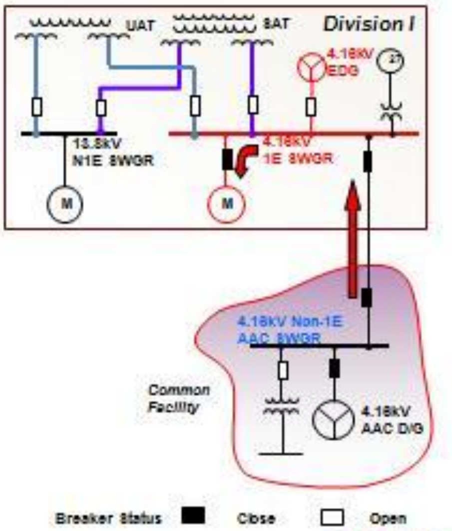

Nuclear Safety First,
Last and Always
Study Case
Source 5
Non-1E diesel generator. This source is valid for LOOP loading condition.
UAT
SAT
4.16kV SWGR
27
480V LC
M
Non-1E 480V DG
Breaker Status
Close
Open
19
KEPCO E&C

Nuclear Safety First, Last and Always

Study Case

- Source 6

AAC diesel generator. This source is valid for SBO loading condition.



KEPCO E&C

Nuclear Safety First, Last and Always

Study Case Table

- Study Case Table

Load Cond. \ Source Cond.	1 (Main Gen)	2 (UAT)	3 (SAT)	4 (1E EDG)	5 (Non-1E D/G)	6 (AAC)
1 (Start-up)		[illegible]				
2 (Normal)	[illegible]					
3 (LOCA)		[illegible]	[illegible]			
4 (Hot Standby)		[illegible]	[illegible]			
6 (Loop)				[illegible]	[illegible]	
7 (SBO)						[illegible]

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Load Flow)

- **Purpose**

  The main purpose of load flow analysis is to simulate the bus voltage profiles, active & reactive power flows between buses as well as losses. The simulation results are used to evaluate the adequacy of plant auxiliary power distribution system design and design parameters for electrical equipment sizing under various study cases.

- **Assumption**
  - The anticipated voltage range at the connection ofNPP should be considered.

    - When reviewing voltage drop, 95% of offsite power voltage rating should be applied.

    - When reviewing over voltage, 105% of offsite power voltage rating should be applied.
  - Maximum measured data is used for transformer impedance.

22

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Load Flow)

- **Modeling and Consideration**

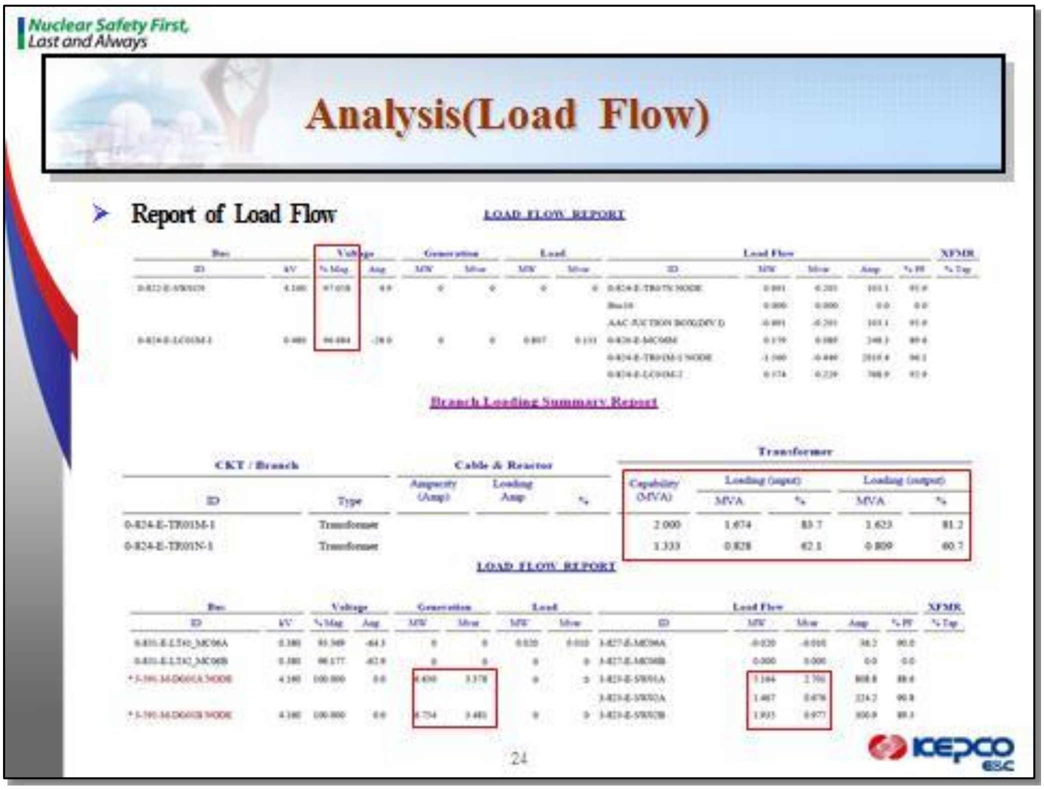
  Almost loads except 120V distribution panel are modeled using load capability. Considering lightest loading and heaviest loading on the auxiliary power system is important. The heaviest loading is generally normal operation (Category 2, Source 1) and LOCA(Category 3, Source 2 or 3). The lightest loading is cold shutdown operation(Category 5, Source 2 or 3).

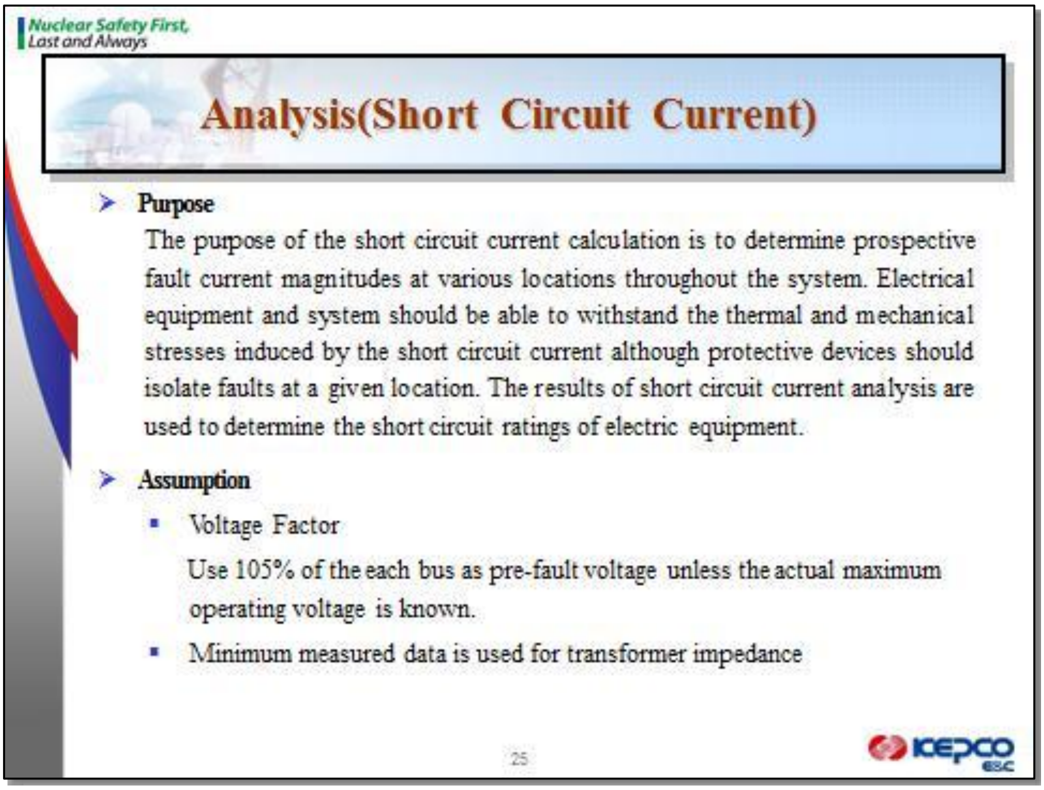
  Loading Diversity Factor applied none.

- **Acceptance Criteria**
  - All distribution bus voltage should maintain 0.9 p.u. to 1.1 p.u. under the minimum and maximum voltage of generator and offsite power.
  - The calculated loading on the transformer and buses should not exceed their capability.
  - The calculated kW and kVAR loading on diesel generator and AAC DG should be within the active and reactive power capability limit.

23

KEPCO E&C


Nuclear Safety First, Last and Always
Analysis(Load Flow)
Report of Load Flow
LOAD FLOW REPORT
Bus
Voltage
Generation
Load
Load Flow
XFMR
ID
kV
% Mag
Ang
MW
Mvar
Amp
% PF
% Tap
Branch Loading Summary Report
CKT / Branch
Cable & Reactor
Transformer
ID
Type
Ampacity (Amp)
Loading Amp
%
Capability (MVA)
Loading (input)
Loading (output)
MVA
%
0-824-E-TR01M-1
Transformer
2.000
1.674
83.7
1.623
81.2
0-824-E-TR01N-1
Transformer
1.333
0.828
62.1
0.809
60.7
LOAD FLOW REPORT
24
KEPCO E&C


Nuclear Safety First, Last and Always
Analysis(Short Circuit Current)
Purpose
The purpose of the short circuit current calculation is to determine prospective fault current magnitudes at various locations throughout the system. Electrical equipment and system should be able to withstand the thermal and mechanical stresses induced by the short circuit current although protective devices should isolate faults at a given location. The results of short circuit current analysis are used to determine the short circuit ratings of electric equipment.
Assumption
Voltage Factor
Use 105% of the each bus as pre-fault voltage unless the actual maximum operating voltage is known.
Minimum measured data is used for transformer impedance
25
KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Short Circuit Current)

- **Modeling**
  - Utility Grid & Generation Modeling

    Utility Grid - 3 Phase short circuit capacity and X/R ratio

    Generation - generator rating, impedances and X/R ratio
  - Motor Modeling

    All medium and low voltage motors are modeled using LRC(Locked Rotor Current) of supplier's technical data.

    Multiplying Factors is calculated in accordance with IEEE Std C37.010 by selecting Std MF in ETAP.
  - Lumped Load Modeling

    Average LRC(Locked Rotor Current) and % total load of Constant KVA.

    Calculating method of Multiplying Factors is the same as induction load by selecting Std MF.

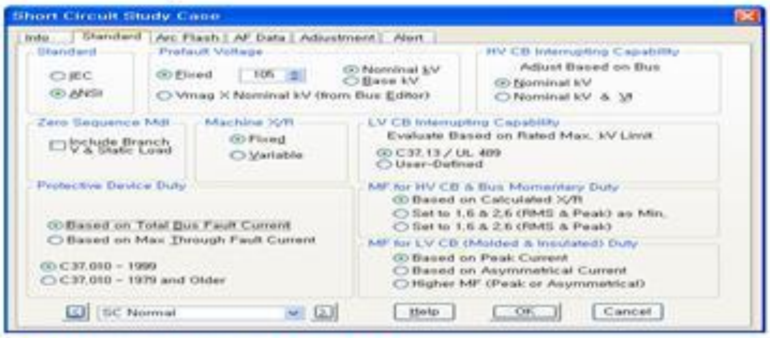
26

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Short Circuit Current)

- **Short Circuit Study Case**



  - Prefault Voltage & Protective Device Duty

    Apply 105% of nominal voltage for the maximum short circuit current calculation. Calculation results are based on 'Total Bus Fault Current' option since this option is to calculate and summate all contribution currents to a fault location for a conservative design.

27

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Short Circuit Current)

- **Short Circuit Study Case**
  - MF for HV CB & Bus Momentary Duty

    With "based on calculated X/R" option selected, the multiplication factors used to compute the asymmetrical and peak duty for high-voltage circuit breakers and high-voltage buses are based on calculated system X/R ratio.
  - MF for LV(Molded & Insulated) Duty

    All LV circuit breakers used in Korean NPPs are classified as the unfused breaker type. So, "Based on Peak Current" option is selected to calculate multiplication factor (MF) based on the peak current, which is the same method used for calculating MF for an unfused low voltage power circuit breaker.
  - Transformer Tap

    "Use Nominal Tap" option is used since minimum transformer impedances are entered without z tolerance. Transformer impedances are not adjusted in case of Nominal Tap option.

28

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Short Circuit Current)

- **Consideration**

  When analysing short circuit current, it's important to assume the most severe case. During normal operation in the power plant, the emergency DG is not synchronized to system. But, when there is synchronization test of the emergency DG, a fault current at this time will be the most severe case. So, Category 2 and Source 1 condition including EDG(Emergency diesel generator) source should be considered to analysis short circuit current as the most severe case.
- **Acceptance Criteria**
  - Calculated short circuit current should not exceed the momentary and interrupting ratings of medium voltage and low voltage circuit breakers.
  - Calculated short circuit current should not exceed the short time current rating of buses.

29

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Short Circuit Current)

➢ **Report of Short Circuit Current**

- HV CB & Bus Duty

3-Phase Fault Currents: (Prefault Voltage = 105 % of the Bus Nominal Voltage)

Bus ID	Bus kV	Device ID	Device Type	Momentary Duty Symm. kA rms	Momentary Duty X/R Ratio	Momentary Duty M.F.	Momentary Duty Asymm. kA rms	Momentary Duty Asymm. kA Peak	Device Capability Symm. kA rms	Device Capability Asymm. kA rms	Device Capability Asymm. kA Peak
1-821-E-SW01M	13.800	21-01M B2	5 cy Sym CB	35.882	22.1	1.583	56.795	94.766		64.000	104.000
	13.800	21-1M C2	5 cy Sym CB	35.882	22.1	1.583	56.795	94.766		64.000	104.000

Bus ID	Bus kV	Device ID	Device Type	Interrupting Duty CPT (Cy)	Interrupting Duty Symm. kA rms	Interrupting Duty X/R Ratio	Interrupting Duty M.F.	Interrupting Duty Adj. Sym. kA rms	Device Capability kV	Device Capability Test PF	Device Capability Rated Int.	Device Capability Adjusted Int.
		21-01M B2	5 cy Sym CB	3.0	30.664	22.8	1.066	32.680	15.000		40.000	40.000
		21-1M C2	5 cy Sym CB	3.0	30.664	22.8	1.066	32.680	15.000		40.000	40.000

30

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Short Circuit Current)

➢ **Report of Short Circuit Current**

- LV CB & Bus Duty

Bus ID	Bus kV	Device ID	Device Type	Momentary Duty Symm. kA rms	Momentary Duty X/R Ratio	Momentary Duty M.F.	Momentary Duty Asymm. kA rms	Momentary Duty Asymm. kA Peak	Device Capability Symm. kA rms	Device Capability Asymm. kA rms	Device Capability Asymm. kA Peak
1-834-E-LC02M	0.480	1-834-E-LC02M	Switchgear	24.699	9.9	1.436	35.473	60.592	50.000	66.500	
1-834-E-LC02N	0.480	1-834-E-LC02N	Switchgear	23.409	10.2	1.443	33.777	57.454	50.000	66.500	

Bus ID	Bus kV	Device ID	Device Type	Interrupting Duty CPT (Cy)	Interrupting Duty Symm. kA rms	Interrupting Duty X/R Ratio	Interrupting Duty M.F.	Interrupting Duty Adj. Sym. kA rms	Device Capability kV	Device Capability Test PF	Device Capability Rated Int.	Device Capability Adjusted Int.
1-834-E-LC02M	0.480	CB30	PowerCutler		24.699	9.9	1.067	26.346	0.480	15.00	50.000	50.000
		CB28	PowerCutler		24.699	9.9	1.067	26.346	0.480	15.00	50.000	50.000
1-834-E-LC02N	0.480	CB120	PowerCutler		23.409	10.2	1.071	25.064	0.480	15.00	50.000	50.000
		CB99	PowerCutler		23.409	10.2	1.071	25.064	0.480	15.00	50.000	50.000

31

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Motor Starting)

➢ **Purpose**

Large induction motors draw six (6) or seven (7) times their full load currents from their power supply under starting conditions, which may last up to several seconds. Motor starting study can guarantee the stable operation of onsite power system by analyzing the voltage drop during the large motor staring.

➢ **Assumption**

- The minimum system voltage should be taken into consideration. It should be assumed to be 95% of system nominal voltage.
- Maximum measured data is used for transformer impedance.

32

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Motor Starting)

➢ **Modeling**

There are two types of motor starting calculations: Dynamic Motor Acceleration and Static motor Starting. Since the purpose of motor starting analysis is to confirm voltage drop, static motor starting method can be used for analysis of motor starting.

➢ **Motor Starting Study Case**

- Transformer LTC

It is assumed OLTC is not operated during starting time. If "For Prestart Load Flow" option is selected, voltage regulation actions reflected only prestart loading conditions.

33

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Motor Starting)

- **Motor Starting Study Case**
  - Starting Load of Accelerating Motors

    "Based on Motor Mechanical load" option is selected for dynamic motor starting method because actual load torque based on rated output is used. In this option the load curve will be applied as it is without any adjustments.
- **Consideration**

  When evaluating the starting of a motor connected in the same bus, we analyze only the effects of starting the largest motor. Logically if the largest motor can start successfully, it is safe to assume that the rest of the motors will successfully start too. Normal (Category 2, Source 1) and start-up(Category 1,Souce 2 or 3) prestart loading category is considered as the prestart loading case.
- **Acceptance Criteria**
  - The minimum required motor terminal voltage for Non-Class 1E motors and the Class 1E motors should not be less than 80% and 75% of motor rated voltage respectively.

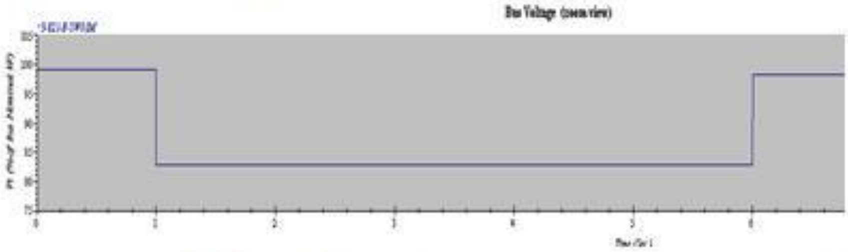
34

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Motor Starting)

- **Report of Motor Starting**



Bus		Voltage		Generation		Load		Load Flow					XFMR
ID	kV	% Mag	Ang	MW	Mvar	MW	Mvar	ID	MW	Mvar	Amp	% PF	% Tap
3-821-E-SW01M	13.800	82.883	6.5	0	0	0	0	3-824-E-TR01M NODE	0.164	0.003	8.3	100.0	

35

KEPCO E&C

Nuclear Safety First, Last and Always

Analysis(Fast Bus Transfer)

- **Purpose**

  For nuclear power plants in Korea, the main purpose of the fast bus transfer is to transfer the aux. loads from one power source to an alternate power source in order to maintain continuous power supply without power interruptions.

- **Assumption**
  - The system voltage angle and pu V/Hz are assumed as zero (0) degree and a 1 p.u. respectively for conservative results for the resultant pu V/Hz.
  - Any faults on the Class 1E motor bus (Switchgear/MCC) shall not initiate the fast bus transfer process.
  - For breaker opening and closing time, the minimum incomer opening time and the maximum alternative incomer closing time should be used for conservative calculations of the worst case out of phase condition.
  - Assume there is a fault on the primary and/or secondary windings of the UAT.

36

KEPCO E&C

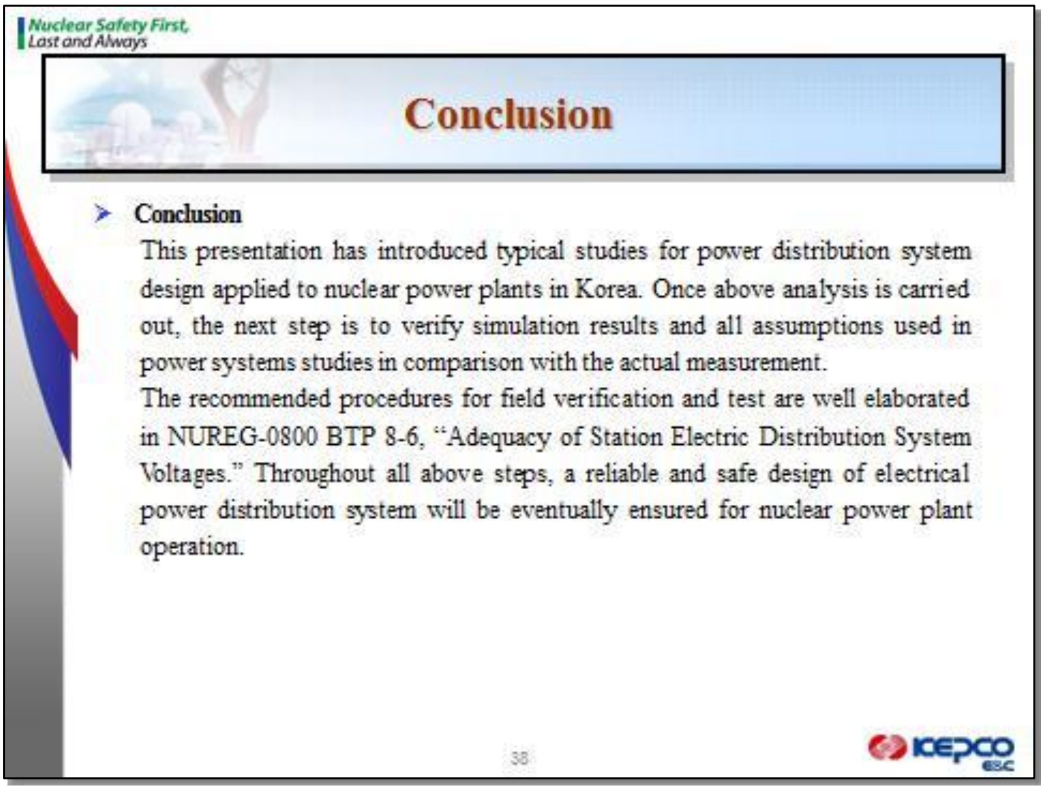
Nuclear Safety First, Last and Always

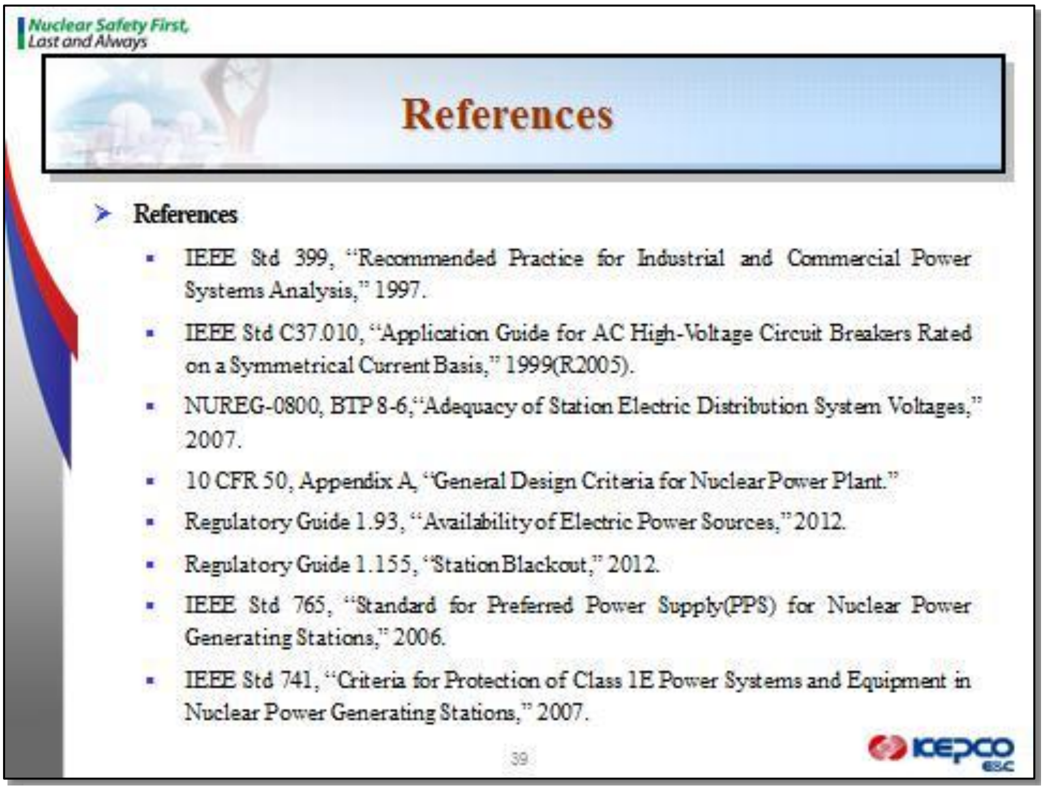
Analysis(Fast Bus Transfer)

- **Modeling and Consideration**
  - All medium voltage motors are individually modelled in equivalent circuit representing stator and rotor windings, and load torque characteristics are modelled in the simulation program.
  - Plant normal operation loading and configuration (Category 2, Source 1) are considered for the fast bus transfer study.
- **Acceptance Criteria**
  - Fast transfer occurs within a time period of 10 cycles or less.
  - The maximum phase angle between the motor residual V/Hz vector and the system equivalent V/Hz vector does not exceed 90 degrees.
  - The resultant V/Hz between the motor residual V/Hz phasor and the incoming source V/Hz phasor at the instant of transfer completion does not exceed 1.33 pu V/Hz.
  - Class 1E motors should be able to re-accelerate to its rated speed.
  - During the fast bus transfer processing, any nuisance operations of protective relaying system should be avoided.

37

KEPCO E&C


Nuclear Safety First,
Last and Always
Conclusion
Conclusion
This presentation has introduced typical studies for power distribution system design applied to nuclear power plants in Korea. Once above analysis is carried out, the next step is to verify simulation results and all assumptions used in power systems studies in comparison with the actual measurement.
The recommended procedures for field verification and test are well elaborated in NUREG-0800 BTP 8-6, "Adequacy of Station Electric Distribution System Voltages." Throughout all above steps, a reliable and safe design of electrical power distribution system will be eventually ensured for nuclear power plant operation.
38


Nuclear Safety First,
Last and Always
References
References
IEEE Std 399, "Recommended Practice for Industrial and Commercial Power Systems Analysis," 1997.
IEEE Std C37.010, "Application Guide for AC High-Voltage Circuit Breakers Rated on a Symmetrical Current Basis," 1999(R2005).
NUREG-0800, BTP 8-6,"Adequacy of Station Electric Distribution System Voltages," 2007.
10 CFR 50, Appendix A, "General Design Criteria for Nuclear Power Plant."
Regulatory Guide 1.93, "Availability of Electric Power Sources," 2012.
Regulatory Guide 1.155, "Station Blackout," 2012.
IEEE Std 765, "Standard for Preferred Power Supply(PPS) for Nuclear Power Generating Stations," 2006.
IEEE Std 741, "Criteria for Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations," 2007.
39


Nuclear Safety First,
Last and Always
Thank you
KEPCO E&C
40
KEPCO E&C

Computer Simulation of Complex Power System Faults under various Operating Conditions

Tanuj Khandelwal
ETAP, USA

Mark Bowman
Tennessee Valley Authority, USA

Abstract

A power system is normally treated as a balanced symmetrical three-phase network. When a fault occurs, the symmetry is normally upset, resulting in unbalanced currents and voltages appearing in the network. For the correct application of protection equipment, it is essential to know the fault current distribution throughout the system and the voltages in different parts of the system due to the fault. There may be situations where protection engineers have to analyze faults that are more complex than simple shunt faults. One type of complex fault is an open phase condition that can result from a fallen conductor or failure of a breaker pole. In the former case, the condition is often accompanied by a fault detectable with normal relaying. In the latter case, the condition may be undetected by standard line relaying. The effect on a generator is dependent on the location of the open phase and the load level. If an open phase occurs between the generator terminals and the high-voltage side of the GSU in the switchyard, and the generator is at full load, damaging negative sequence current can be generated. However, for the same operating condition, an open conductor at the incoming transmission lines located in the switchyard can result in minimal negative sequence current. In 2012, a nuclear power generating station (NPGS) suffered series or open phase fault due to insulator mechanical failure in the 345 kV switchyard. This resulted in both reactor units tripping offline in two separate incidents. Series fault on one of the phases resulted in voltage imbalance that was not detected by the degraded voltage relays. These undervoltage relays did not initiate a start signal to the emergency diesel generators (EDG) because they sensed adequate voltage on the remaining phases exposing a design vulnerability. This paper is intended to help protection engineers calculate complex circuit faults like open phase condition using computer program. The impact of this type of fault will be analyzed and for various system operating conditions and possible mitigation methods will be discussed.

1 . Introduction

Electric power systems are generally designed to server loads in a safe and reliable manner. One of the major considerations in the design of the power system is determination and adequate protection against short circuits. Uncontrolled short circuits can cause serve outages, interruption of vital services, equipment damage, and possible personnel injury. There are four basic sources of short circuit current contribution in an electrical power system:

- Generators
- Synchronous Motors
- Induction Motors
- Electric Utility Systems

Short-circuit programs provide the equipment voltages and fault currents, in the sequence and phase domain, for simple balanced and unbalanced short circuits in the network under study. The results from short circuit programs are used for selecting power system equipment ratings and for setting and coordinating protective relays. Frequently, protection engineers have to analyze faults that are more complex than simple shunt faults. In many cases, they have to analyze simultaneous shunt and/or series faults, study systems with unbalanced network elements, and calculate equivalent impedances required to study the stability of a network during system faults and during single-phase open conditions.

Major advances in short-circuit computations in the last 20 years have resulted in new short-circuit computer programs that handle different fault types and very large networks with very small computation times. However most standard short-circuit programs do not handle most complex faults, such as simultaneous shunt and/or series-faults. Engineers have traditionally resorted to complex hand calculations or to more advanced programs such as the Electromagnetic Transient Program (EMTP) to solve protection problems. Though this approach is acceptable, it requires protection engineers to also have expertise on the dynamics of power systems. In addition, for new engineers attempting to solve complex faults under various operating conditions is an overwhelming task. This paper will include an example analysis of open phase fault on system under various operating conditions and include comparison of results against EMTP. The time savings over EMTP modeling will also be highlighted.

2. Short circuit analysis – sequence networks

The classical short-circuit method models the power system network using the bus impedance matrix, Z_{bus}. The steps required to calculate the short-circuit voltages and currents are as follows:

1. Compute the sequence network bus impedance matrices.
2. Extract the sequence network single-port Thevenin equivalent impedances of the faulted bus, given by the diagonal terms, Z_{ii}, of the respective sequence network Z_{bus} matrices, where *i* is the index of the faulted bus.
3. Use the sequence equivalent networks to compute the sequence fault currents at the faulted bus.
4. Use the computed sequence fault currents as compensating currents to calculate the network post fault voltages and currents.

3. Complex faults

In a poly-phase system, a fault may affect all phases equally which is a "symmetrical fault". If only some phases are affected, the resulting “unsymmetrical fault" becomes more complicated to analyze due to the simplifying assumption of equal current magnitude in all phases being no longer applicable. The analysis of this type of fault is often simplified by using methods such as symmetrical components.

A symmetric or balanced fault affects each of the three phases equally. In transmission systems, symmetrical faults occur infrequently (roughly 5%). In practice, most faults in power systems are unbalanced or unsymmetrical where the three phases are not affected equally. With this in mind, symmetrical faults can be viewed as somewhat of an abstraction; however, as unsymmetrical faults are difficult to analyze, analysis of asymmetric faults is built up from a thorough understanding of symmetric faults.

Common types of asymmetric faults, and their causes:

- **line-to-line -** a short circuit between lines, caused by ionization of air, or when lines come into physical contact, for example due to a broken insulator.
- **line-to-ground -** a short circuit between one line and ground, very often caused by physical contact, for example due to lightning or other storm damage
- **double line-to-ground -** two lines come into contact with the ground (and each other), also commonly due to storm damage.

An asymmetric fault breaks the underlying assumptions used in three-phase power, namely that the load is balanced on all three phases. Further complication is introduced while modeling simultaneous faults such as open phase or series fault in conjunction with a line to ground fault or shunt fault. Consequently, it has been difficult to directly use software tools such as the one-line diagram, where only one phase is considered. This paper describes a computer simulation program used to model, analyze and report such asymmetric or complex faults.

4. Design vulnerability in electric power system

On January 30, 2012, Byron Station, Unit 2, experienced an automatic reactor trip from full power because the reactor protection scheme detected an undervoltage condition on the 6.9-kilovolt (kV) buses that power reactor coolant pumps (RCPs) B and C (two of four RCPs trip initiate a reactor trip). A broken insulator stack of the phase C conductor for the 345-kV power circuit that supplies both station auxiliary transformers (SATs 242-1 and 242-2) caused the undervoltage condition as shown in Fig 2. This insulator stack failure caused the phase C conductor to break off from the power line disconnect switch, resulting in a phase C open circuit and a high impedance ground path. Specifically, the parted phase C connection remained electrically connected on the transformer side, and the loose bus bar conductor end fell to the ground. This ground was a direct result of the broken insulator and not an independent event. The connected loose bus bar provided a path to ground for the transformer high-voltage terminal, but did not result in a detectable ground fault (i.e., neither solid nor impedance) as seen from the source. Since the switchyard (i.e., source side) relaying was electrically isolated from the fault, it did not detect a fault; therefore, it did not operate.

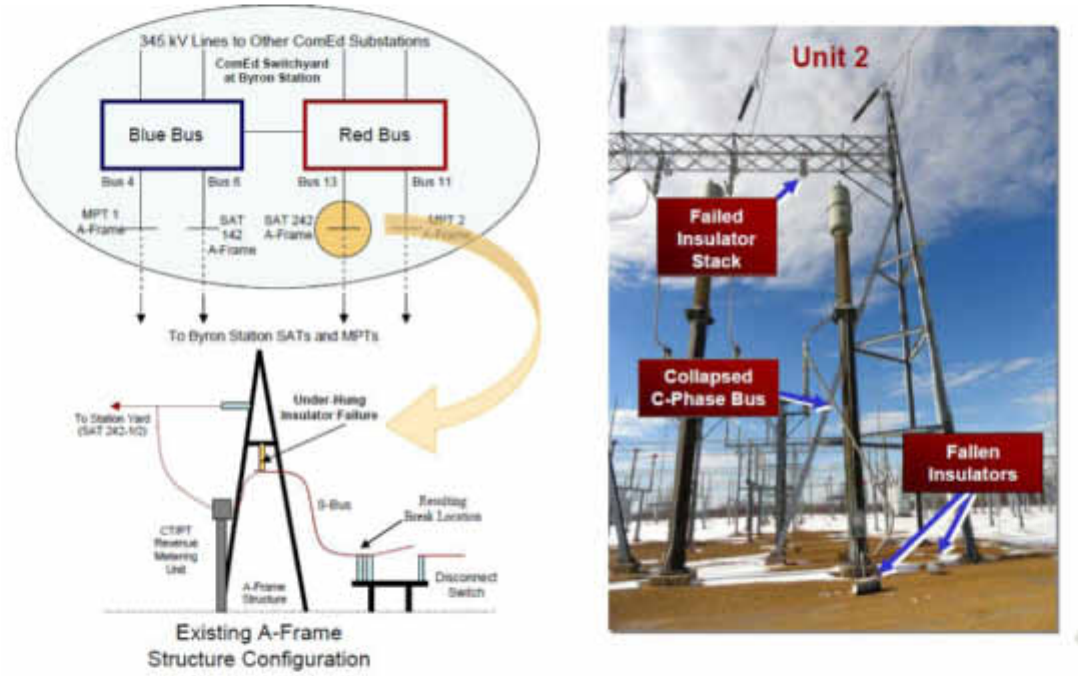


Fig 2. Byron Unit 2 Insulator Failure

After the reactor trip, the two 6.9-kV buses that power RCPs A and D, which were aligned to the unit auxiliary transformers (UATs), automatically transferred to the SATs, as designed.

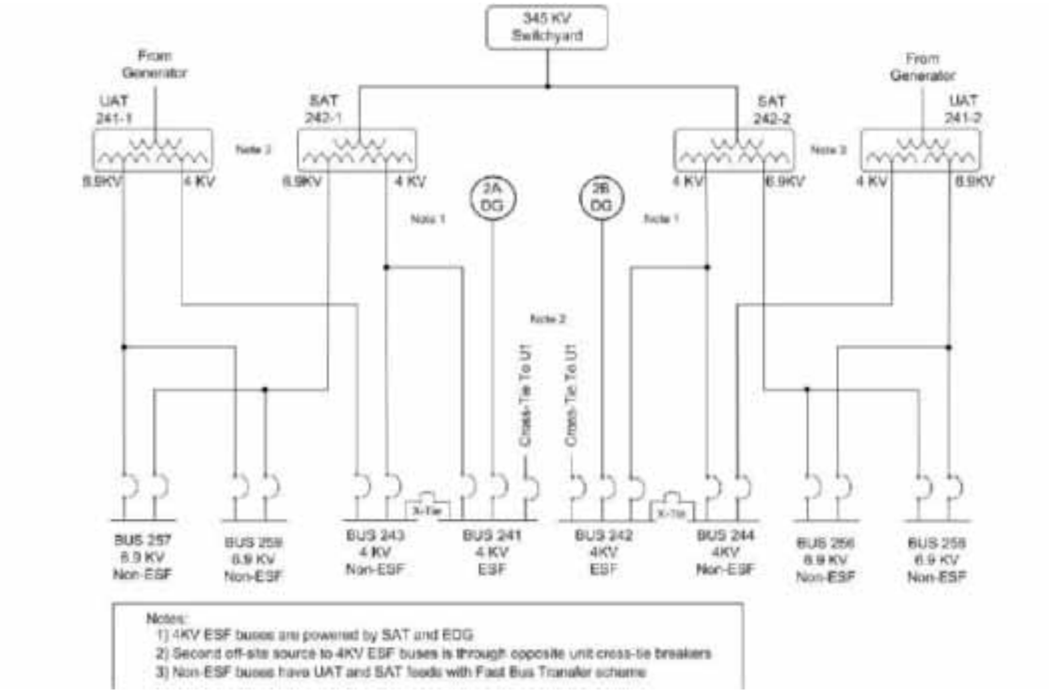


Fig 3. Byron Unit 2 Single Line Diagram

Because phase C was on an open circuit condition, the flow of current on phases A and B increased because of unbalanced voltage and caused all four RCPs to trip on phase overcurrent. Even though phase C was on an open circuit condition, the SATs continued to provide power to the 4.16-kV ESF buses A and B. The open circuit created an unbalanced voltage condition on the two 6.9-kV nonsafety-related RCP buses and the two 4.16-kV 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.

With no RCPs functioning, control room operators performed a natural-circulation cool down of the unit. Approximately 8 minutes after the reactor trip, the control room operators diagnosed the loss of phase C condition and manually tripped breakers to separate the unit buses from the offsite power source. When the operators opened the SAT feeder breakers to the two 4.16-kV ESF buses, the loss of ESF bus voltage caused the emergency diesel generators to start automatically and restore power to the ESF buses.

Byron NPGS reviewed the event and identified design vulnerabilities in the protection scheme for the 4.16-kV ESF buses. The loss of power instrumentation protection scheme is designed with two undervoltage relays on each of the two ESF buses. These relays are part of a two-out-of-two trip logic based on the voltages being monitored between phases A–B and B–C of ESF buses. Even though phase C was on open circuit, the voltage between phases A–B was normal; therefore, the situation did not satisfy the trip logic. Because the conditions of the two-out-of-two trip logic were not met, the protection system generated no protective trip signals to automatically separate the ESF buses from the offsite power source.

A second event occurred at Byron Station Unit 1 on February 28, 2012 (approximately a month apart). This event was also initiated by a failed inverted porcelain insulator. In this event, the 4.16-kV ESF buses did sense fault condition and separated SATs from the 4.16-kV buses. The 1A and 1B DGs started and energized the 4.16-kV ESF buses as designed.

At Byron, a failure to design the electric power system's protection scheme to sense the loss of a single phase between the transmission network and the onsite power distribution system resulted in unbalanced voltage at both ESF buses (degraded offsite power system), trip of several safety-related pieces of equipment such as essential service water pumps, centrifugal charging pumps, and component cooling water pumps and the unavailability of the onsite electric power system. This situation resulted in neither the onsite nor the offsite electric power system being able to perform its intended safety functions (i.e., to provide electric power to the ESF buses with sufficient capacity and capability to permit functioning of structures, systems, and components important to safety).

Since loss of a single phase on the offsite power source can potentially damage both trains of the emergency core cooling system, the protection scheme must automatically initiate isolation of the degraded offsite power source and transfer the safety buses to the emergency power source within the time period assumed in the accident analysis.

The United States Nuclear Regulatory Commission took regulatory actions to require licensees to provide design features to detect and automatically respond to a single-phase open circuit or high impedance fault condition on the high voltage side of a credited offsite circuit. This would ensure that an offsite and an onsite electric power system with adequate capacity and capability will be immediately available to permit the functioning of structures, systems, and components important to safety in the event of anticipated operational occurrences and postulated accidents.

It was determined that evaluations based on the industry guidance are generic assessments cannot be formally credited as a basis for an accurate response.

Hence without formalized engineering calculations the electrical consequences of such an open-phase event, including plant response could not be sufficiently evaluated.

A need for detailed plant-specific models was identified (e.g., transformer magnetic circuit models, electric distribution models, motor models; including positive, negative, and zero sequence impedances, voltage, and currents). Further, the models and calculations were also required to be validated, and analyzed for the plant-specific Class 1E electric distribution system.

5. Open phase fault modeling

INPO Event Reports IER L2-12-14, IER L3-13-13, and NRC Bulletin 2012-01 describe a nuclear safety concern involving an open-phase fault occurring on the offsite power supply of a nuclear plant. This is a previously unanalyzed failure mode for nuclear station offsite power and there has previously been no standard method for analyzing the effects of such faults. An OPF is considered to be an open-phase condition, with or without ground, located on the high-voltage (switchyard) side of each offsite power (OSP) transformer.

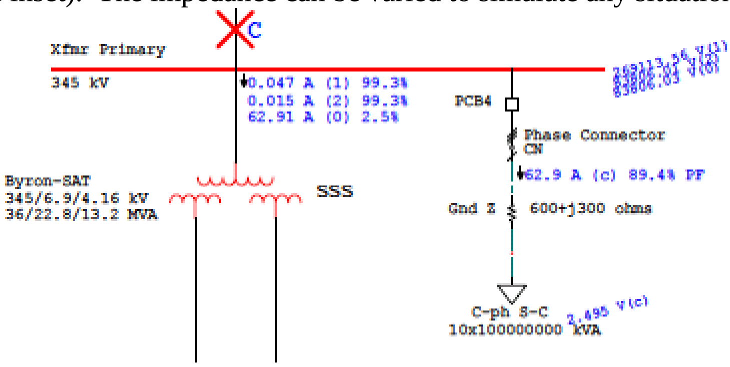
It should be noted that there are two aspects to an open-phase fault analysis: "acceptability" and "detectability". Acceptability involves the ability continue functioning during the open-phase condition without damage and/or spurious operations. Detectability involves the ability of protection systems to detect the open-phase condition. The outcome of OPF analysis is to identify levels of unbalance (voltage and current) during an OPF condition throughout the plant auxiliary power system and determine if existing protective systems will sense the OPF condition. For any cases where the open-phase condition cannot be detected with existing protection systems, this should be identified as a potential vulnerability.

The overall analytical method is a steady-state load flow technique, which of course cannot determine the immediate transient response of the power system to an open-phase fault. However, that is usually not necessary as the steady-state (~30 cycle) voltages and currents (phase and sequence quantities) throughout the plant power system (including at load terminals) can typically be used to properly characterize the potential vulnerabilities to an OPF condition. These results, which are indicative of the system's response to the open-phase condition with all loads remaining in their initial condition (i.e. running or starting) can be compared to a given criteria for either detectability or acceptability. Because it would take an almost unlimited number of simulations to produce "accurate" results for every eventuality (various loading conditions, temperature variations of cable impedance, transformer and machine impedance tolerances, grid voltage variation, grid voltage balance, etc.) bounding techniques can be used to account for the competing conservatisms needed to address these variations and tolerances. In addition, margins can be applied to the results when determining the ability of protective devices to detect the open-phase condition.

The OPF analysis should consider all pertinent plant operating scenarios (events/loading), alignments (configurations), and also the amount of potential voltage unbalance in the incoming plant power supplies (grid unbalance).

6. Example of nuclear plant analytical bases for opf study

- Enter additional transformer data[1] (beyond that typically needed):
  - Zero-Sequence Impedances (%Z and X/R), obtained from zero-sequence short-circuit tests, but for transformer with "buried delta" regulating winding, also need zero-sequence open-circuit tests (e.g. Pri-regulating, Sec-regulating, Pri-Sec)
  - Zero Sequence No Load Losses (%FLA and kW)
- Ensure induction motors have all required data to support the OPF analysis, especially negative-sequence reactance (X2). If exact values are not know, this can be approximated as $X_2 = X_{LR}$.
- The amount of impedance between open phase and ground (transformer side of the open) can be simulated in ETAP by adding a "phase adapter" and a single phase "infinite load" referenced to ground (see inset). The impedance can be varied to simulate any situation from true open to sold ground



- Determine the voltage unbalance at each critical bus by the formula (line-to-line magnitudes):

$$V_{ub} = 100 * \frac{Maximum\ Deviation\ From\ Average}{Average}$$

- Determine the motor on each bus with the worst-case current unbalance (use motor with smallest X_2 which is indicative of the largest I_2) by the formula:

[1] In most cases, actual data must be used or meaningful OPFA is not possible (it cannot be assumed). It is recommended that each transformer model be validated by simulating the factory short-circuit tests in ETAP, both positive and zero sequence, and comparing to the actual test reports.

$I_{ub} = 100 * \frac{I_2}{I_{fl}}$, where I_2 is the negative sequence current and I_{fl} is the motor full load current

- Consider both balanced and unbalanced grid conditions.
- Ensure sufficient study cases are run to bound all combinations of OSP transformers, amount of transformer loading, and amount of open-phase ground impedance. For example:
  - Two offsite power sources
    - Startup/Shutdown Transformer
    - Main Transformer with connected Unit Auxiliary Transformer (consider with and without main generator connected)
  - Three transformer loading scenarios
    - Heaviest (e.g. LOCA loading with any extra plant buses connected)
    - Normal Operation (normal alignment)
    - Lightest (e.g. Refuel loading)
  - Two types of open-phase faults[2]
    - Open
    - Open w/ solid ground
- For detectability, compare the OPF results to existing plant protective device schemes/settings in order to determine if the open-phase condition is adequately detected. This typically involves transformer differential (87T), transformer neutral overcurrent (51N), transmission line negative-sequence, and in-plant bus undervoltage relays. In order to account for various unknowns such as modelling inaccuracy, data inaccuracy, and competing conservatisms (e.g. cable impedance, load diversity, grid voltage level/unbalance) consider application of margins when determining acceptability. Suggested values[3] are:
  - undervoltage detection 10%
  - overcurrent detection 10%
  - differential detection 5%

7. Example results

This table provides an example of an overall summary of the OPF analysis results by identifying areas where detectability is achieved and also highlighting areas of vulnerability.

OPFA Results for Shutdown Transformer XYZ

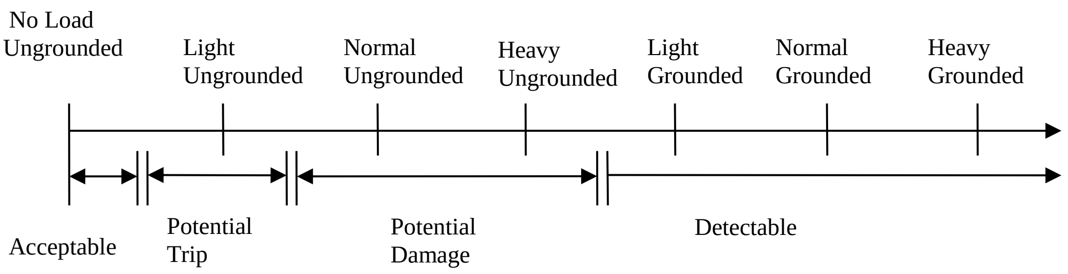
OPF Type	Transformer Loading		
	Light (Refuel)	Normal	Heavy (LOCA)
Grounded	Detectable	Detectable	Detectable
Ungrounded(1)	Not Detectable(2)	Not Detectable(3)	Not Detectable(3)

(1) Bus voltage unbalance within NEMA MG-1 allowable values for transformer 13% or less.
(2) Motor current unbalance indicates potential tripping (motors overcurrent).
(3) Motor current unbalance indicates potential motor damage.

[2] Further study can be done as needed to determine the outcome for other amounts of ground impedance.

[3] the ETAP Nuclear Utility User Group determined that similar analytical techniques with ETAP could simulate transformer factory short-circuit test results (positive and zero-sequence) as well as actual results from the open-phase condition at Byron Station with close correlation (within these margins).

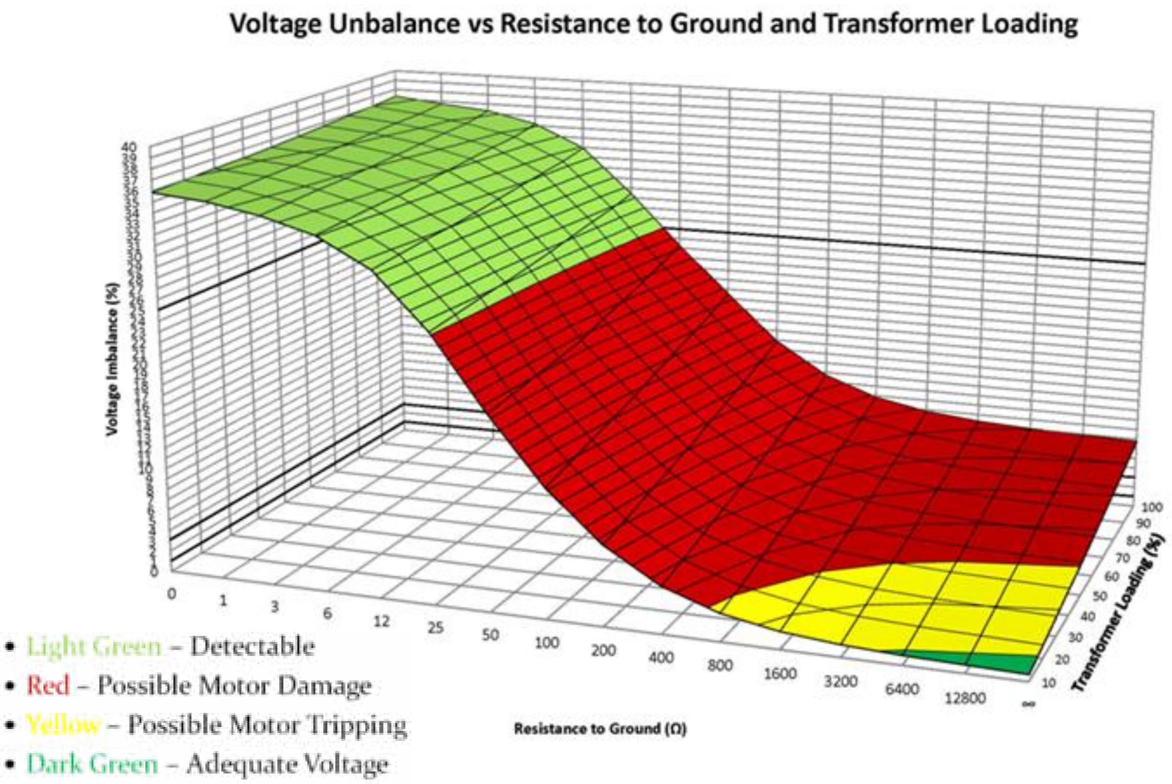
Which can be visually displayed as:



However, this two-dimensional view of limited case studies does not fully characterize the outcome of an OPF on a given transformer. A more complete characterization (i.e. all eventualities for both detectability and acceptability) can be thought of as five "dimensions", which are:

1. Transformer loading (analysis variable)
2. Open-phase grounding (analysis variable)
3. Worst-case bus voltage unbalance (analysis result)
4. Protective device detectability (analysis result)
5. Acceptability of worst-case current unbalance on motor loads (analysis result)

Since ETAP allows quick and efficient simulation of the analysis variables and relatively easy evaluation of the results, multiple OPF simulations can be performed for the analysis variables (transformer loading and open-phase grounding) to allow plotting these five dimensions in sufficient detail to fully characterize the OPF analysis (see example).



8. Comparison of ETAP VS EMTP

Detailed modeling required for open phase fault simulation is possible in EMTP however it is impractical to do so due to a number of reasons:

1. Open phase fault like any other fault has a transient and stead-state component. The transient component only lasts a few cycles as compared to the steady state fault current. It is not necessary to include these transients in the calculation since the protective relaying settings will be based on steady state values in order to avoid nuisance tripping.
2. EMTP requires considerable amount of time to model a complete power electrical system with accurate operating load conditions to fully understand the impact of current and voltage changes in an open phase condition.
3. Most of the electrical systems from HV to LV have already been modeled in ETAP and minimal data entry is need in order to expand the model to perform open phase fault simulation.

	Operating Mode	Offsite Power Xfmr Type	Xfmr Loading	Open-Phase Fault Type	%Unbalance Acceptable? [1]	Detectable by Voltage? [2]	Detectable by Current? [3]
A	Normal	CSST YΔYY (TVA)	Loaded 97%	Open	No • < 10% (Vbus) • 30% (Mtr I2)	No	Yes 87 / 51N
B	Normal	CSST YΔYY (TVA)	Loaded 97%	Open with Ground	No • 35% (Vbus) • 120% (Mtr I2)	Yes (2s < 70%)	Yes 51 / 87 / 51N
C	Refueling	CSST YΔYY (TVA)	Loaded 25%	Open	No • ~3% (Vbus) • > 12% (Mtr I2)	No	Yes 87
D	Refueling	CSST YΔYY (TVA)	Loaded 25%	Open with Ground	No • 45% (Vbus) • 170% (Mtr I2)	Yes (2s < 70%)	Yes 51 / 87 / 51N
E	LOCA	CSST YΔYY (TVA)	Loaded 97%	Open	No • < 10% (Vbus) • 30% (Mtr I2)	No	Yes 87 / 51N
F	LOCA	CSST YΔYY (TVA)	Loaded 97%	Open with Ground	No • 35% (Vbus) • 115% (Mtr I2)	Yes (2s < 70%)	Yes 87 / 51N

[1] Acceptable is < 3% voltage imbalance and also < 12% motor negative sequence current
[2] Using conventional undervoltage protection schemes (with sensing on all phases)
[3] Using conventional overcurrent protection schemes: 51 = Xfmr Over[illegible], 51N = Xfmr Neutral Overcurrent (>= 3% grid imbalance value)
[4] ETAP results match actual event data (SAT primary current)

EMTP analysis was carried out for one of the facilities using simpliocation of the electrical system as shown in Fig 4. The following simplified test system was dervied from one of the nuclear generation facilities and was modeled in EMTP. This particular system took months of simplication and data entry in order to perform transient caluclations of the open phase condition. The cost for performing such calculations was over hundreds of thousands of dollars. However, as shown, all MV motors were simplified into lumped motor model. This is not accureate since open phase fault calculations is affected by motor and transformer models as well as the operating load of the system.

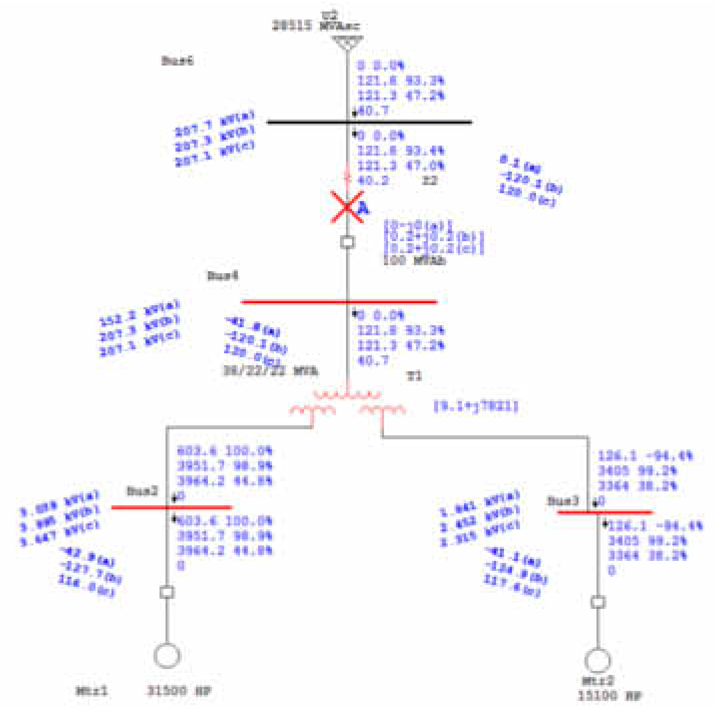


Fig 4. Test System created in EMTP and duplicated in ETAP

It was evident that the entire plant simulation was necessary in order to determine the voltages and currents with high degree of accuracy. Hence the same test system was created in ETAP software once again depicted in Fig 4. The motor circuit parameters were updated in the ETAP model with correct negative sequence impedances and initial loading as shown in Fig 5.

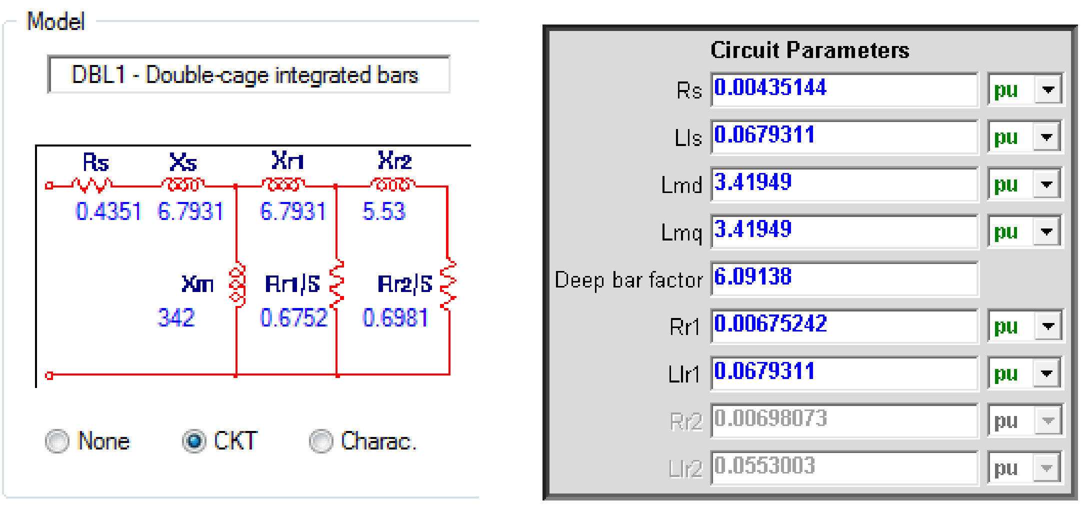


Fig 5. Machine parameters in ETAP and EMTP

The software simulation was performed in ETAP using Mtr1 at 100% load and the motor terminal line-neutral voltages and currents were compared as shown in Fig 6 and Fig 7 below.

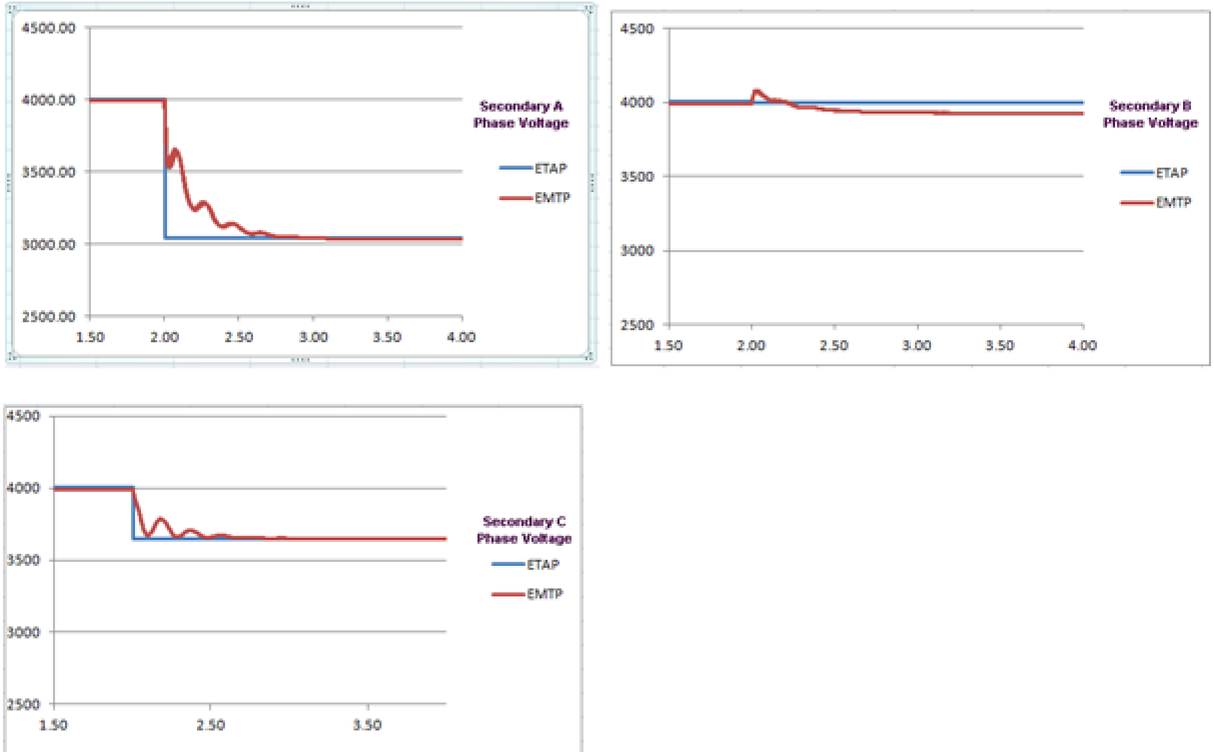


Fig 6. Mtr1 (100% loading) terminal L-N voltages

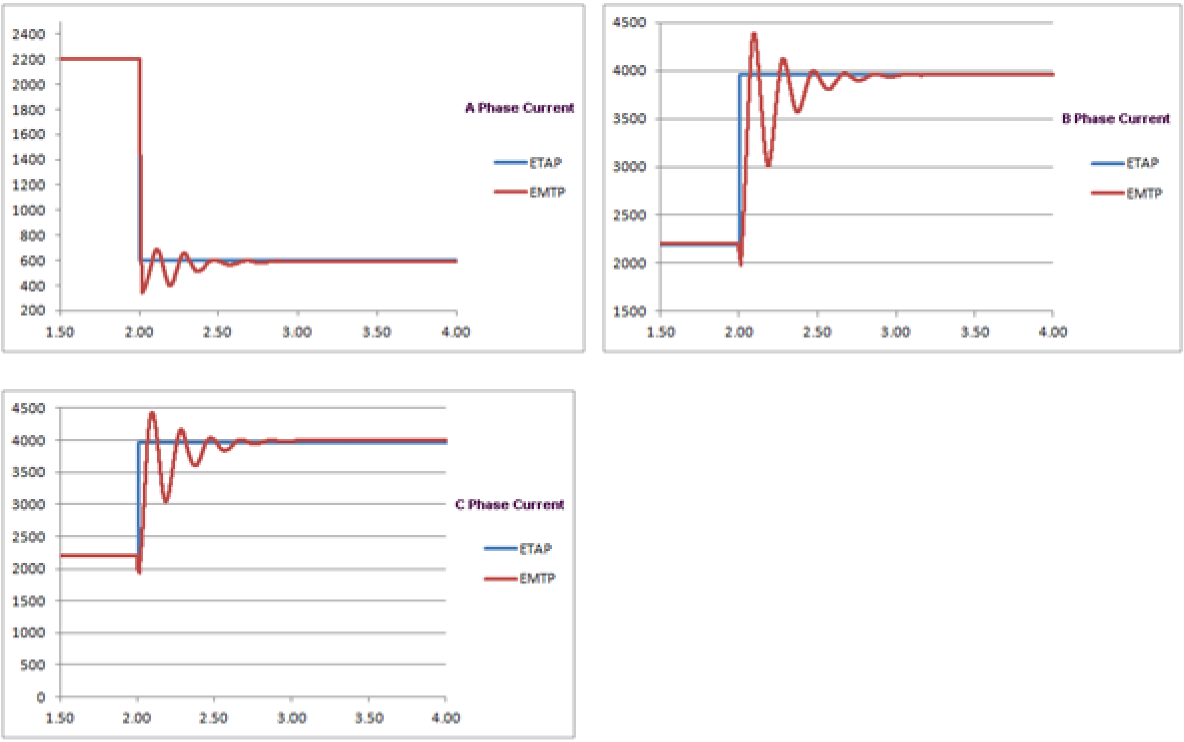


Fig 7. Mtr1 (100% loading) current

From Fig 6 and 7 it can be see that ETAP simulation is a steady state simulation as compared to EMTP however for determining protection relaying, the transients have to be neglected since they only last for a few cycles. The steady state values from both calculation programs that were used to set the protection relays were identical.

Several other comparison tests were conducted into those with Mtr1 at 50% loading to understand the impact of open phase condition under lightly loaded system. Fig 8 is the comparison of ETAP simulation results versus response from EMTP program.

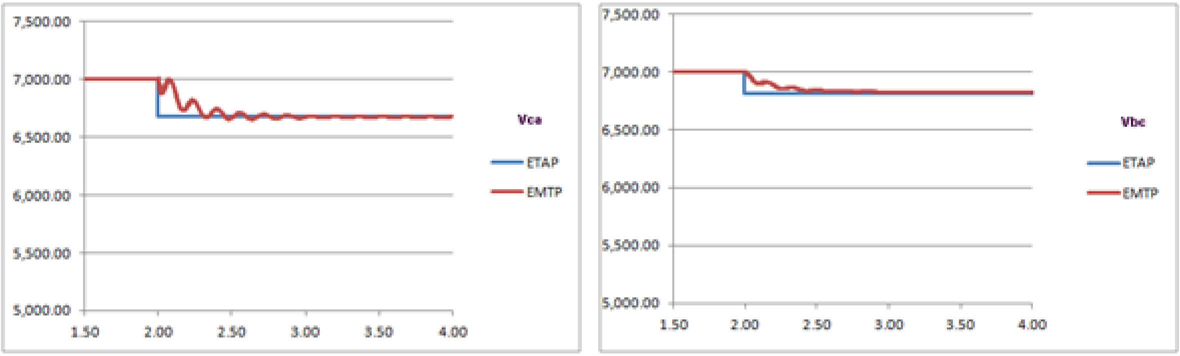


Fig 8. Mtr1 (50% loading) terminal L-N voltages

9. Computer simulation software requirements

1. **Graphical Placement of the Open-Phase on the One-Line Diagram** – Power system simulation software should allow user to easily place open-phase faults (phase A, B, or C) at any terminal of the three-phase branches, including two-winding and three-winding transformers, cables, transmission lines, impedances, and reactors.
2. **Induction Motor Modeling** – The modeling of induction motors should be capable of handling severe unbalanced system conditions caused by an open-phase fault, including the effects of negative-sequence current.
3. **Transformer Type** - The capability to model various types of transformers, including Shell and Core with 3, 4, and 5 limbs, for both 2-winding and 3-winding transformers should be available.
4. **Transformer Magnetization Coupling** - Based on the no-load data, the magnetizing impedance for positive, negative, and zero sequence couplings should be calculated and taken into account.
5. **Transformer Embedded Winding** - The effects of an embedded (buried) winding, for two and three winding transformers should be included.
6. **Report Current Flows inside Transformer Embedded Winding** - The zero-sequence current circulating inside the embedded delta–connected winding should be calculated and reported.
7. **Ground Impedance** - Simulate open-phase faults with any ground type and with specific values of ground impedance.

10 Findings

Leading to the development of the software module and, as part of the verification and validation (V&V) process, numerous studies and benchmarks were created to simulate open-phase conditions in various networks, including the off-site power supply system of a nuclear power plant. V&V test cases have been created to simulate electrical network behavior with different models and under various operating conditions. The following is a summary of findings:

1. Under low loading, certain transformer configurations, and depending on the amount of impedance between the open transformer phase and ground, detection of an open-phase condition on the primary side of a transformer can be difficult on the secondary side.
2. In some cases, detection of the fault in not possible by monitoring the phase currents and voltages. Under voltage relay schemes are not always able to detect a single open phase.
3. Depending on the location of the relays/monitoring devices, the effects of motor back-emf and voltage drop across cables can be significant for detection.
4. Better accuracy of simulation results is obtained with an actual detailed system model rather than a simplified model.
5. Motor and transformer modeling changes are essential. These expanded models are currently unavailable in other software tools and are essential for obtaining accurate results.
6. The user of the tool must understand that the accuracy of the open phase fault simulation is directly affected by the unavailable, incorrect or incomplete transformer data.

11 Conclusions

In the event of a broken conductor, series or open phase fault, the load currents cannot be neglected, as these are the only currents that are flowing in the network and expanded models are needed for motors and transformers in order to accurately simulate the effect of open phase fault on bus voltages and sequence currents. Without accurate steady state values, it will not be possible to set undervoltage and negative sequence relays properly. The developed software has been validated to perform qualitative analysis of plant response to open phase fault event and provide steady state sequence current and voltages throughout the model. The software was shown to accurately simulate transformer factory impedance tests (positive and zero-sequence short circuit tests) as well as actual open-phase “events”. The software has also been enhanced to calculation asymmetric faults such as LL, LG, LLG on unbalanced systems. Further development is in progress to simulate simultaneous fault such as combination of series and shunt fault.

etap

Computer Analysis of Complex Faults in Power Systems

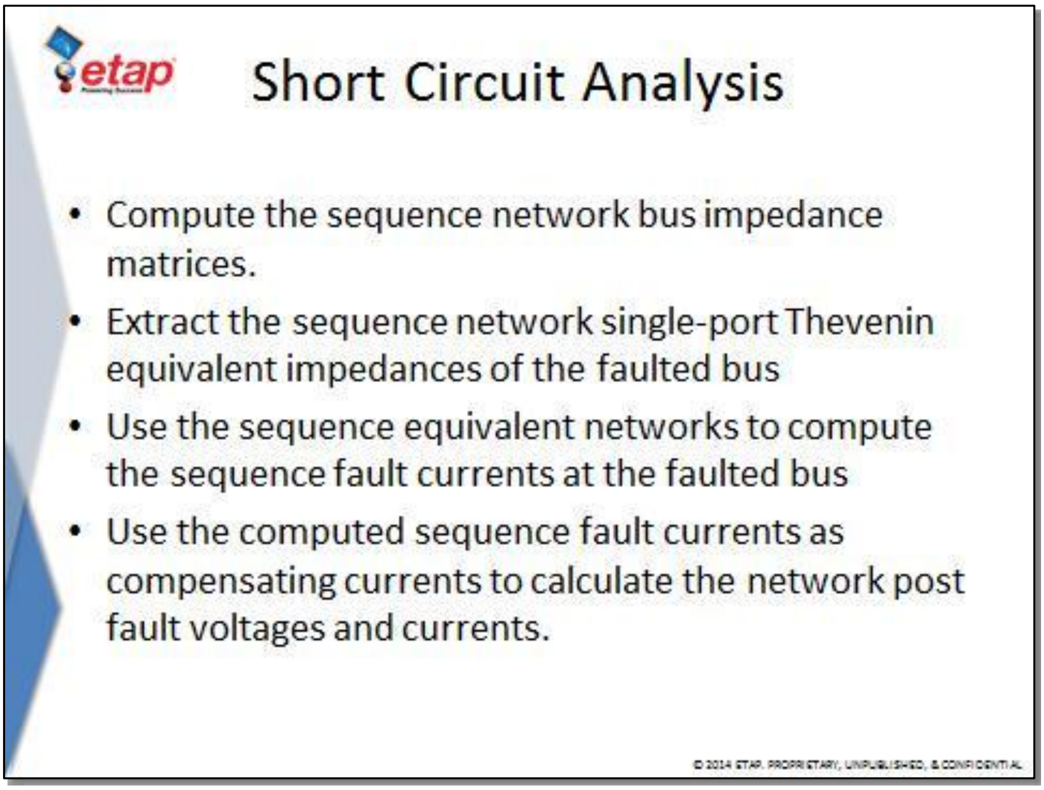
Tanuj Khandelwal
Chief Product Officer
ETAP

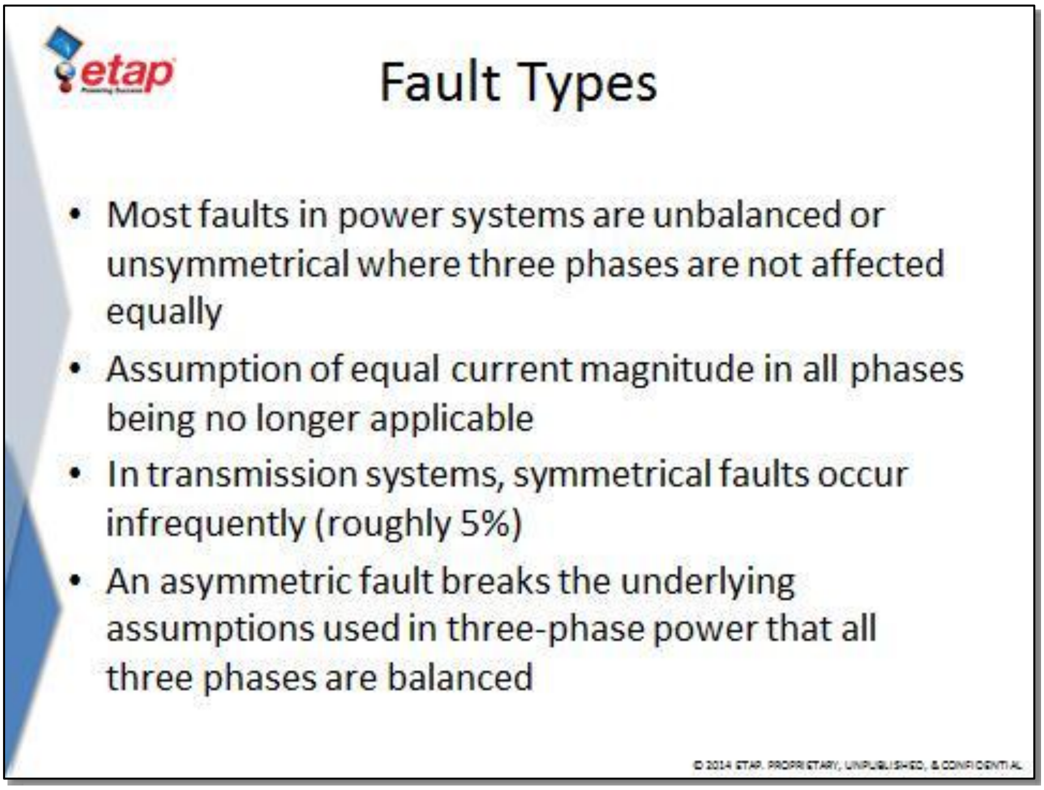
Mark Bowman
TVA, Sr. Program Mgr - Power System Analysis
ETAP NUUG Technical Chair

etap

Introduction

- A power system is normally treated as a balanced symmetrical three-phase network
- During a fault the symmetry is upset, resulting in unbalanced currents and voltages
- Complex faults include open phase condition
- Open phase may be undetected by standard line relaying
- Damaging negative sequence current can be generated for fault at generator terminals


etap
Short Circuit Analysis
• Compute the sequence network bus impedance matrices.
• Extract the sequence network single-port Thevenin equivalent impedances of the faulted bus
• Use the sequence equivalent networks to compute the sequence fault currents at the faulted bus
• Use the computed sequence fault currents as compensating currents to calculate the network post fault voltages and currents.
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

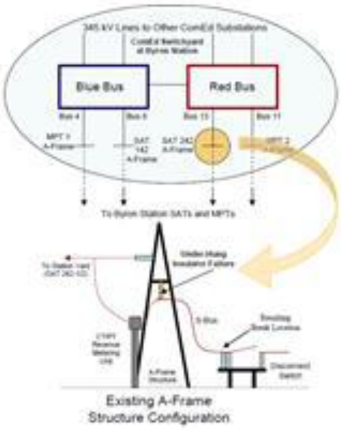

etap
Fault Types
• Most faults in power systems are unbalanced or unsymmetrical where three phases are not affected equally
• Assumption of equal current magnitude in all phases being no longer applicable
• In transmission systems, symmetrical faults occur infrequently (roughly 5%)
• An asymmetric fault breaks the underlying assumptions used in three-phase power that all three phases are balanced
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

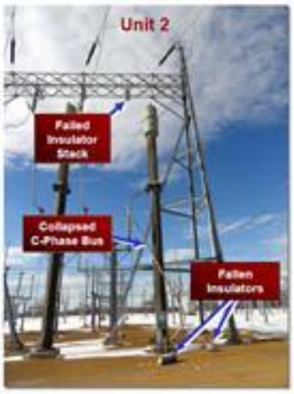
Fault Types

- **line-to-line** - a short circuit between lines, caused by ionization of air, or when lines come into physical contact, for example due to a broken insulator.
- **line-to-ground** - a short circuit between one line and ground, very often caused by physical contact, for example due to lightning or other storm damage
- **double line-to-ground** - two lines come into contact with the ground (and each other), also commonly due to storm damage.

Open Phase – Event 1

- On January 30, 2012, Byron Station, Unit 2, experienced an automatic reactor trip





Design Vulnerability

- A 345-kV phase C insulator stack failed mechanically
- Resulted in a phase C open circuit and a high impedance ground path
- Transformer HV terminal had a ground path, but did not result in a detectable ground fault
- Since the switchyard (i.e., source side) relaying was electrically isolated from the fault, it did not detect a fault; therefore, it did not operate
- Flow of current on phases A and B increased because of unbalanced voltage

Design Vulnerability

- Caused all four Reactor Coolant Pumps (RCPs) to trip on phase overcurrent
- Control room operators performed a natural-circulation cool down of the unit
- Approximately 8 minutes after the reactor trip, the control room operators diagnosed the loss of phase C condition
- Operators manually tripped breakers to separate the unit buses from the offsite power source
- Byron NPGS reviewed the event and identified design vulnerabilities in the protection scheme

Open Phase – Event 2

- A second event occurred at Byron Station Unit 1 on February 28, 2012 (approximately a month apart)
- In this event, the 4.16-kV ESF buses did sense fault condition
- Loss of a single phase on the offsite power source can potentially damage both trains of the emergency core cooling system
- Protection scheme must automatically initiate isolation of the degraded offsite power source and transfer the safety buses to the emergency power source

Event Impact

- The United States Nuclear Regulatory Commission took regulatory actions to require licensees to provide design features to detect and automatically respond to a single-phase open circuit or high impedance fault condition on the high voltage side of a credited offsite circuit
- A need for detailed plant-specific models was identified (e.g., transformer magnetic circuit models, electric distribution models, motor models; including positive, negative, and zero sequence impedances, voltage, and currents)

etap

Open Phase Fault (OPF)

- INPO Event Reports IER L2-12-14, IER L3-13-13, and NRC Bulletin 2012-01 describe a nuclear safety concern involving an open-phase fault occurring on the offsite power supply of a nuclear plant
- An OPF is considered to be an open-phase condition, with or without ground, located on the high-voltage (switchyard) side of each offsite power (OSP) transformer

etap

Open Phase Fault (OPF)

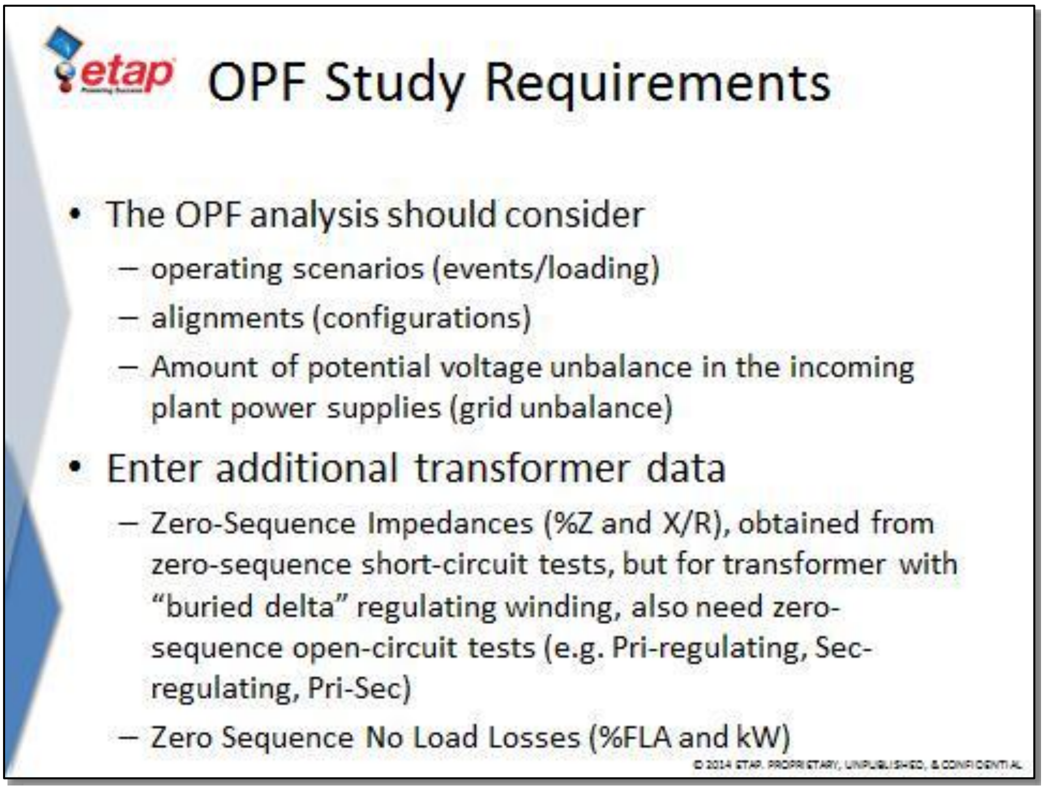
- Two aspects to an open-phase fault analysis:
  – Acceptability
  – Detectability
- Acceptability involves the ability continue functioning during the open-phase condition without damage and/or spurious operations
- Detectability involves the ability of protection systems to detect the open-phase condition

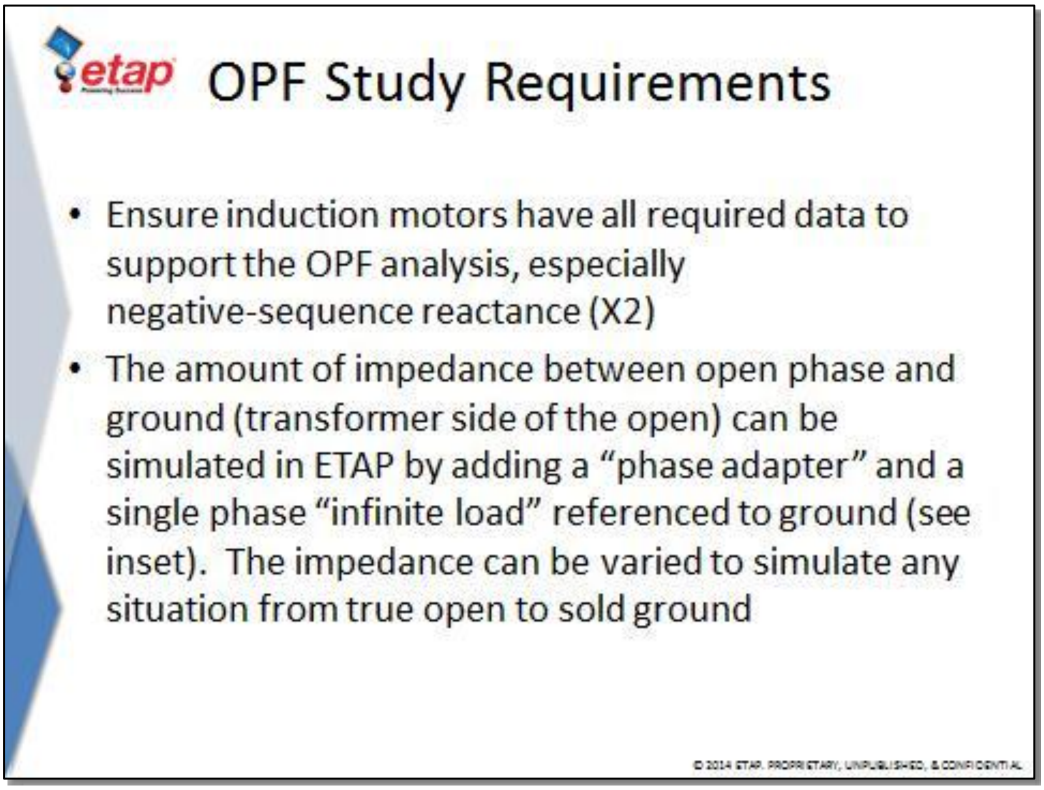
OPF Study Objective

- Outcome of OPF analysis is to identify levels of unbalance (voltage and current) throughout the plant auxiliary power system
- Determine if existing protective systems will sense the OPF condition
- For any cases where the open-phase condition cannot be detected with existing protection systems, this should be identified as a potential vulnerability

OPF Study

- Overall analytical method is a steady-state load flow technique
- Cannot determine the immediate transient response of the power system to an open-phase fault
- Usually not necessary as the steady-state (~30 cycle) voltages and currents (phase and sequence quantities) throughout the plant power system (including at load terminals) can typically be used to properly characterize the potential vulnerabilities to an OPF condition


etap
OPF Study Requirements
• The OPF analysis should consider
– operating scenarios (events/loading)
– alignments (configurations)
– Amount of potential voltage unbalance in the incoming plant power supplies (grid unbalance)
• Enter additional transformer data
– Zero-Sequence Impedances (%Z and X/R), obtained from zero-sequence short-circuit tests, but for transformer with “buried delta” regulating winding, also need zero-sequence open-circuit tests (e.g. Pri-regulating, Sec-regulating, Pri-Sec)
– Zero Sequence No Load Losses (%FLA and kW)
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

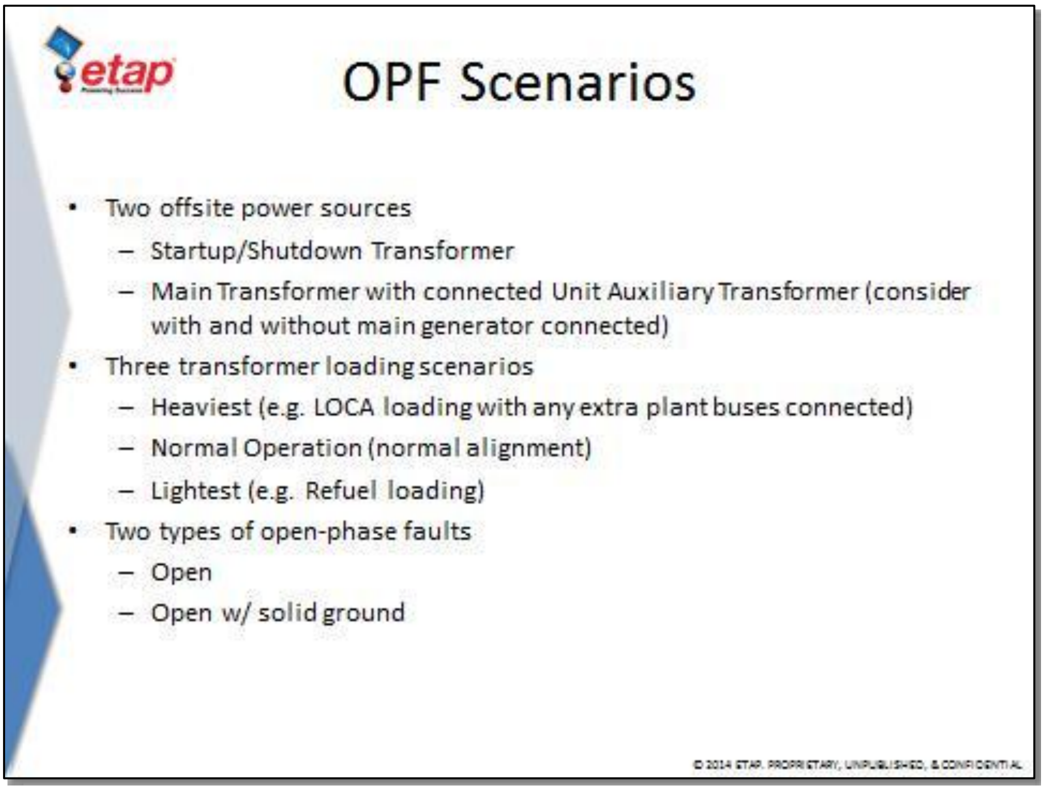

etap
OPF Study Requirements
• Ensure induction motors have all required data to support the OPF analysis, especially negative-sequence reactance (X2)
• The amount of impedance between open phase and ground (transformer side of the open) can be simulated in ETAP by adding a “phase adapter” and a single phase “infinite load” referenced to ground (see inset). The impedance can be varied to simulate any situation from true open to sold ground
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

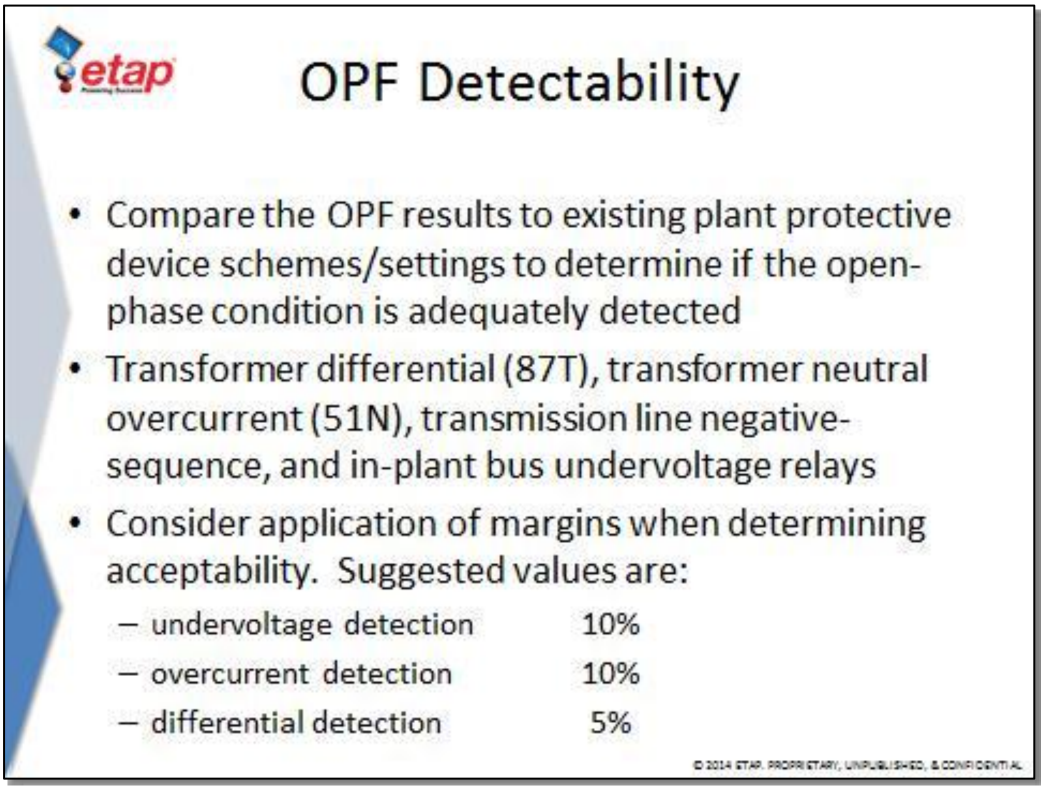
Computer Simulation Software Requirements

- Graphical Placement of the Open-Phase on the One Line Diagram
- Induction motor modeling.
- Transformer type.
- Transformer Embedded winding
- Report current flow inside Transformer Embedded winding
- Ground Impedance

OPF Analysis Steps

- Determine the voltage unbalance at each critical bus
- Determine the motor on each bus with the worst-case current unbalance
- Consider both balanced and unbalanced grid conditions
- Ensure sufficient study cases are run to bound all combinations of OSP transformers, amount of transformer loading, and amount of open-phase ground impedance


etap
OPF Scenarios
• Two offsite power sources
– Startup/Shutdown Transformer
– Main Transformer with connected Unit Auxiliary Transformer (consider with and without main generator connected)
• Three transformer loading scenarios
– Heaviest (e.g. LOCA loading with any extra plant buses connected)
– Normal Operation (normal alignment)
– Lightest (e.g. Refuel loading)
• Two types of open-phase faults
– Open
– Open w/ solid ground

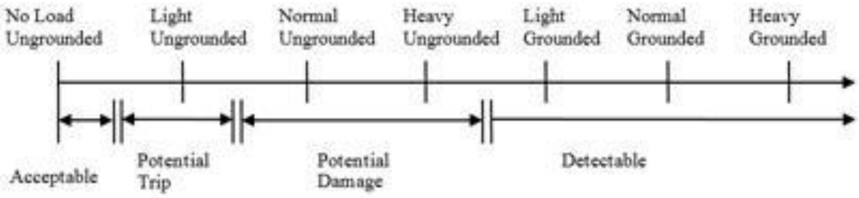

etap
OPF Detectability
• Compare the OPF results to existing plant protective device schemes/settings to determine if the open-phase condition is adequately detected
• Transformer differential (87T), transformer neutral overcurrent (51N), transmission line negative-sequence, and in-plant bus undervoltage relays
• Consider application of margins when determining acceptability. Suggested values are:
– undervoltage detection 10%
– overcurrent detection 10%
– differential detection 5%

etap

OPF Results

OPFA Results for Shutdown Transformer XYZ

OPF Type	**Transformer Loading**		
	Light (Refuel)	**Normal**	**Heavy (LOCA)**
Grounded	Detectable	Detectable	Detectable
Ungrounded(1)	Not Detectable(2)	Not Detectable(3)	Not Detectable(3)



etap

OPF Results

- 2D view of limited case studies does not fully characterize outcome of an OPF on a given transformer
- Complete characterization (i.e. all eventualities for both detectability and acceptability) can be thought of as five “dimensions”, which are:
  - Transformer loading (analysis variable)
  - Open-phase grounding (analysis variable)
  - Worst-case bus voltage unbalance (analysis result)
  - Protective device detectability (analysis result)
  - Acceptability of worst-case current unbalance on motor loads (analysis result)

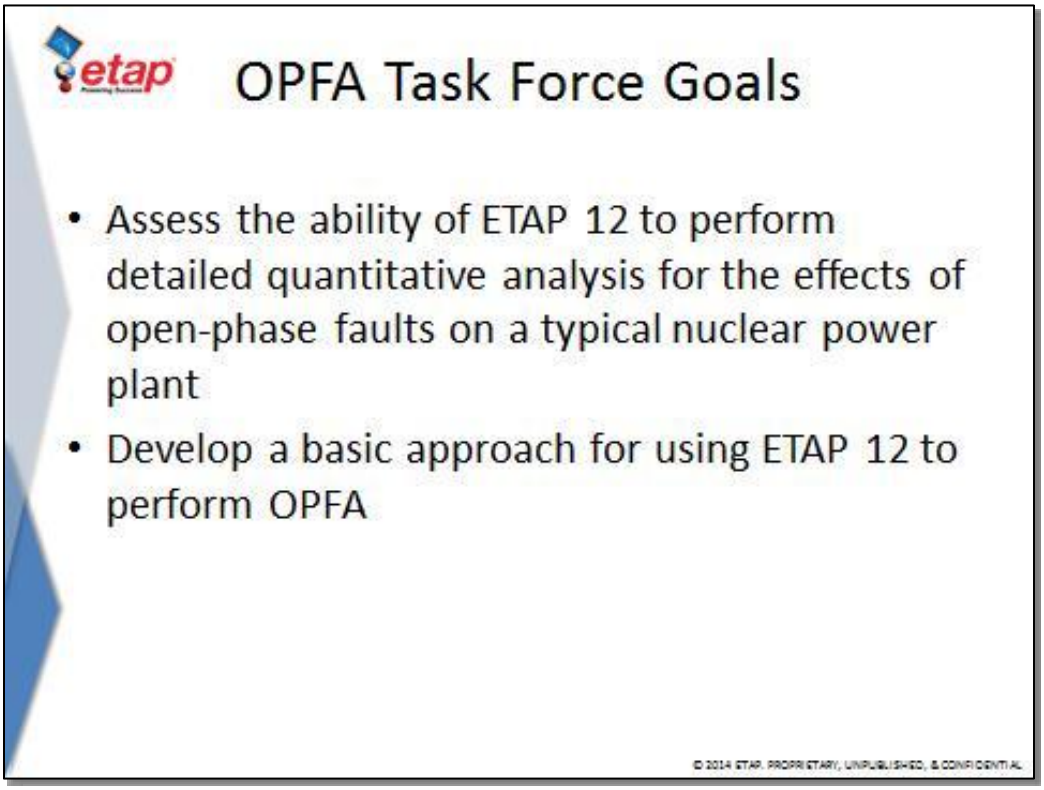
Why ETAP?

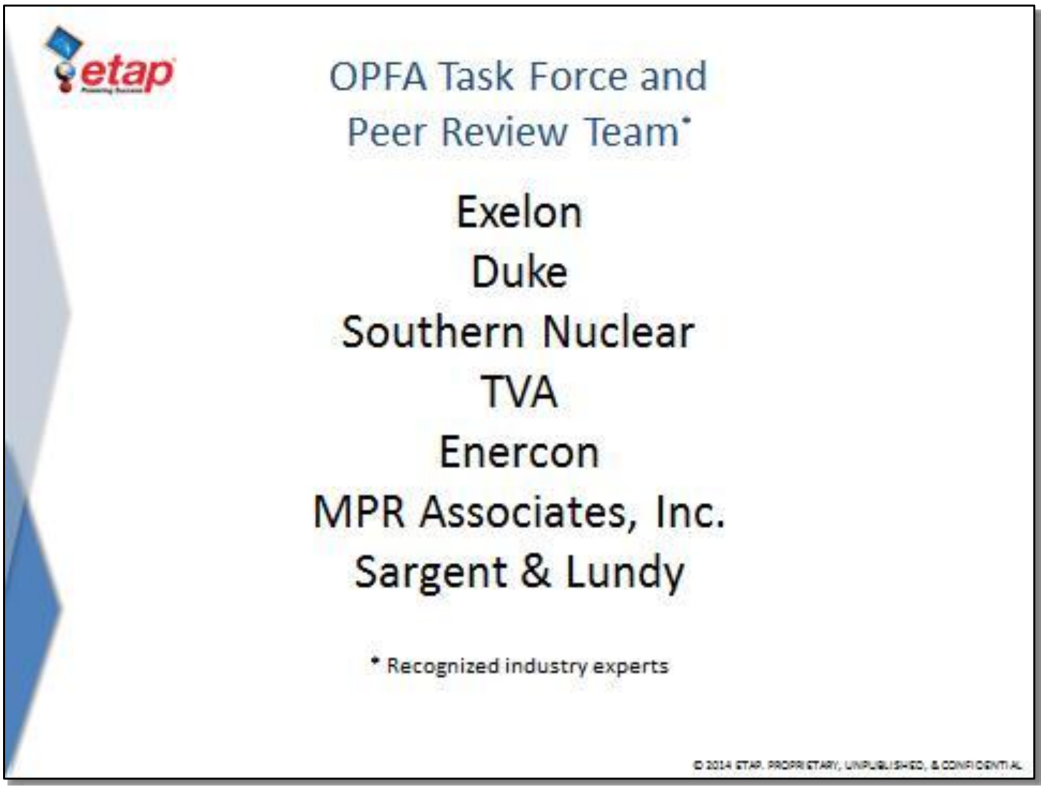
ETAP is the most commonly used analysis software in US nuclear plants and has established itself as the de facto standard: **60 out of 64 operating plants (94%) have standardized on ETAP.**

ETAP Nuclear is used throughout the world by nuclear plants, research laboratories, consulting firms, government agencies, and other organizations.

ETAP NUUG

- ETAP NUUG began review of ETAP's ability to perform OPFA shortly after the Byron open-phase event in early 2012
- May 2012: ETAP developer (OTI) issued Informative Report INFR-12-003 to identify limitations and future enhancements related to OPFA
- February 2013: Revised version of ETAP issued to better simulate open-phase faults
- March 2013: ETAP NUUG formed OPFA Task Force


etap
OPFA Task Force Goals
• Assess the ability of ETAP 12 to perform detailed quantitative analysis for the effects of open-phase faults on a typical nuclear power plant
• Develop a basic approach for using ETAP 12 to perform OPFA
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL


etap
OPFA Task Force and Peer Review Team*
Exelon
Duke
Southern Nuclear
TVA
Enercon
MPR Associates, Inc.
Sargent & Lundy
* Recognized industry experts
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

OPFA Task Force Effort

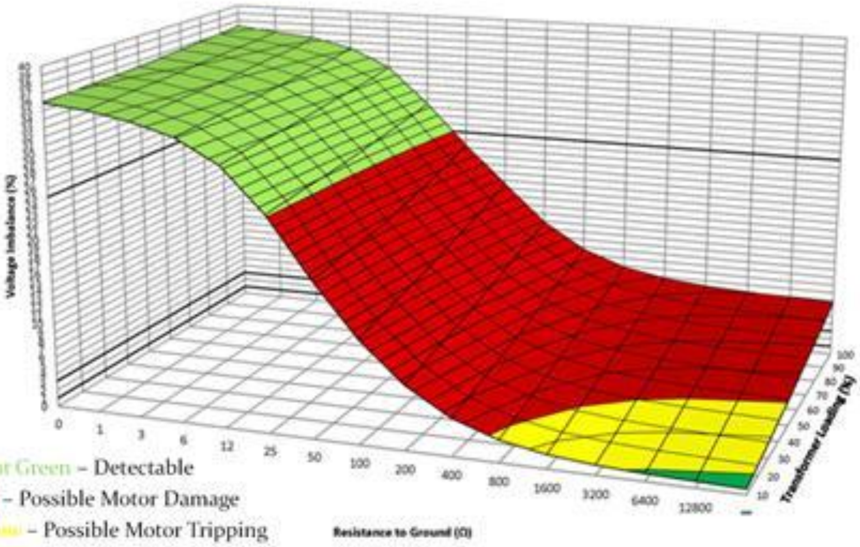
- 3 month effort (March thru May 2013)
- Performed "mock" OPFA using existing ETAP models
  - Reviewed additional data entry needed
  - Considered broad spectrum of plant types, offsite power configurations, transformer types, and operating conditions
  - Developed basic approach for modeling open-phase faults (open, open w/ gnd, open w/ hi-Z gnd)
- Reviewed available results related to OPFA
  - Voltage and current results: "L-L", "L-N", and "sequences"
  - Xfmr neutral and buried delta results
- Format developed to evaluate the "mock" results

ETAP Simulation

- ETAP allows quick and efficient simulation of the analysis variables and relatively easy evaluation of the results
- Multiple OPF simulations can be performed for the analysis variables (transformer loading and open-phase grounding) to allow plotting these five dimensions in sufficient detail to fully characterize the OPF analysis

ETAP Simulation

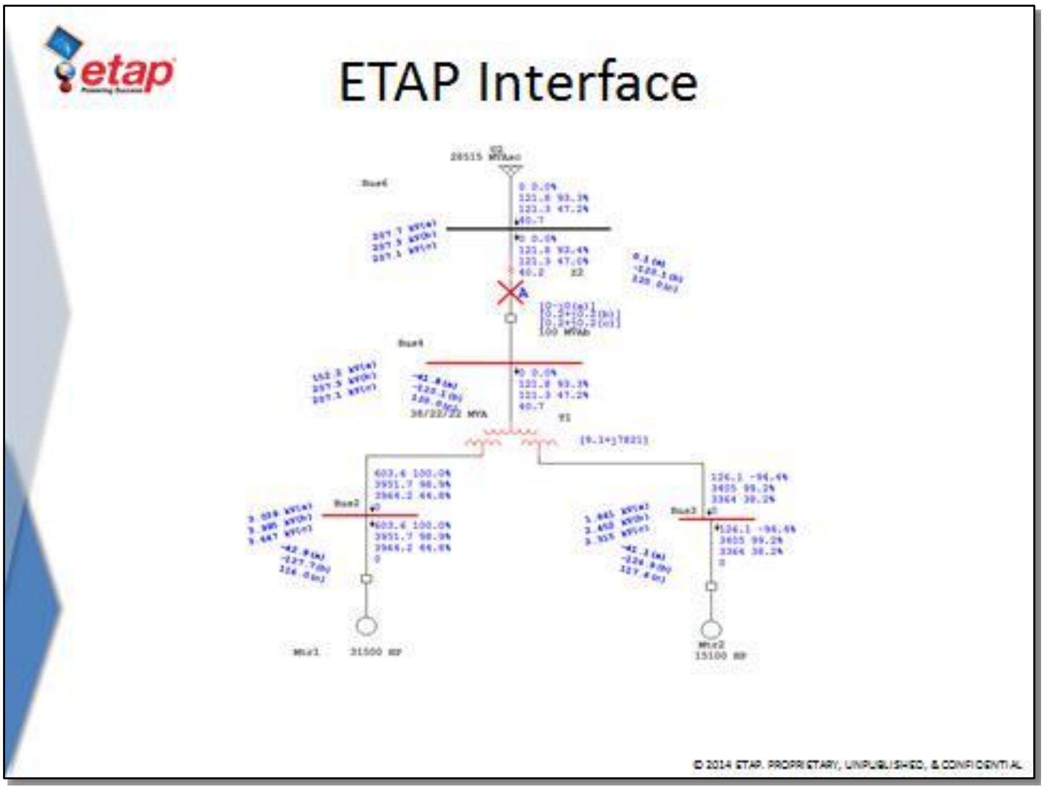
Voltage Unbalance vs Resistance to Ground and Transformer Loading

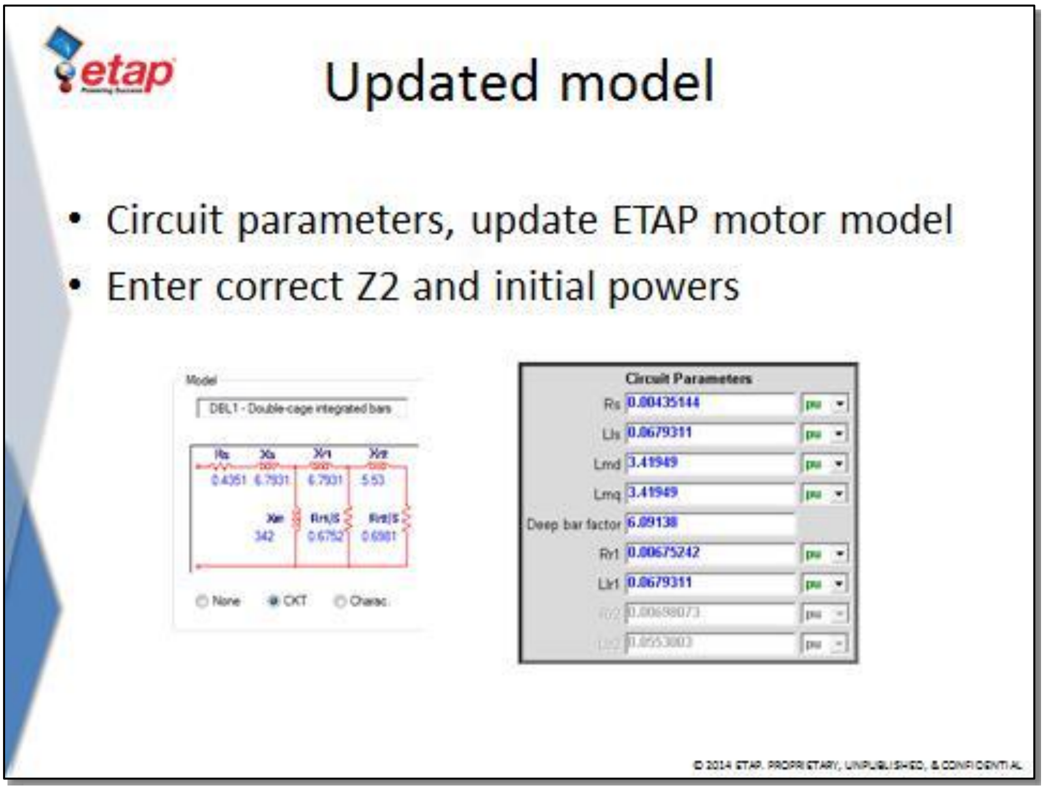


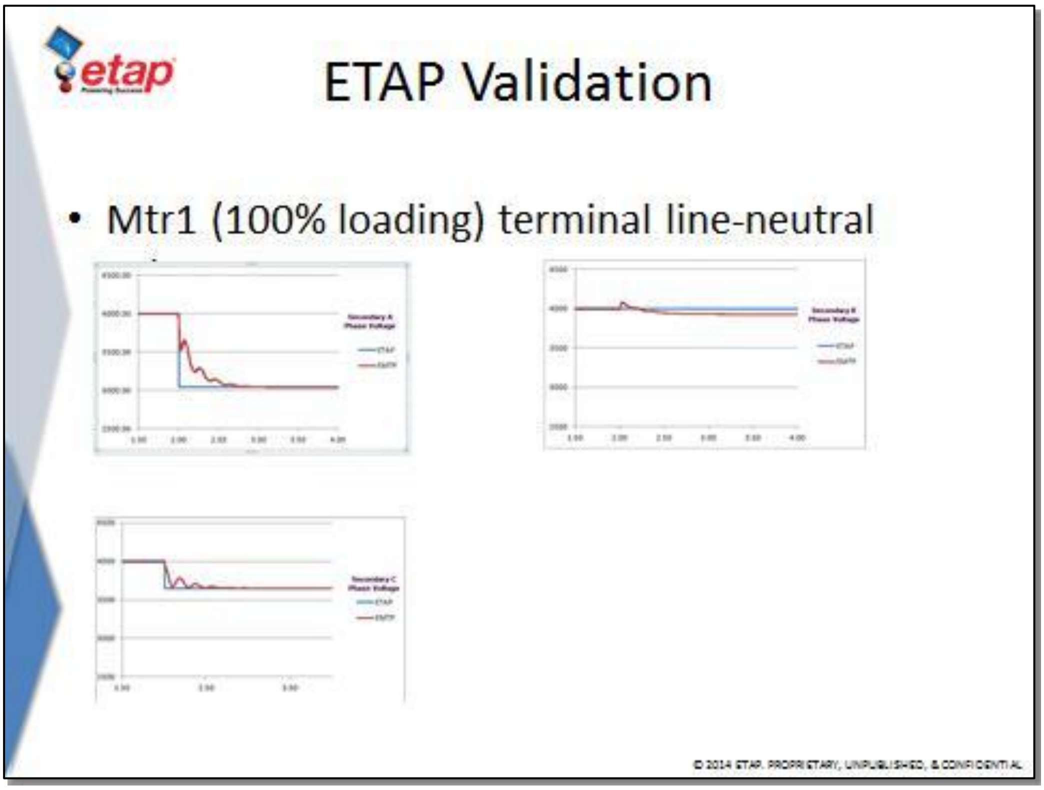
- Light Green – Detectable
- Red – Possible Motor Damage
- Yellow – Possible Motor Tripping
- Dark Green – Adequate Voltage

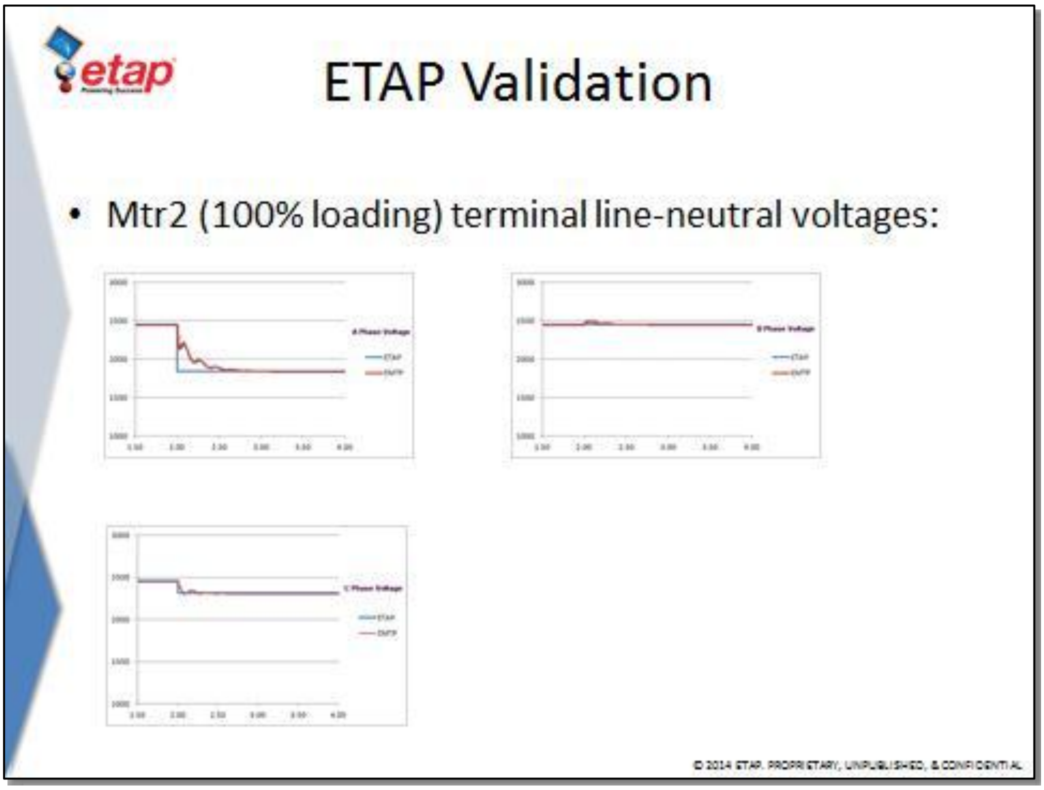
ETAP Utilization

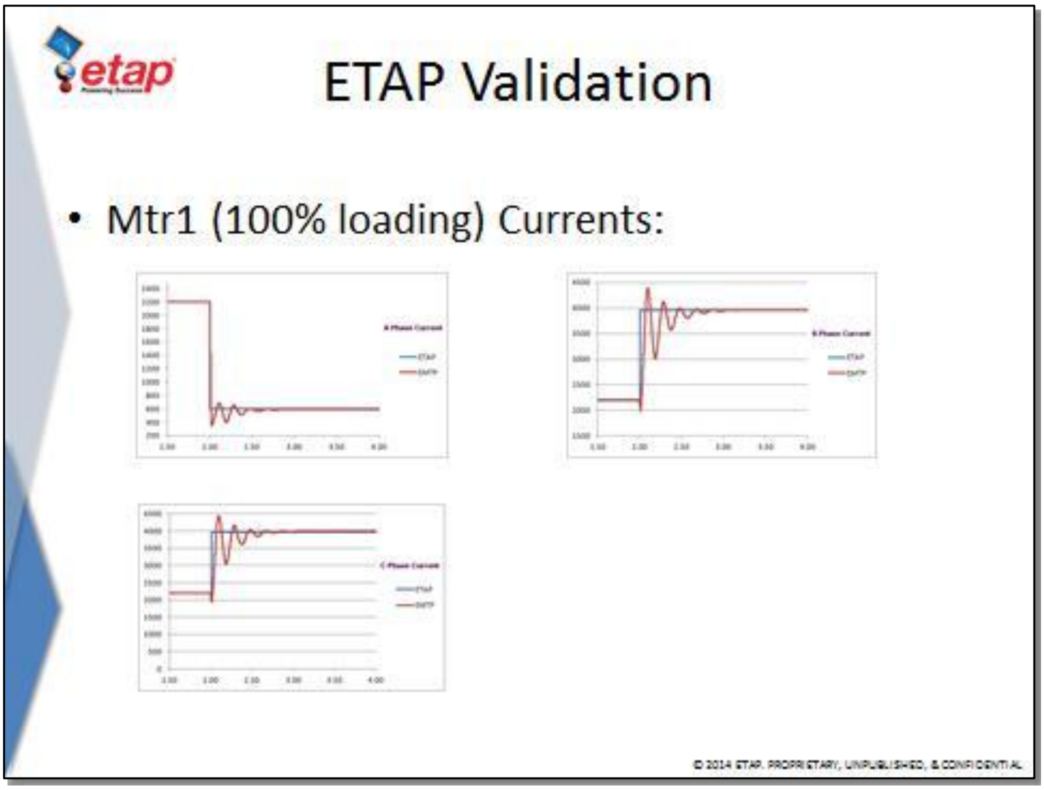
- Detailed modeling required for open phase fault simulation is possible in EMTP however it is impractical and not required:
  - Protective relaying settings will be based on steady state values in order to avoid nuisance tripping
  - EMTP requires considerable amount of time to model a complete power electrical system
  - Most of the electrical systems from HV to LV have already been modeled in ETAP and minimal data entry is need in order to expand the model to perform open phase fault simulation

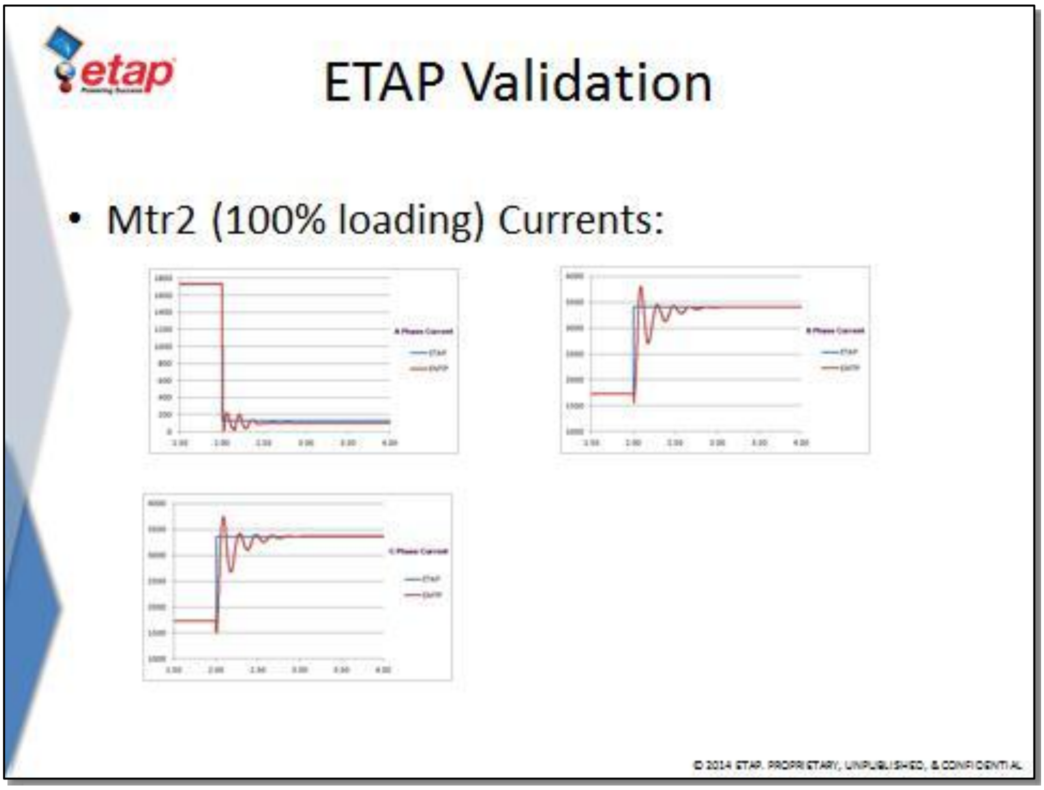

etap
ETAP Interface
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

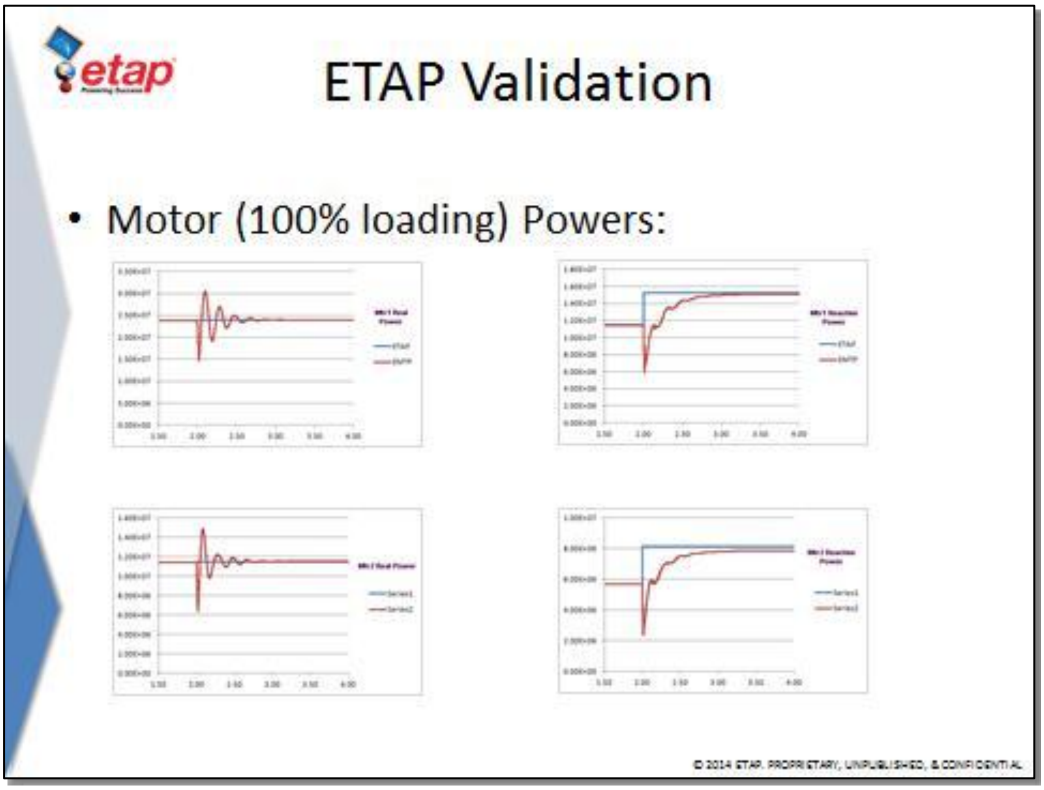

etap
Updated model
• Circuit parameters, update ETAP motor model
• Enter correct Z2 and initial powers
Model
DBL1 - Double-cage integrated bars
None
CKT
Charac.
Circuit Parameters
Rs 0.00435144 pu
Lls 0.0679311 pu
Lmd 3.41949 pu
Lmq 3.41949 pu
Deep bar factor 6.09138
Rr1 0.00675242 pu
Llr1 0.0679311 pu
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

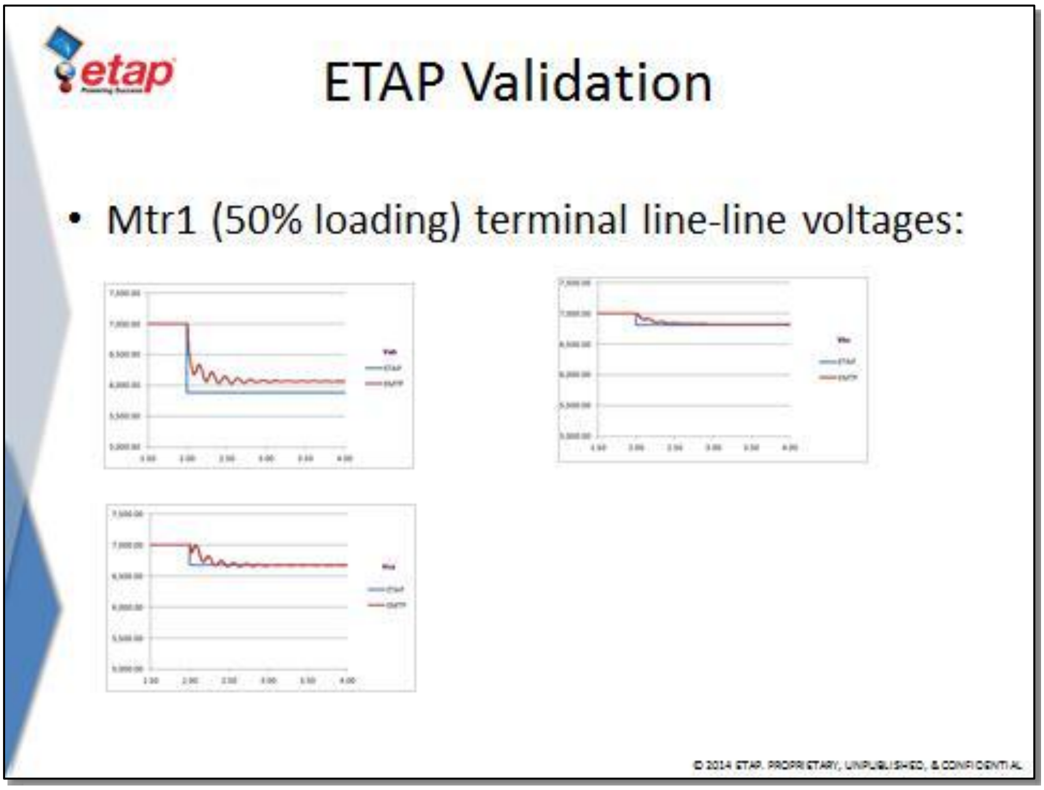

etap
ETAP Validation
• Mtr1 (100% loading) terminal line-neutral
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL


etap
ETAP Validation
• Mtr2 (100% loading) terminal line-neutral voltages:
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL


etap
ETAP Validation
• Mtr1 (100% loading) Currents:
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

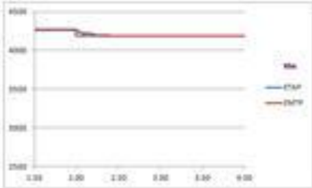

etap
ETAP Validation
• Mtr2 (100% loading) Currents:
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL


etap
ETAP Validation
• Motor (100% loading) Powers:
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL


etap
ETAP Validation
• Mtr1 (50% loading) terminal line-line voltages:
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

ETAP Validation

- Mtr2 (50% loading) terminal line-line voltages:



OPFA Task Force Results

- ETAP 12 is validated to perform OPFA (steady-state)
- Minimal additional data entry needed for OPFA (beyond a typical ETAP plant model)
- ETAP 12 can simulate open-phase faults with specific values of ground Z
- ETAP 12 was shown to accurately simulate Xfmr factory impedance tests (positive and zero-sequence short-circuit tests) as well as actual open-phase "events"
- Issues / Limitations
  - Unavailable/incorrect/incomplete Xfmr data
  - Not intended for dynamic/transient analysis

Summary of Findings

- Under low loading, certain transformer configurations, and depending on the amount of impedance between the open transformer phase and ground, detection of an open-phase condition on the primary side of a transformer can be difficult on the secondary side
- In some cases, detection of the fault in not possible by monitoring the phase currents and voltages. Under voltage relay schemes are not always able to detect a single open phase

Summary of Findings

- Depending on the location of the relays/monitoring devices, the effects of motor back-emf and voltage drop across cables can be significant for detection
- Better accuracy of simulation results is obtained with an actual detailed system model rather than a simplified model

© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

Summary of Findings

- Motor and transformer modeling changes are essential. These expanded models are currently unavailable in other software tools and are essential for obtaining accurate results.
- The user of the tool must understand that the accuracy of the open phase fault simulation is directly affected by the unavailable, incorrect or incomplete transformer data.

Conclusion

- ETAP 12 is a validated analysis software package that is now available to allow current nuclear users to quickly move toward performing a qualitative analysis of their plant's response to an open-phase fault
- ETAP 12.6 includes double phase open fault simulation capability
- ETAP 14 includes simulation of simultaneous complex faults


etap
Questions
Thank you
© 2014 ETAP. PROPRIETARY, UNPUBLISHED, & CONFIDENTIAL

SESSION FIVE

"Requirements for Equipment Used for Emergency Response"

Design Provisions for Station Blackout at Nuclear Power Plants
Alexander Duchac (IAEA)

Timing Critiria for Supplemental BWR 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 (CNSC, Canada)

Fundamental Design Bases for Independent Core Cooling in Swedish Nuclear Power Reactors
Thomas Jelinek (SSM, Sweden)

Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
Xavier Hubert Rene Guisez (Electrabel, Belgium)

Design Provisions for Station Blackout at Nuclear Power Plants

Alexander Duchac
IAEA, Vienna, Austria

Abstract

A station blackout (SBO) is generally known as "a plant condition with complete loss of all alternating current (AC) power from off-site sources, from the main generator and from standby AC power sources important to safety to the essential and nonessential switchgear buses. Direct current (DC) power supplies and uninterruptible AC power supplies may be available as long as batteries can supply the loads. Alternate AC power supplies are available".

A draft Safety Guide DS 430 "Design of Electrical Power Systems for Nuclear Power Plants[4]" provides recommendations regarding the implementation of Specific Safety Requirements[5]: Design: Requirement 68 for emergency power systems. The Safety Guide outlines several design measures which are possible as a means of increasing the capability of the electrical power systems to cope with a station blackout, without providing detailed implementation guidance.

A committee of international experts and advisors from numerous countries is currently working on an IAEA Technical Document (TECDOC) whose objective is to provide a common international technical basis from which the various criteria for SBO events need to be established, to support operation under design basis and design extension conditions (DEC) at nuclear power plants, to document in a comprehensive manner, all relevant aspects of SBO events at NPPs, and to outline critical issues which reflect the lessons learned from the Fukushima Dai-ichi accident.

This paper discusses the commonly encountered difficulties associated with establishing the SBO criteria, shares the best practices, and current strategies used in the design and implementation of SBO provisions and outline the structure of the IAEA's SBO TECDOC under development.

1. Introduction

As far back as 1985, the IAEA published a TECDOC on this subject — *Safety Aspects of Station Blackout at Nuclear Power Plants* (IAEA-TECDOC-332). That TECDOC focused mainly on safety aspects of SBO. Owing to the date of publication, it needs to be revised to account for lessons learned from past SBO events, as well as from the Fukushima Daiichi accident.

The IAEA, in cooperation with Member States, is currently developing a Technical Document on the "Design Provisions for Station Blackout for Nuclear Power Plants".

This paper describes design philosophy, station blackout recovery strategies, as well as guidance for existing plant designs that has been observed in Member State Countries participating in the development of the TECDOC.

---

[4] It will supersede the Safety Guide "Design of Emergency Power Systems for Nuclear Power Plants", Safety Standards Series No. NS-G-1.8, IAEA, Vienna (2004).

[5] Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012).

The TECDOC aims to provide a common international technical basis to be considered when establishing the various criteria for SBO events in line with recommendations from DS 430, Chapter 8 Alternate AC power source, regarding the design of electrical power systems for DEC and to provide technical guidance for the design provisions to deal with SBO events at NPPs. This involves a description of current plant practices and design provisions already implemented at some NPPs, as well as proposals for improvement of current design bases and qualification requirements to better deal with an SBO event, in order to further improve robustness of the plant electrical design.

The TECDOC provides a description of current plant practices and design provisions for SBO events already implemented at some NPPs, as well as proposals for improvement of existing plant design and qualification requirements to increase the robustness of the plant electrical design for contending with SBO events.

2. Classification of SBO event

While a Loss of Off-site Power (LOOP) is considered to be within the design basis for all plants and is managed through a range of redundant and diverse means, SBO is considered for most of existing NPP designs as a design extension condition (DEC).

International operational experience has shown that loss of off-site power supply concurrent with a turbine trip and unavailability of the emergency alternating current (AC) power system is a credible event. Lessons learned from the past and recent station blackout events, as well as the analysis of the safety margins performed as part of the ‘stress tests’ that have been conducted on European NPPs as a response to the Fukushima Daiichi accident, have identified the station blackout (SBO) event as a limiting case for most NPPs.

In the Fukushima Daiichi accident in 2011, the common cause failure of electrical power supply systems due to flooding resulted in the melting of the core of three reactors at the Fukushima Daiichi NPP, and severely restricted heat removal at the spent fuel pools for a long period of time. In addition, the flooding caused the loss of DC power supply. The plant was left without essential instrumentation and controls, and this made accident management for the plant operators very difficult. The operators remained without information on the critical plant parameters until the power supply was restored from portable batteries. The readings were discontinued, difficult to obtain.

Although the Fukushima Daiichi accident went well beyond SBO, many of the lessons learned from that accident still remain to be addressed. The design of the electrical power systems for both operating plants and new builds should account for both SBO and the full loss of all on-site AC and DC power. Criteria for the two types of events will necessarily be different, as we want to limit the consequences of SBO within the design basis envelope because the historical frequency of SBO is higher, while a total loss of AC and DC for a prolonged period as at Fukushima Daiichi represents a design extension condition.

2.1 SBO coping time

A coping time for an SBO event of a specific NPP design determines the safety margin that the plant has in response to the SBO event. A textbook definition of coping time is a “*time available from loss of all AC power to the safety bus until onset of core damage if no counter measures*”.

The SBO coping time determines whether the effective countermeasures can be implemented to prevent the core damage. For some NPP design the SBO coping time is very short (e.g. less than one hour), which makes it difficult to implement effective measures to either restore the power supply or ensure the heat removal function. Besides that, plant SBO can challenge performance of the systems and components; e.g. integrity of reactor coolant pump seals, loss of equipment due to loss of ventilation, etc.

SBO coping capability in term of design and organizational provisions currently implemented at NPPs in Member States (MS) varies from country to country; some countries rely on additional diesel generators or mobile means available on site; other countries have incorporated specific SBO provisions into the design as a second protection level (e.g. bunkered systems qualified to anticipated external events). Sizing of additional power sources to be used for SBO, and their qualification requirements are still subjects of discussions.

2.2 SBO coping capability

The plant SBO coping capability determines a time during which the pant withstand SBO without fuel damage. It also involves necessary design provisions, appropriate procedures and personnel training.

The Fukushima accident has showed that the external event which goes beyond the original plant design basis could result in extended loss of all AC power sources. In this case, the important consideration is how long can the plant cope without AC power to prevent core melt scenario.

3. SBO Management

This section describes challenges associated with SBO event, as well as design philosophy, and station blackout recovery strategies that have been observed in Member State Countries participating in the development of the TECDOC.

The objective of SBO management is to provide alternate AC power source to power necessary loads in order to bring the plant to a safe controlled state and to maintain it in the controlled state to prevent a core melt accident.

The SBO event management depends on several aspects, such as whether:

- the plant was operating at full power before the SBO event; or
- the plant was in the shutdown state for refuelling (including mid-loop operation); or
- the AC power can be restored quickly; or
- the restoration of AC power requires several hours but can still be accomplished within the coping time.

The following three SBO cases are discussed;

1. SBO event which can be recovered from within the coping time.
2. Extended SBO event.
3. SBO event that leads to a core melt scenario.

3.1 SBO recovery within coping time

This case is characterized by a short recovery period; i.e. alternate AC power supply can be started and connected to the plant safety bus(es) within 10-30 minutes. Regardless of the plant design, the heat removal function should be accomplished by non-AC powered loads.

SBO coping times varies between the different plant designs; therefore the coping strategies reflect the initiating event that caused the SBO conditions, plant response to the SBO condition, and available means, preferably stationary, which can be used.

For those plants equipped with turbine driven pumps for providing feedwater either to the SGs (PWRs and PHWRs) or reactor vessel (BWRs), the heat removal continues without interruption after the SBO event. The Uninterruptible Power Supply (UPS) buses provide enough power to ensure control and monitoring functions needed for heat removal.

For those plants without turbine driven means, i.e. which depend fully on AC power supply, a fast connection of alternate AC power or restoration of the grid is critical.

During the short duration SBO, the following challenges should be considered:

- Reactor coolant inventory (RCS) is sufficiently maintained;
- Re-criticality does not occur;
- Integrity of reactor coolant pump seals is not challenged;
- Battery capacity is sufficient to power necessary DC/AC loads;
- Alternate AC power source mission time is sufficient;
- CST has enough capacity;
- Spent fuel pool (SFP) heat up is a slow process.

The following steps are recommended during short SBO event (to be performed in parallel):

- Start up and connect the alternate AC power source to a safety bus;
- Ensure SG (PWR) make up from Condensate Storage Tank (CST);
- Ensure reactor vessel make up (BWR) from a suppression pool;
- Try to recover the grid;
- Try to recover at least one division of stand-by AC power sources.

The mission time for PWR the turbine driven feedwater pumps which provide the SGs with water from CST is typically several hours and therefore there is no concern with respect to heat removal in these cases. However, for BWR a rapid depressurization of the BWR could cause starvation of the steam supply to the feed pumps, causing them to trip. The mission time for the alternate AC power source is typically several days, and therefore this mission time does not limit its operation during short duration SBO events.

Continuity of DC power supply is typically needed for several hours, and thus alternate AC power supply can be restored before station battery banks are depleted.

It was observed that sizing of alternate AC power supply sources typically depends on the plant design; for example, plants with turbine driven capabilities (e.g. feedwater can be provided by turbine driven means into the SGs or reactor pressure vessel (BWR case) which means the alternate power source does not have to be sized to power the feedwater pumps, or fully electric plants which means that sufficient electrical power supply is necessary to power feedwater pumps. For PHWRs where SG makeup can be provided by mobile means, the alternate power supply source is only required to power critical instrumentation and monitoring loads.

The permanent pre-alignment of the alternate AC power source is desirable as this permit a shorter connection time. The alternate AC power supply source should be connected to the safety bus(es) only after it has been disconnected from other power supplies to prevent the alternate AC power source from becoming overloaded.

The alternate AC power source power capacity is limited and cannot supply large loads (e.g. cooling the turbine condenser, or ensuring residual heat removal from suppression pool of BWR); this is not an issue during the short SBO event, because the alternate power source is meant to be a temporary solution until the power supply is recovered either from the grid or standby AC power sources.

3.2 Extended SBO

In a situation, where the alternate AC power source was connected, but it was neither possible to recover the grid nor standby AC power sources, the plant enters the extended SBO condition which can last from hours to several days.

During extended SBO events, the Reactor Coolant Pump (RCP) integrity may be challenged if injections pump which provides water to the RCP seals remains unavailable. If RCP seals fail, the RCS leak rate will be equivalent to a small break LOCA. If RCS seal failure occurs maintaining the RCS inventory and sub-cooling margin may be a challenge. The autonomy of Condensate Storage Tank (CST) is limited and typically will last for several hours; however the CST will need replenishing from the external source, consequently, mobile equipment may be necessary.

The suppression pool heats up as steam is discharged into it and the residual heat removal system is no longer in operation because it requires more power than the alternate AC power source is capable of providing. High suppression pool temperatures may challenge the capability of the injection pumps (BWR).

For PWRs or PHWRs, the decay heat produced in a SBO event is removed from the core through natural circulation. A combination of two effects, i.e. shrinkage of RCS inventory due to temperature decrease and expected leakage from the RCS, cause a drop in the RCS pressure. The rate of this pressure decrease depends on the particular reactor design but is typically about 1MPa per hour. Maintaining the RCS inventory and sufficient sub cooling margin is therefore important to avoid formation of a bubble below the reactor pressure vessel (RPV) head which could potentially lead to loss of natural circulation.

During extended SBO, Spent Fuel Pool (SFP) cooling is necessary. If the alternate AC power source has insufficient capacity to power loads in the SFP cooling chain, a contingency cooling strategies via mobile pumps may be necessary.

3.3 SBO resulted in a core melt

There are several possible SBO scenarios which could lead to a severe accident, for example:

- Neither the grid nor stand-by AC power sources could successfully be restored within the coping time;
- The alternate AC power source cannot be started and/or connected to the safety bus within the coping time;
- The alternate AC power source was able to connect within the coping time, but it fails to operate in long-term (e.g. insufficient diesel fuel, damage due to extreme external events, etc.)
- If the entire grid, standby and alternate AC power sources are unavailable, and mobile means were unable to deploy with the coping time.

These scenarios may be caused by a combination of events including: multiple failures of plant equipment and severe external events (e.g. earthquake, flooding beyond design bases, severe weather conditions, airplane crash, etc). In addition to the reactor core, the on-site SFPs also require heat removal capability.

The stationary equipment, including alternate AC power source remains unavailable. From an electrical point of view, it may not be possible to provide power supply to the loads via the plant distribution system and therefore certain predefined loads would require direct power supply connection (via provisional cable connection).

4. Establishing Design Criteria for designated SBO equipment

This section describes SBO related design considerations as observed in countries participating in the development of the SBO TECDOC. These are applicable for alternate AC power sources of different voltage and power output, specific design features to better serve its purpose, i.e. mobility, connectivity, accessibility to a specific load to be powered, and capacity to allow for starting and operating required loads.

4.1 Safety classification

The alternate AC power sources, which provides for diversity, are classified, but not necessarily in the same class as the standby AC power sources. The equipment which makes it possible to connect alternate AC power source, including the connecting point to the plant buses have the same safety class as the alternate AC power source. Mobile AC power sources are typically not safety classified; demonstrating the functions associated with a safety class may be difficult.

4.2 Sizing criteria

The alternate AC power supplies have sufficient capacity to operate systems necessary for coping with a station blackout for the time required to bring the plant to and maintain it in a controlled state. A combination of postulated internal initiating events (e.g. LOCA) concurrent with a SBO is typically not considered.

If an alternate AC power source serves more than one unit at a site where safety standby AC power sources are shared between units, the alternate AC power source is designed to have sufficient capacity to operate systems necessary for coping with a station blackout for the time required to bring all units that share the safety AC power sources to, and maintain them in a controlled state. The alternate AC power source for one unit is normally connected neither to the on-site power system of that unit nor off-site power systems.

4.3 Qualification of SBO equipment

Equipment qualification includes functional qualification, qualification for the effects of internal events, and qualification for the effects of external events. Qualification for the effects of internal events and external events aims to ensure that these events do not result in common cause failure of alternate AC power source.

4.4 Storage of equipment

Plants in some Member States employ stationary alternate AC power sources. In these cases the stationary AC power sources are housed in bunkers or the AC power source are hardened so that there are adequately protected from external events.

Portable alternate power source(s) are stored in a location or locations such that it is reasonably protected such that no one external event can reasonably damage all the portable AC supply source(s). Reasonable protection is provided for example, through provision of multiple portable AC supply sources stored in diverse locations or through storage in structures designed to reasonably protect from applicable external events.

5. Differences for the new and existing plants

The integration of alternate AC Power sources is obviously easier and can be accomplished without compromise for a new plant compared to a retrofit application at an existing plant. If design and performance criteria are taken into consideration already in conceptual design of the plant, searching for suitable place where alternate AC power source can be installed, providing additional connecting points, additional spare batteries, raceway and sheltered locations for mobile power sources can be avoided. These design features can be accomplished already into the early design phase.

6. Design provisions to increase robustness of existing plants

The improvement measures to further enhance the robustness of the plant electrical systems require implementation of a complex solution, i.e. it should not be based just on supplying one additional alternate AC power source. The SBO design provisions should be seen in greater perspective, i.e. from initiating even or combination of events that actually caused SBO condition, protections against those events, availability alternate AC power source with pre-installed connecting points, both qualified for anticipated external events, availability of mobile power generating means that can be deployed on place, considering possible site devastation.

The Final peer review report[6] on the Stress Tests performed on European nuclear power plants underlined the "Necessary implementation of measures allowing prevention of accidents and limitation of their consequences in case of extreme natural hazards is a finding of the peer review that national regulators should consider. Typical measures which can be considered are bunkered equipment to prevent and manage severe accident including instrumentation and communication means, mobile equipment protected against extreme natural hazards, emergency response centres protected against extreme natural hazards and contamination, rescue teams and equipment rapidly available to support local operators in long duration events. Such possible measures, as identified by the peer review, are detailed in the report".

6.1 Design provisions implemented to cope with SBO

By analysing different member states solutions to cope with SBO event in different nuclear power plant designs, the following common level of defence were observed:

- A reliable (normal) power supply from the high voltage grid;

[6] Final peer review report on the Stress Tests performed on European nuclear power plants, April 2012

- House load capability of the turbine and generator island;
- At least two feeds from a backup grid (independent from the output grid);
- Standby AC power sources (redundant);
- A small generating nearby plants DGs (used for frequency control such as hydro, diesel generator station, gas turbine with a power output around 30 MW);
- Alternate (dedicated) AC power source designed and qualified for anticipated external events;
- Mobile diesel generators (high or low voltage);
- High capacity station batteries;
- Backup (charged) batteries stored on site.

The above level of defence appear to be sufficient to (i) minimize the occurrence of SBO event, or if SBO event occurs (ii) to prevent fuel damage by providing technical means and organizational measures to cope with SBO event and to prevent the fuel damage.

In order to cope with extended SBO duration, the following additional means or provisions have been considered to enhance the plant SBO coping capability:

- Medium size generators to re-energize battery chargers;
- Emergency diesel engine driven pumps to replenish water sources, i.e. CST make-up;
- Medium size generators and injection pumps to restore RCP seal cooling;
- RCP Shutdown seal package designs to limit seal leakage;
- Hardened wet well venting systems and suppression pool make-up with cold water (BWR);
- Pre-plan and pre-stage more emergency equipment to make manual actions easier and train more personnel to use it.

It is obvious that for extended SBO duration, it may be necessary to use alternative means of cooling including alternate heat sinks. SG gravity feeding, or using other sources of water, supply from stored condenser cooling water, alternate tanks or wells on the site, or water sources in the vicinity (reservoir, lakes, etc.) is an additional way of enabling core cooling and prevention of fuel degradation.

6.2 Design provisions for non-electric equipment

It has been discussed already that nether either alternate or mobile AC power source itself, despite their qualification to external events, may be insufficient to ensure a power supply function to designated SBO mitigation equipment. The AC/DC power distribution system, connecting points, cables, etc. should also be protected against effect of external or internal events.

Some plants have introduced improvement measures that better protects the electrical equipment from adverse effect or external natural events such as tsunami. This includes the following design improvements:

- Fastening outside transformers with anchor bolts to the grant to protect them from forces generated by tsunami or earthquake;
- Improving outdoor switchyards that are vulnerable to external natural events such as earthquake, tsunami;
- Installing water proof doors sealing the electrical compartments for stand-by and alternate AC power sources, DC batteries, and switchgear rooms;
- Sealing external cable traces to prevent water intrusion into the electrical distribution systems from the outside;

- Mounting connection points for connecting external power sources in an elevation which consider sufficient margin for the most severe flood anticipated in the design;
- Providing small floating transport means so that personnel is able to reach connecting points on site;
- Providing heavy equipment that is able to clear the road after a devastating event (earthquake, mud slides, etc.)
- Training the plant personnel for manual actions for as SBO duration increases.

6.3 Design provisions for extended mission time

The goal for SBO coping is to establish sufficient coping capability by relying upon installed equipment, onsite portable equipment, and pre-staged offsite resources to ensure fuel cooling function. The alternate as well as mobile AC power sources are deigned to operate autonomously, i.e. without need of support system provided by the plant (e.g. component cooling, instrument air, DC power, etc.). Typically, the equipment, procedures, and training necessary to implement an extended SBO consider mission time of 72 hours for core and spent fuel pool cooling and for reactor coolant system and primary containment integrity.

The alternate stationary as well as portable AC power sources typically have a capacity which does not allow powering all main and support systems needed for a standard heat removal function. For example heat, ventilation and air-conditioning system is not included among loads powered in SBO conditions. Some equipment credited in SBO cooping such as turbine driven pumps are enclosed in a small room, in which without ventilation the ambient temperature may rise to values at which the equipment is outside the design basis and which may fail to operate in a long term. Some member states implemented design provisions to power loads ensuring ventilation functions (e.g. local ventilators and chillers) for designated equipment.

7. Conclusions

This paper provides an outline of main topics that are discussed in the IAEA TECDOC on design provisions for SBO event in greater details. Furthermore, the SBO TECDOC provides examples, including illustrative figures, on design provisions that have already been implemented in participating Member State Countries.

The improvement measures to further enhance the robustness of the plant electrical systems for SBO event require implementation of a complex solution, i.e. it should not be based just on supplying one additional alternate AC power source.

The SBO design provisions should be seen in greater perspective, i.e. from initiating even or combination of events that actually caused SBO condition, protections against those events, availability alternate AC power source with pre-installed connecting points, both qualified for anticipated external events, availability of mobile power generating means that can be deployed on place, considering possible site devastation.

A mission time for SBO equipment should be carefully considered in the design, especially for extended SBO events. The only fact that the AC power sources has started and connected to the bus successfully is not sufficient.

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

Design Provisions for Station Blackout for Nuclear Power Plants
IAEA TECDOC

Alexander DUCHAC
SAS,
NSNI

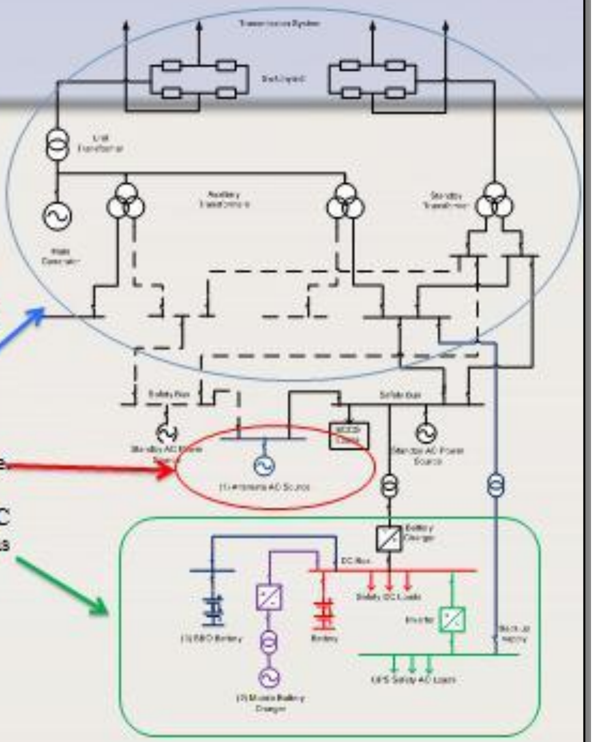
IAEA
International Atomic Energy Agency

Contents

- Why SBO topic
- Relation with IAEA Safety Standards
- Objective
- Content of SBO Tecdoc
- Examples of SBO design provisions
- Preliminary results

IAEA

SBO Definition



A station blackout (SBO) is defined as a plant condition with complete loss of all AC power to safety and non-safety buses from off-site sources, from the main generator and from standby AC power sources important to safety.

Alternate AC power supplies are available.

DC power supplies and uninterruptible AC power supplies may be available as long as batteries can supply the loads.

IAEA

Why SBO Topic?

Year	NPP	Event
1986	Kori 4 (Korea)	SBO caused by a typhoon
1990	Vogtle 1 (Georgia, USA)	Off-site power was lost from switchyard work during a refuelling outage
1993	Narora 1 Event (India)	Ejected turbine blade caused a fire and hydrogen explosion
1993	Kola Event (Russia)	LOOP induced by high wind and failure of EDGs
2001	Maanshan (Taiwan)	Tropical storm caused loss of off-site power
2006	Forsmark 1 (Sweden)	Near SBO, Switchyard work resulted in overvoltage
2011	Fukushima (Japan)	Following a major earthquake of magnitude 9.0 on the recter scale, a 15-metre tsunami disabled the power supply and cooling of three Fukushima Daiichi reactors, causing a nuclear accident on 11 March 2011.
2012	Byron event (USA)	Failure of insulator resulted in open phase conditions on offsite power source. The failure was not detected by the onsite degraded voltage relays. As a result, the standby sources did not start.
2012	Kori 1 (Korea)	An error in generator protective relay testing resulted in loss of off-site power to shutdown cooling.
2013	Forsmark 3	Human error resulted in two open phase conditions. The failure was not detected by the onsite voltage relays. As a result, the standby sources did not start.

IAEA

Why SBO Topic?

- More than 10 (reported) events so far
- Early recovery in most cases
- Only Fukushima resulted in fuel melt
- OEF show important precursors not to be ingored
- EU Stress tests identified SBO as most limiting
- SBO Classification

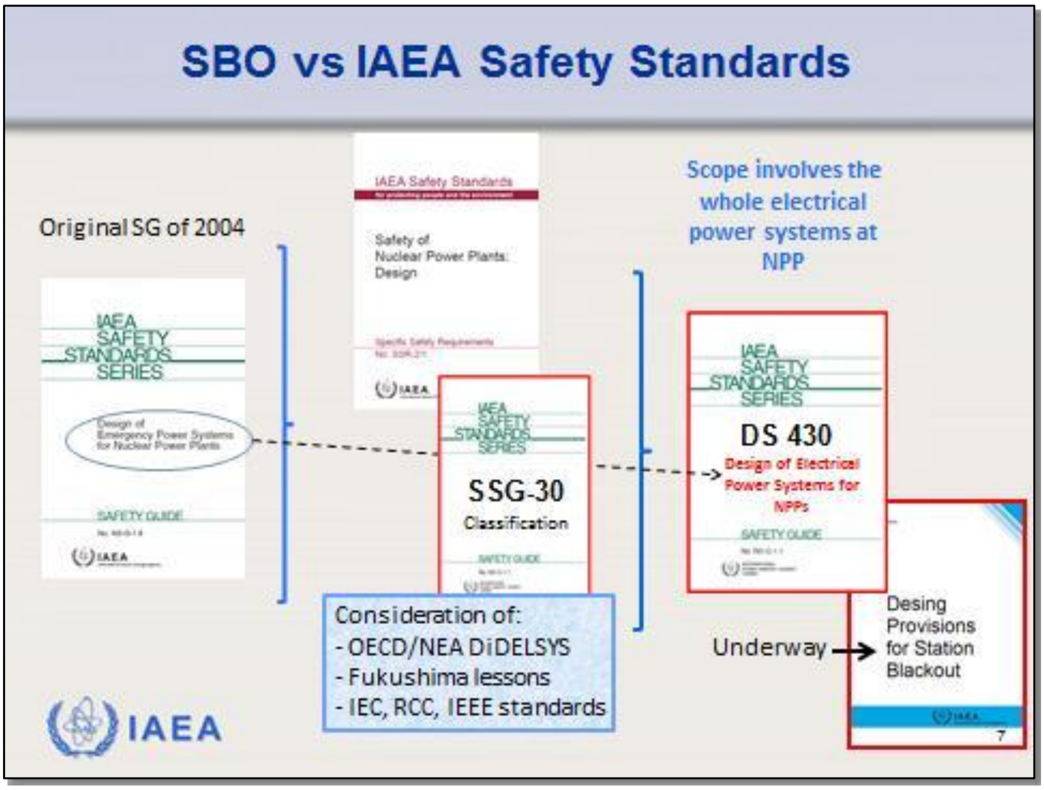
  DBA vs DEC?

IAEA

SBO vs IAEA Safety Standards

- 1985 – TECDOC 332 "Safety Aspects of Station Blackout"
- 2012 – DS 430 Design of Electrical power systems (revision of NS-G-1.8)
- 2013 – DS 462 Revision of SSR 2/1 Design
  - The design shall include an emergency power supply capable of supplying the necessary power in AOO and DBAs, in the event of the loss of off-site power. The design shall also include an alternate power source to supply, in particular, the necessary power in DEC.
- 2014 – new TECDOC "Design Provisions for SBO"

IAEA



Scope of the new Electrical Guide

- Describes the **whole electrical power system** at NPP
- Describes defense-in-depth concept for electrical systems
- Provides for design basis, general and detailed design guidance considering:
  - Anticipated electrical events (AOO, DBA)
  - Station Blackout
- Highlights
  - the interface with off-site power
  - the role of normal distribution systems as:
    - A source of power for many systems, and as
    - A source of power for emergency systems
  - the importance of electrical protection (breakers and their coordination)

IAEA

8

SBO TECDOC Objectives

- Further develop Chpt 8 of DS 430 on Alternate power source
- Provide common international technical basis
- Provide current regulatory basis
- Describe current plant practices and qualification requirements
- Show examples "what and how"…
- Provide proposal to further increase robustness

Our SBO Team →

IAEA

SBO TECDOC Content

- SBO management
  - within coping time
  - Extended SBO
  - SBO leading to SA
- Design criteria for SBO equipment
  - Classification
  - Sizing
  - Qualification
  - Storage
- Differences between existing and new plant designs
- Design provisions to increase robustness
- Operating experience

IAEA

SBO TECDOC Content

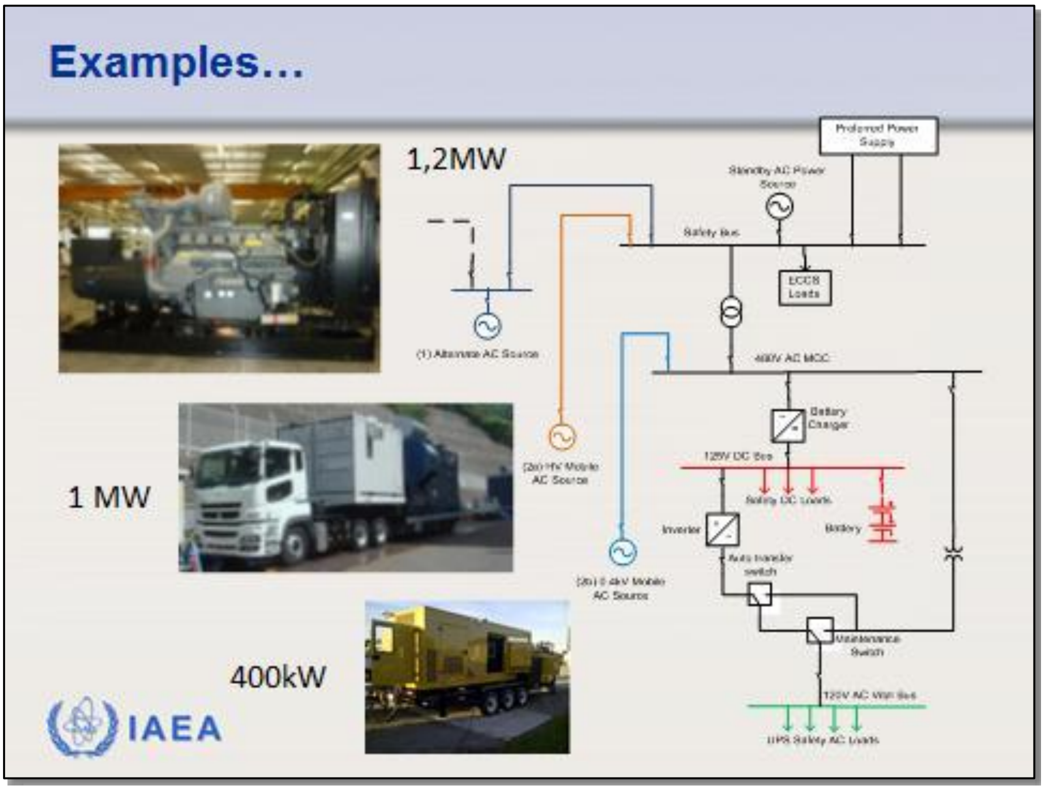
- Addresses SBO related issues:
  - RCP seals integrity
  - Fuel pool cooling
  - DC power continuity
  - Condensate supply to replenish EFT, or CST;
  - Instrument air
  - HVAC
  - Emergency illumination
  - Power supply for communication.

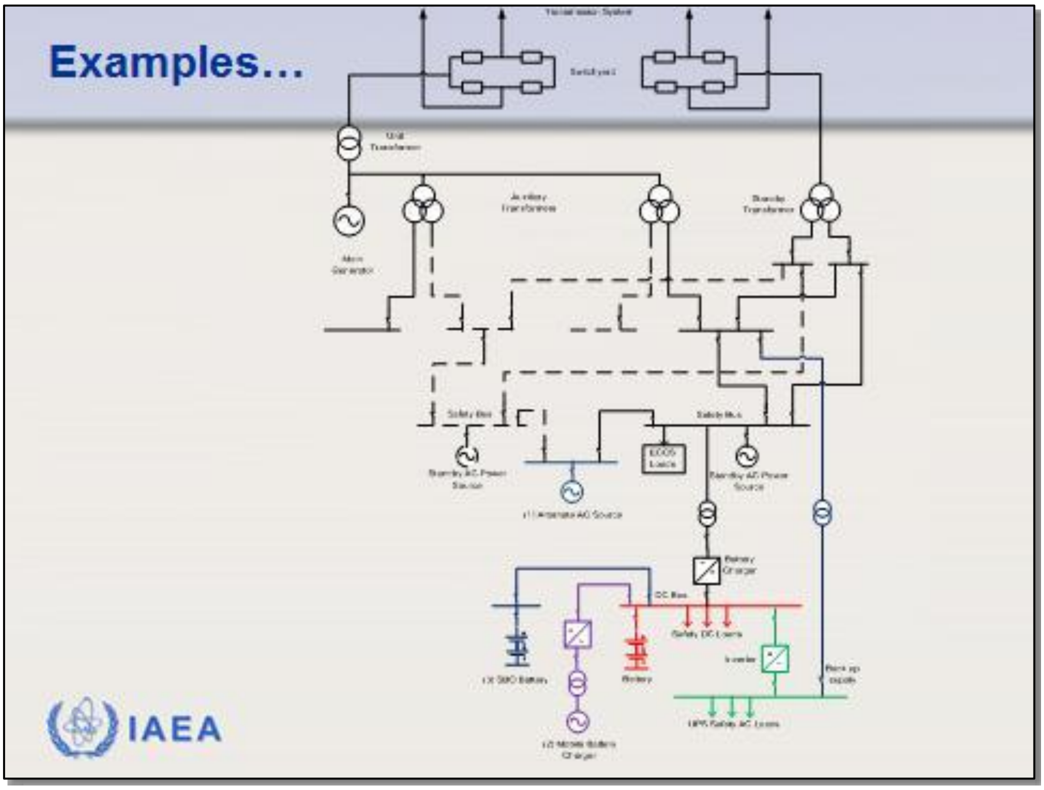
IAEA

Design & performance criteria

- Sizing?
- Qualification for external events?
- Storage and location on the site?
- Do diverse diesels have any advantage?
- What about power connections?
- How does possible failure of plant distribution systems affect alternate AC power sources guidance?
- Sharing alternate AC power sources at multi unit sites?

IAEA


Examples…
1,2MW
1 MW
400kW
Preferred Power Supply
Standby AC Power Source
Safety Bus
ECCS Loads
(1) Alternate AC Source
400V AC MCC
Battery Charger
(2a) HV Mobile AC Source
125V DC Bus
Safety DC Loads
Inverter
Battery
Auto transfer switch
(2b) 0.4kV Mobile AC Source
Maintenance Switch
120V AC Vital Bus
UPS Safety AC Loads
IAEA


Examples…
Unit Transformer
Auxiliary Transformers
Main Generator
Safety Bus
ECCS Loads
Standby AC Power Source
(1) Alternate AC Source
Battery Charger
DC Bus
Safety DC Loads
Inverter
Battery
UPS Safety AC Loads
IAEA

Preliminary results

- No solution "one fit to all"
- A complex issue, not just a new EDG
  - How to get AC/DC power to specific loads
  - Protected pre-installed connection, power distribution system, electrical protection, etc.
  - Qualification, what hazards to be considered
- A mission time not only for SBO equipment
- RCP integrity, RCS inventory

IAEA

When is it published?

- November 2013 – 1st CS meeting
- Mach 2014 – 2nd CS meeting
- June 17-20, 2014 – Technical Meeting
- October 2014 – 3rd CS Meeting
- December 2014 – Final Draft
- March 2015 – Internal review
- June 2015 - Publication

IAEA

Timing criteria for supplemental BWR emergency response equipment

Dr. John H. Bickel
Evergreen Safety & Reliability Technologies, LLC, USA

Abstract

The Great Tohuku Earthquake and subsequent Tsunami represented a double failure event which destroyed offsite power connections to Fukushima-Daiichi site and then destroyed on-site electrical systems needed to run decay heat removal systems. The accident could have been mitigated had there been supplemental portable battery chargers, supplemental pumps, and in-place piping connections to provide alternate decay heat removal. In response to this event in the USA, two national response centers, one in Memphis, Tennessee, and another in Phoenix, Arizona, will begin operation. They will be able to dispatch supplemental emergency response equipment to any nuclear plant in the U.S. within 24 hours. In order to define requirements for supplemental nuclear power plant emergency response equipment maintained on-site vs. in a regional support center it is necessary to confirm: (a) the *earliest time such equipment might be needed* depending on the specific scenario, (b) the nominal time to move the equipment from a storage location either on-site or within the region of a nuclear power plant, and (c) the time required to connect in the supplemental equipment to use it. This paper describes an evaluation process for a BWR-4 with a Mark I Containment starting with: (a) severe accident simulation to define best estimate times available for recovery based on the specific scenario, (b) identify the key supplemental response equipment needed at specific times to accomplish recovery of key safety functions, and (c) evaluate what types of equipment should be warehoused on-site vs. in regional response centers.

Introduction

The existing fleet of General Electric designed BWR-4s with Mark I containments were originally designed to meet the requirements of a regulatory-driven design bases large break LOCA with subsequent loss of offsite power. To address the requirements of such scenarios assumptions were made that batteries would be sized to provide for uninterruptible instrument and control power to allow emergency diesel starting and loading of essential coolant makeup and decay heat removal systems. While batteries were typically designed for greater capacity than these diesel starting and loading sequences, they were not sized to provide an indefinite source of DC instrumentation and control power to operate safety/relief valves (SRVs) or start/stop control of steam driven pumps such as High Pressure Coolant Injection (HPCI) and Reactor Core Isolation Cooling (RCIC).

Risk assessments, starting with the WASH-1400 Reactor Safety Study [Ref. 1] in the mid-1970's, indicated that design bases LOCA scenarios for which the reactor plant was "*over-designed for*" were not the greatest threat to reactor safety. It was the Station Blackout (SBO) and prolonged loss of decay heat removal scenarios which relied upon existing DC power systems, SRVs, and HPCI/RCIC pumps that posed the greater challenge to safety. Such scenarios involved:

- eventual loss of DC power due to slow battery discharge (below voltage levels required to operate equipment),
- heat up of the suppression pool to the point containment back pressure causes the SRVs to re-close (thus eliminating the key heat removal path from the reactor), and

- eventual overpressure failure of the containment.

Risk assessments performed by US BWR owners in the 1980's as a result of USNRC requirements for plant specific Individual Plant Examinations [Ref. 2] identified a number of modifications which could dramatically reduce the risks of SBO and prolonged loss of decay heat removal. These included:

- alternate means of recharging station batteries without the emergency diesel generators
- installation of a high pressure hard pipe containment vent from the suppression pool to the atmosphere to maintain containment pressures below the pressure where SRVs re-close
- installation/upgrading of piping connections to allow alternate water injection to the reactor vessel from external sources such as site fire water systems which exist on all plant sites
- development of emergency procedures to better deal with beyond design bases accident scenarios.

In the aftermath of the September 11, 2001 terrorist attacks, the USNRC issued orders to all operating US reactors to improve their ability to cope with extensive plant damage scenarios and its effects on spent fuel pool, core, and containment cooling. Many of the supplemental features identified in the previous 1980's-1990's era risk assessments, such as: portable battery chargers were then credited as flexible or "FLEX" mitigation devices which would be warehoused away from the specific plant locations where they were to be used. In other cases new portable pumps were procured and strategically warehoused in specified secure locations.

Critical Assumptions in Defining Timing Requirements

To systematically assess timing requirements the "Coping Time" will be used as the bases for comparisons. For the purposes of this analysis, the Coping Time is the time available from the onset of the accident scenario to the point where if some recovery action is not already taken, it is not possible to recover without core damage as defined in Section SC-A2 of the ASME Risk Standard [Ref. 3]. Before assessment of critical timing requirements it is necessary to define the key or bounding assumptions which govern the timing requirements for mitigation strategies for Station AC Blackout or prolonged loss of decay heat removal. These include:

- the spectrum of accident scenarios to be considered (or excluded)
- the consequential failure assumptions to be considered (or excluded)
- limitations in equipment performance (e.g. pressure and or temperature limits)
- time-dependent limitations on equipment performance such as battery depletion, fuel oil depletion

These are each discussed below.

Accident Scenario Assumptions

1. Seismic vs. Non-Seismic SBO scenario: a Seismic SBO would likely severely damage typical *site fire water systems*[7] rendering the typical diesel firewater pump unable to serve as an alternate makeup source.
2. Seismic vs. Non-Seismic SBO scenario: a Seismic SBO would likely severely damage the Condensate Storage Tank which is the normal water supply for the HPCI and RCIC pumps. This places reliance on the Suppression pool as a water source for HPCI/RCIC pumps during Seismic events.

[7] Fire water systems in US nuclear power plants are not typically designed to cope with seismic events and piping sections would be assumed to fail.

3. A prolonged Station AC Blackout leads to overpressurization of the reactor pressure vessel and the slow boil-off of reactor coolant through the continuous cycling of SRVs. Consideration of larger leakage rates (e.g. Small, Medium, Large LOCAs[8]) obviously results in much more rapid rates of depletion of coolant inventory and hence significantly shorter Coping Times.
4. The simultaneous loss of DC power coincident with Station AC Blackout is not further analyzed as this would eliminate the possibility of monitoring or operating HPCI, RCIC, SRVs, and Containment Hard Pipe Vent valves. Effectively there would be very little coping time available for such scenarios.

Consequential Failure Assumptions

1. The failure to automatically SCRAM given an SBO is not further analyzed as it is a very low probability event and is assumed to yield insufficient Coping Time for any supplemental equipment to be credited.
2. The continuous cycling of an SRV for the purposes of removing core decay heat presents a possible scenario for a stuck upon SRV occurring at some time after the event has started. Obviously the more limiting case is the consequential stuck open SRV occurring at the start of the scenario. This limiting assumption is used for evaluating stuck open SRVs.
3. Miscellaneous coolant leakage into the Drywell: prolonged loss of cooling to the main recirculation pump (RCP) seals may result in consequential RCP seal leakage. The amount of consequential RCP seal leakage in BWR RCPs is subject to high uncertainties ranging from 130 gpm [Ref. 4] to 200 gpm [Ref. 5].

Limitations on Equipment Performance

1. If larger 4kV AC powered pumps (e.g.: LPCI/RHR, or Core Spray pumps) are to be used based upon re-powering the safeguards buses, the reconnection of 4kV power must occur prior to the point where pump Net Positive Suction Head (NPSH) is lost due to suppression pool temperature rise.
2. SRVs depend upon DC power and compressed Nitrogen gas to properly operate. In the event there is insufficient DC power (e.g. DC voltages < ~92% Nominal) or Nitrogen gas pressure <90 psia, the SRVs will only operate as mechanical spring loaded safety valves in the range of 1124 psia.
3. SRVs are located in the Drywell region and utilize electro-pneumatic controls to open and close. The electro-pneumatic components are only qualified to a temperature of: 335°F. Proper operation above this point is beyond their design bases and *cannot be assured*. Because of this limitation, BWR emergency operating procedures require manual depressurization of the reactor if Drywell temperatures exceed 281°F and no means exist to reduce temperature (such as RHR Sprays). This Drywell temperature limitation becomes a critical limit in how long manual depressurization can be avoided.
4. To assure availability of the Suppression Pool to control containment pressure rise from a subsequent blowdown of the reactor pressure vessel, BWR emergency operating procedures require manual depressurization below pressure limits according to a Heat Capacity Temperature Limit curve such as shown in Figure 1.

[8] LOCA sizes are as follows:

LOCA Classification	Break Diameter Size
Small LOCA	100 gpm to 2 inch steam 100 gpm to 1 ¼ inch water
Medium LOCA	2 - 3 inch steam 1 ¼ - 3 inch water
Large LOCA	3 - 28 inch steam 3 - 28 inch water

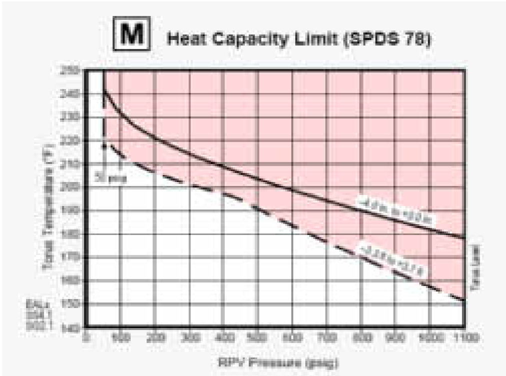


Figure 1 – Heat Capacity Temperature Limit

5. When the containment pressure exceeds 89.7 psia, the electro-pneumatic controls for the SRVs cannot open the SRVs in the control mode. SRVs will then only operate in the mechanical spring loaded safety valve mode, cycling ~1124 psia.
6. When the water temperature to the RCIC pump exceeds 200°F, self cooling of the RCIC pump is beyond the design bases and the pump is assumed to shutdown, necessitating use of the "FLEX pump".

Time Dependent Limitations on Equipment Performance

1. The rate of DC battery depletion is dependent on the assumed duty cycle of SRVs, HPCI/RCIC pumps, and continuous instrumentation and control power consumption. Rather than evaluating hundreds of possible duty cycles, one limiting duty cycle was chosen for evaluating the depletion times of the 125V and 250V batteries. This is acknowledged to be a conservatism which could be re-visited if necessary in the future. Making this assumption yielded: 5.75hrs for the Div. I 125VDC Battery (limits RCIC operation), 5.5hrs for the Div. II 125VDC Battery (limits HPCI operation), 7.0 hours for Div. I 250VDC Battery (limits SRV operation), and 8.0hrs for Div. II 250VDC Battery (limits SRV operation).
2. The rate of fuel oil consumption for the diesel fire pump (credited in Non-Seismic SBO scenarios) was actually measured. It was determined that the existing day tank would require replenishment in ~11hrs after the diesel fire pump is started.
3. Room Heat-up considerations: the diesel fire pump (credited in Non-Seismic SBO scenarios) is located in an enclosure which must have a door opened within 30 minutes to maintain temperatures at a level that would allow manual entry to top off the diesel fuel tank. This is addressed in SBO procedures.
4. Bottled Nitrogen gas supplies were estimated to require changing out bottles approximately every 9 hours if SRVs or containment Hard Pipe Vent valves were cycling. This is addressed in SBO procedures.

Scenario Analysis

The analysis was performed for a 2004 MWt BWR using the MAAP4.0.6 code [Ref. 6] with best-estimate decay heat loads and all of the previously noted operating limitations embodied as a part of the control logic. The assumed water temperature and water levels in the suppression pool were chosen to envelope 90% of observed normal plant operation. Similarly, the water temperature of the external heat sink was chosen to envelope 90% of observed environmental conditions.

Approximately 80 separate scenarios and sensitivity cases were evaluated to separate out timing requirements for connection of supplemental emergency response equipment. The approach taken was to evaluate *Coping Times to prevent core damage* for SBOs in conjunction with Small and Medium LOCAs, and Stuck Open Relief Valve scenarios which are assumed to occur coincident with the Loss of Offsite Power and Subsequent SBO. The analyses postulated various successes/failures of the LPCI/RHR, HPCI, RCIC, Diesel Fire Water, and FLEX pumps by first determining the longest *Coping Times* available to reconnect 4kV AC power to the main safety related safeguards buses while still avoiding a peak core temperature of 1800°F.

Results of the Evaluation

Without analysis it was presumed that the following scenarios can not be mitigated *without immediate availability of AC power*:

- Large Design Bases LOCA with SBO
- SBO and ATWS

For these cases, safety must be assured by *providing robust design criteria to prevent large pipe failures or SCRAM failure*.

Table 1 provides a summary overview of the Coping Times to recover either 4kV power, or installation of supplemental FLEX pumps, or battery chargers. The following is noted:

- Scenarios involving very short Coping Times (< 3.5 hours) and/or failure of HPCI cannot be mitigated with FLEX equipment. Recovery of emergency diesel generators to power emergency safeguards buses would *be the only mitigation strategy possible from a timing perspective.*
- For scenarios with Coping Times greater than ~4 hours, the use of portable FLEX pumps and battery chargers becomes a very reasonable alternative, provided that the equipment is located on-site.
- Provision of mobile diesel generator sets from a regional support center would benefit longer term scenarios where the issue becomes containment heat removal, if containment venting is not performed.
- If operation of the HPCI/RCIC pumps and containment venting is possible - and is supplemented by portable battery chargers and a suitably sized FLEX pump, it is possible to cope with a seismic SBO scenario indefinitely without external equipment, provided that sufficient quantities of fuel and compressed Nitrogen are available.

Figure 2 shows one of the simulations of a successful strategy to cope with a Seismic SBO with concurrent RCP seal leakage – which is a more probabilistically likely scenario. It involves allowing the HPCI/RCIC to both automatically start after taking suction from the Suppression Pool, and flood up the RPV to the high level trip point. At this point the high capacity HPCI is deactivated to conserve DC power – and leave it as a backup in case of failure of the RCIC pump. After the RPV level boils off, RCIC is restarted and manually throttled to maintain a relatively constant RPV level. Anticipating that eventually steam driven HPCI and RCIC will no longer be viable because of containment pressure and temperature, plant personnel make hose connections for the portable FLEX pump to the fire water connection to the LPCI injection pathway. Following this, portable battery chargers are brought in and cable rolled out to begin recharging the various station batteries. When all is in place (but no later than the point where RCIC shuts down) operators manually depressurize the RPV allowing the FLEX pump to take over maintaining RPV level using an external water source. There would be a minor drop in RPV water levels during depressurization but flashing of coolant allows steam cooling that keeps core temperatures continuously dropping. The containment is vented using the Hard Pipe Vent and a long term heat removal pathway is established through the Suppression Pool. Throughout this period there would be a need to monitor and maintain fuel supplies to the FLEX pump and portable battery chargers, as well as maintain sufficient inventories of compressed Nitrogen gas to keep SRVs and Hard Pipe Vent valves operable.

Conclusions

This analysis was focused on determining the timing requirements and portable equipment to *avoid any core damage.* [The timing and equipment requirements to cope with core damage and mitigation of offsite releases were beyond the scope of this evaluation.] The analysis resulted in the following insights and conclusions regarding timing requirements for Supplemental Emergency Response Equipment:

1. Scenarios involving Seismic-induced Large or Medium LOCAs with concurrent SBO cannot be practically addressed with supplemental portable equipment because the connection time requirements are far too short. Assuring safety for these scenarios *must rely upon design margins to prevent Large and/or Medium LOCAs with onsite power system failure given a seismic event*.
2. *Requirements for FLEX pumps:* The likelihood of eventual loss of steam driven HPCI/RCIC pumps due to either: (a) Drywell heatup >281°F requiring depressurization of the reactor and thus loss of steam supply as early as 1.1 hours (Sesimic SBO with Small LOCA, initial HPCI operation) - 3.9 hours (SBO with Stuck Open Relief Valve and initial HPCI operation), or (b) eventual turbine high exhaust pressure or suppression pool temperature - gives high priority to the ability to quickly connect a portable FLEX pump via hose connections and pre-installed fittings. The earliest connection time need for a portable FLEX pump to a suitable water source would be within ~1.0 hour (very worst case and likely difficult to achieve) but more likely longer (e.g. >4 hrs). These timing requirement dictate that the portable FLEX pump be *located onsite* and portable enough to be moved with hoses to where needed along with an adequate supply of fuel.
3. *Requirements for Portable Battery Chargers:* If the HPCI/RCIC pumps are able to continue running beyond ~4 hours, the loss of DC control power to the pumps from the Div I and II 125VDC batteries becomes the next critical limiting failure. The connection of a portable battery charger within < 5 hours becomes the next essential requirement to successfully mitigate a beyond design bases SBO (whether caused by a seismic event or other natural phenomenon). This timing requirement dictates that the portable battery charger be *located onsite* and portable enough to be moved to where needed along with an adequate supply of fuel.
4. *Requirements for Mobile Diesel Generators:* Equipment to facilitate the recovery of 4kV safeguards buses (thus allowing operation of LPCI/RHR pumps) using a mobile skid mounted, self-contained diesel generator could be effective depending on proximity of equipment and availability of quick high voltage connection points. The analysis indicates the possibility of using such equipment is helpful at almost any time it becomes available.

A key conclusion of this analysis is that the onsite supplemental FLEX equipment (with adequate fuel and compressed Nitrogen gas stores) is fully sufficient to keep the core covered and prevent any fuel damage for an indefinite period of time and that the 24 hour time dispatch time requirement for external support is not limiting.

References

[1] Reactor Safety Study, WASH-1400, December 1975.

[2] Individual Plant Examination for Severe Accident Vulnerabilities – 10 CFR 50.54(f), US Nuclear Regulatory Commission Generic Letter No. 88-20, issued November 23, 1988.

[3] Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS Standard RA-S-2008.

[4] Recirculation Pump Shaft Seal Leakage Analysis, General Electric Topical Report NEDO-24083, issued November 1978.

[5] Evaluation of Recirculation Pump Seal Failure in BWRs, Brookhaven National Laboratory Report A-3806-4-93 Rev.1, issued June 1993.

[6] MAAP4, Modular Accident Analysis Program, Electric Power Research Institute, May 1994.

Table 1 – Coping Times Available for Supplemental Emergency Response Equipment

Scenario	*Coping Time*	*Limitations*	*Comment*
Medium LOCA with SBO	13.2 minutes	Need to restore 4kV AC power to LPCI pumps. Steam driven HPCI/RCIC pumps are insufficient to provide necessary makeup.	Recovery using FLEX pump not credible
SBO with Stuck Open Relief Valve and HPCI failure	24 minutes	Need to restore 4kV AC power to LPCI pumps. Steam driven RCIC pumps are insufficient to provide necessary makeup.	Recovery using FLEX pump not credible
Small LOCA with SBO and HPCI failure	30 minutes	Need to restore 4kV AC power to LPCI pumps. RCIC is insufficient to provide necessary makeup. Diesel Fire Pump cross-connection cannot be implemented in sufficient time.	Recovery using FLEX pump not credible
Small LOCA with SBO and initial HPCI operation with suction from CST	2 hours	High Drywell Temperature requires depressurization which causes loss of steam driven HPCI at ~46 minutes. Need to restore 4kV AC power to LPCI pumps. CST would not be available following Seismic event	Recovery using FLEX pump not credible
Small LOCA with SBO, initial HPCI operation with suction from CST or Suppression Pool, failure of Diesel Fire Pump. - or – Seismic SBO with Small LOCA, initial HPCI operation with suction from CST, seismic failure of Diesel Fire Water	2.5 hours	High Drywell Temperature requires depressurization which causes loss of steam driven HPCI at ~1.1 hours. RCIC is insufficient to provide necessary makeup. Need to restore 4kV AC power to LPCI pumps. CST would not be available following Seismic event	Recovery using FLEX pump not credible
SBO with Stuck Open Relief Valve and initial HPCI operation	3.5 hours	High Drywell Temperature requires depressurization at ~ 3.9 hours which causes loss of steam driven HPCI. Need to restore 4kV AC power to LPCI pumps and RHR. Steam driven HPCI pump operation provides a little more time to recover AC power to LPCI pumps and RHR	Need for FLEX pump in ~ 3.9 hours
SBO with initial HPCI operation taking suction from CST - or – Seismic SBO with initial HPCI operation taking suction from Suppression Pool	4.5 hours	High Drywell Temperature requires depressurization which causes loss of steam driven HPCI. Need to restore 4kV AC power to LPCI pumps and RHR.	
SBO with failure of Diesel Fire Water, initial RCIC operation taking suction from CST - or –	6.5 hours	High Drywell Temperature requires depressurization at ~4.9 hours. RCIC pump looses DC control power ~ 5.75 hours RCIC pump would also shut down on high exhaust Temperature at ~5.75 hours. Need to restore 4kV AC power to LPCI pumps and RHR.	Need for Supplemental Battery Charger in <5 hours

Seismic SBO with seismic failure of Diesel Fire Water, initial RCIC operation taking suction from Suppression Pool			
Scenario	*Coping Time*	*Limitations*	*Comment*
Seismic SBO with Stuck Open Relief Valve, seismic failure of Diesel Fire Water, and initial HPCI/RCIC operation taking suction from Suppression Pool	7.0 hours	HPCI pump looses DC control power ~5.5 hours RCIC pump looses DC control power ~5.75 hours Need to restore 4kV AC power to LPCI pumps and RHR.	Need for Supplemental Battery Charger in <5 hours
Small LOCA with SBO, initial HPCI operation with suction from CST, manual depressurization, injection of Diesel Fire Water	9.0 hours	High Drywell Temperature requires depressurization at ~1.1 hours which causes loss of steam driven HPCI. RCIC is insufficient to provide required makeup. Diesel Fire Water is sufficient until Div I, II 250VDC batteries deplete to point SRVs re-close, reactor re-pressurizes above shutoff pressure of Diesel Fire Water pump. Need to restore 4kV AC power to LPCI pumps and RHR.	Need for Supplemental Battery Charger in <8 hours
SBO with initial HPCI/RCIC injection taking suction from CST, manual depressurization and Diesel Fire Water injection until 250VDC battery discharge. - or – SBO with Stuck Open Relief Valve, initial HPCI/RCIC injection taking suction from CST, manual depressurization and Diesel Fire Water injection until 250VDC battery discharge.	11.0 hours	Discharge of 250VDC batteries ~8 hours causes reactor to re-pressurize above the shutoff pressure of the Diesel Fire Pump Need to restore 4kV AC power to LPCI pumps and RHR.	Need for Supplemental Battery Charger in <8 hours
SBO with RCIC taking suction from CST, ***supplemental battery charger connected <5hrs prior to loss of DC control power for RCIC and SRVs***	21.5 hours	RCIC shuts down at 18.7 – 19.5 hours due to high turbine exhaust temperature. Need to restore 4kV AC power to LPCI pumps and RHR.	Need for Hard Pipe Vent operation at < 20 hours
SBO with Stuck Open Relief Valve,	23.0 hours	Stuck Open Relief Valve causes eventual loss of steam driven HPCI/RCIC pumps.	Need for Hard Pipe Vent operation

initial HPCI/RCIC taking suction from CST, ***supplemental battery charger connected <5hrs prior to loss of DC control power for RCIC and SRVs,*** Diesel Fire Water injection until containment back-pressure closes SRVs		Long term rise in containment back-pressure causes all SRVs to re-close. Re-pressurization of reactor above discharge pressure of Diesel Fire Water pump causes loss of injection. Need to restore 4kV AC power to LPCI pumps and RHR for Drywell and Suppression Pool Cooling.	at < 20 hours
Scenario	*Coping Time*	*Limitations*	*Comment*
SBO with initial HPCI/RCIC taking suction from CST, ***supplemental battery chargers connected <5hrs prior to loss of DC control power for RCIC and SRVs,*** Diesel Fire Water injection until containment back-pressure closes SRVs	24.0 hours	Long term rise in containment back-pressure causes all SRVs to re-close Re-pressurization of reactor above discharge pressure of Diesel Fire Water pump causes loss of injection. Need to restore 4kV AC power to LPCI pumps and RHR for Drywell and Suppression Pool Cooling.	Need for Hard Pipe Vent operation at < 20 hours
SBO with Small LOCA, or Stuck Open Relief Valve, initial HPCI/RCIC taking suction from CST, ***supplemental battery chargers connected <5hrs prior to loss of DC control power for RCIC and SRVs,*** Diesel Fire Water injection, controlled Containment Venting	***Indefinite***	Fuel supply to FLEX pumps and portable battery chargers. Compressed Nitrogen gas to operate SRVs and Hard Pipe Vent valves.	
Seismic SBO with Small LOCA, or Stuck Open Relief Valve, initial HPCI/RCIC taking suction from Suppression Pool, ***supplemental battery chargers connected <5hrs prior to loss of DC control power for RCIC and SRVs, supplemental FLEX pump connected***, controlled Containment Venting	***Indefinite***	Fuel supply to FLEX pumps and portable battery chargers. Compressed Nitrogen gas to operate SRVs and Hard Pipe Vent valves.	

Figure 2 – Successful Mitigation Strategy for Seismic SBO using FLEX Equipment

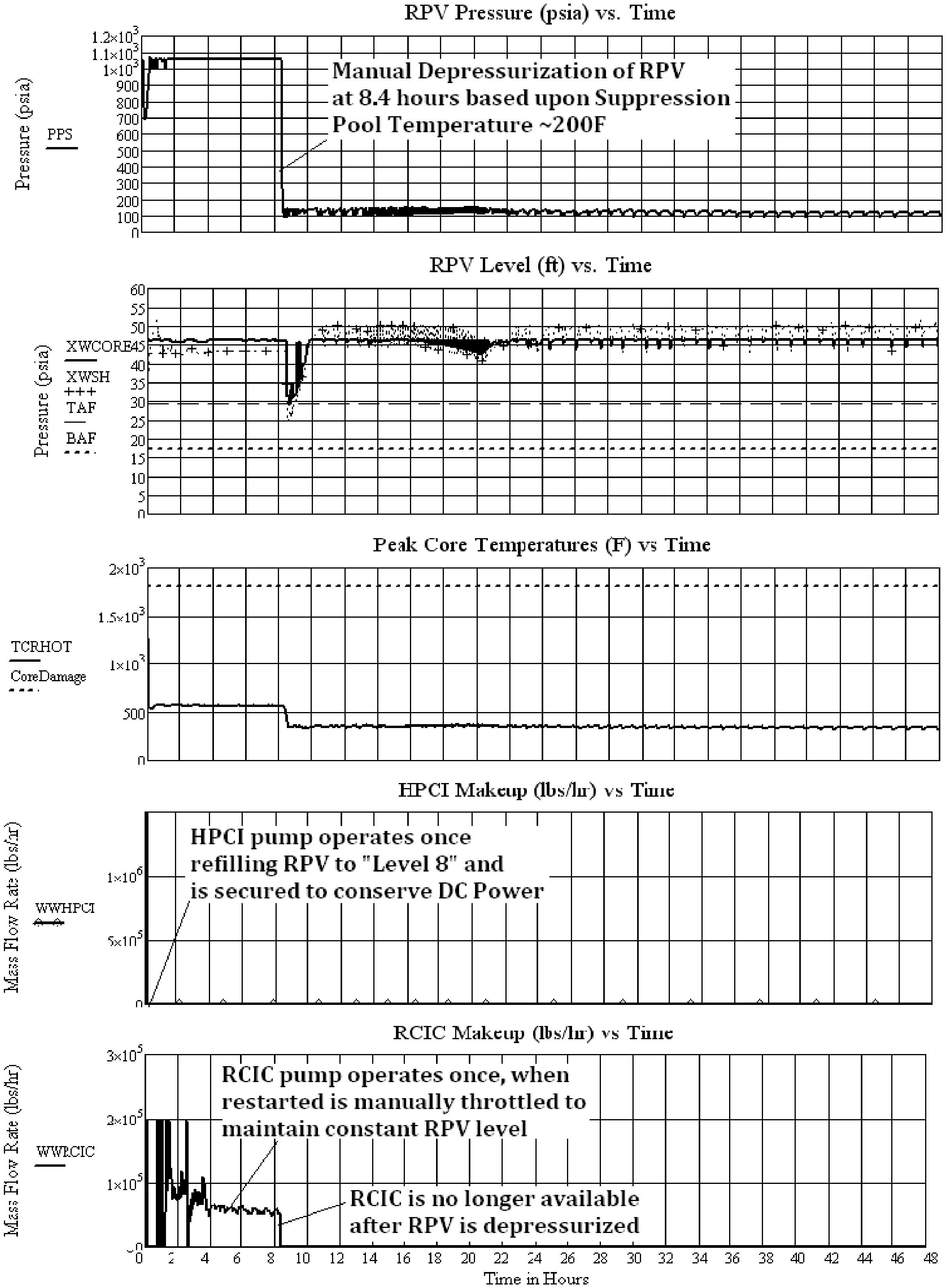


Figure 2 – Successful Mitigation Strategy for Seismic SBO using FLEX Equipment

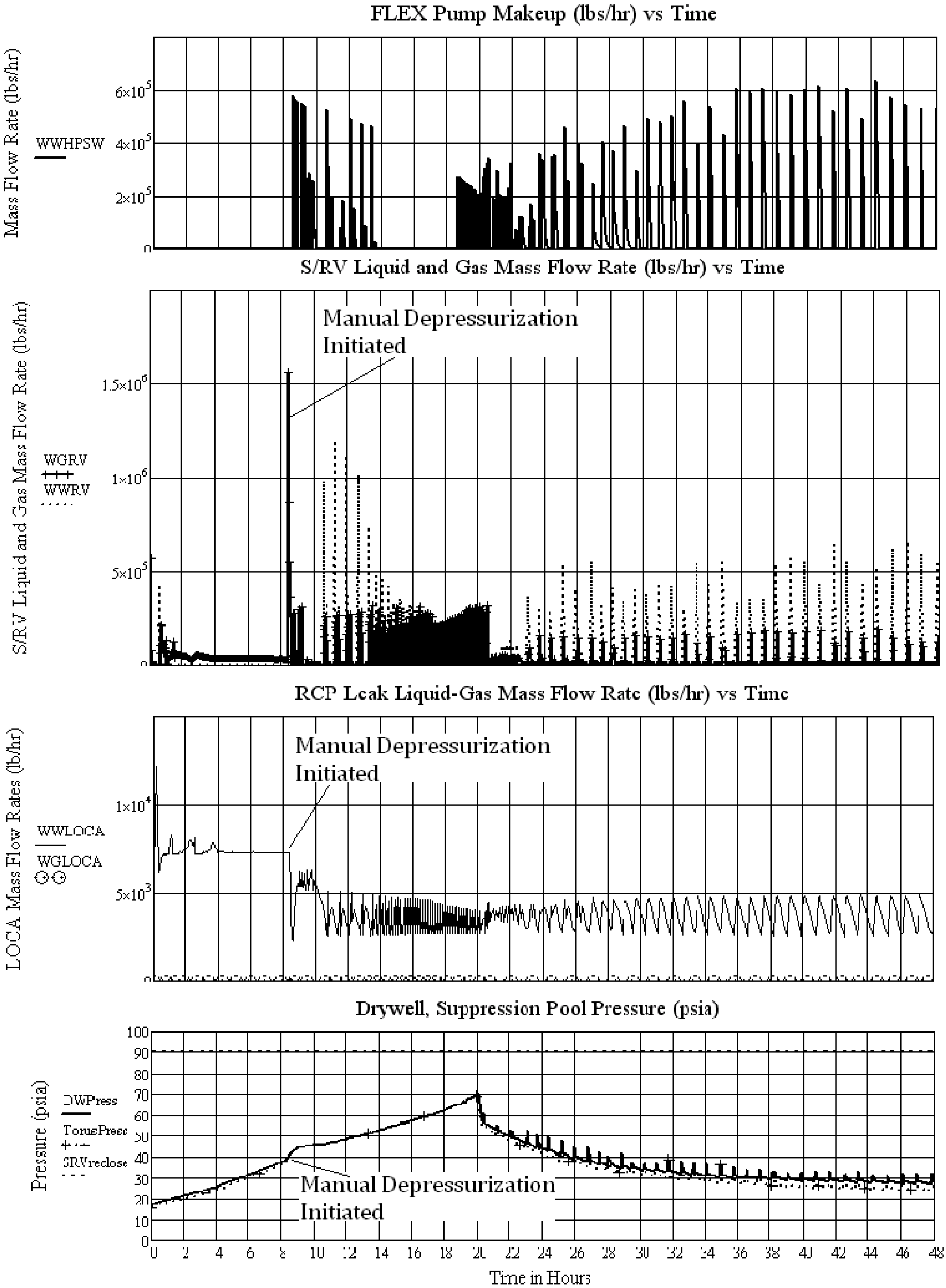
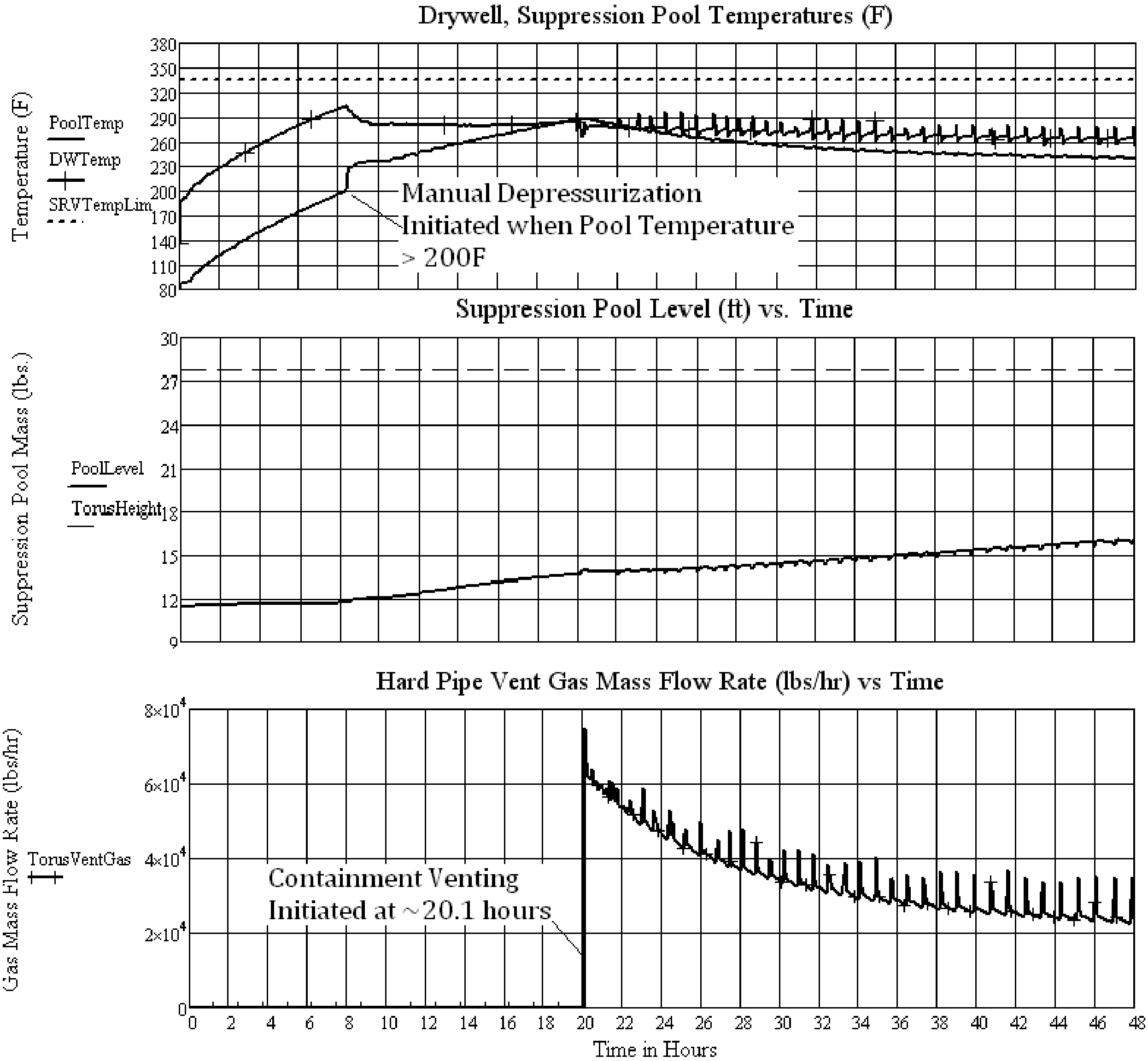
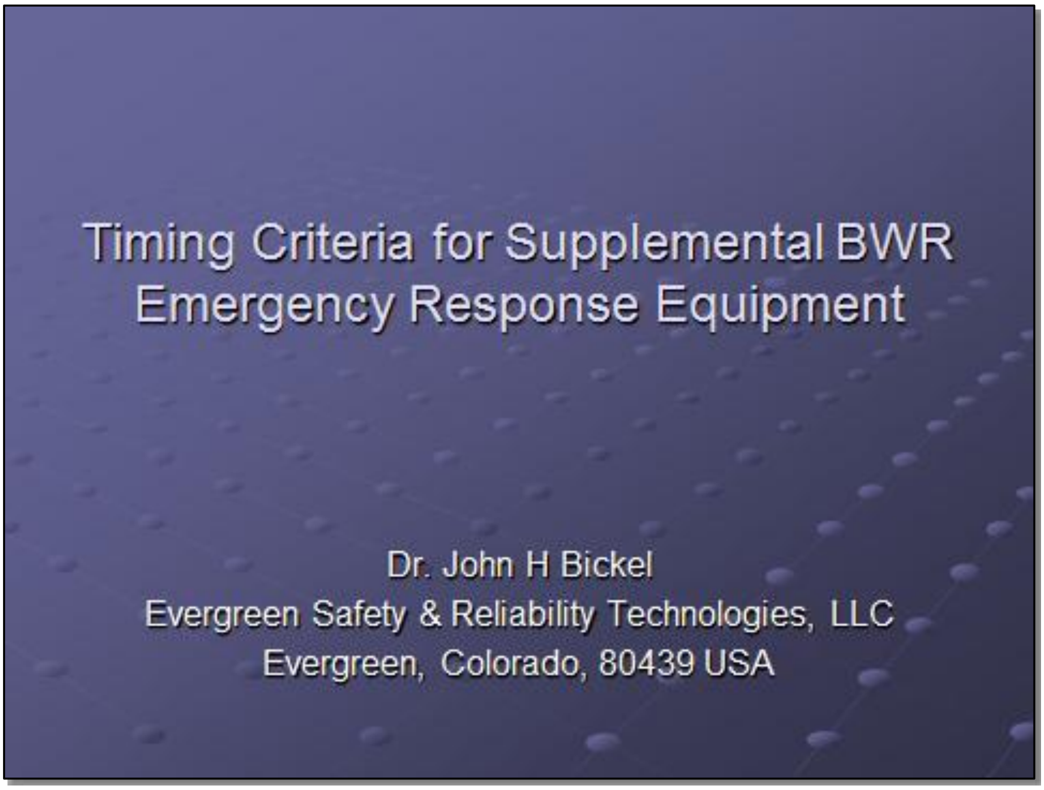
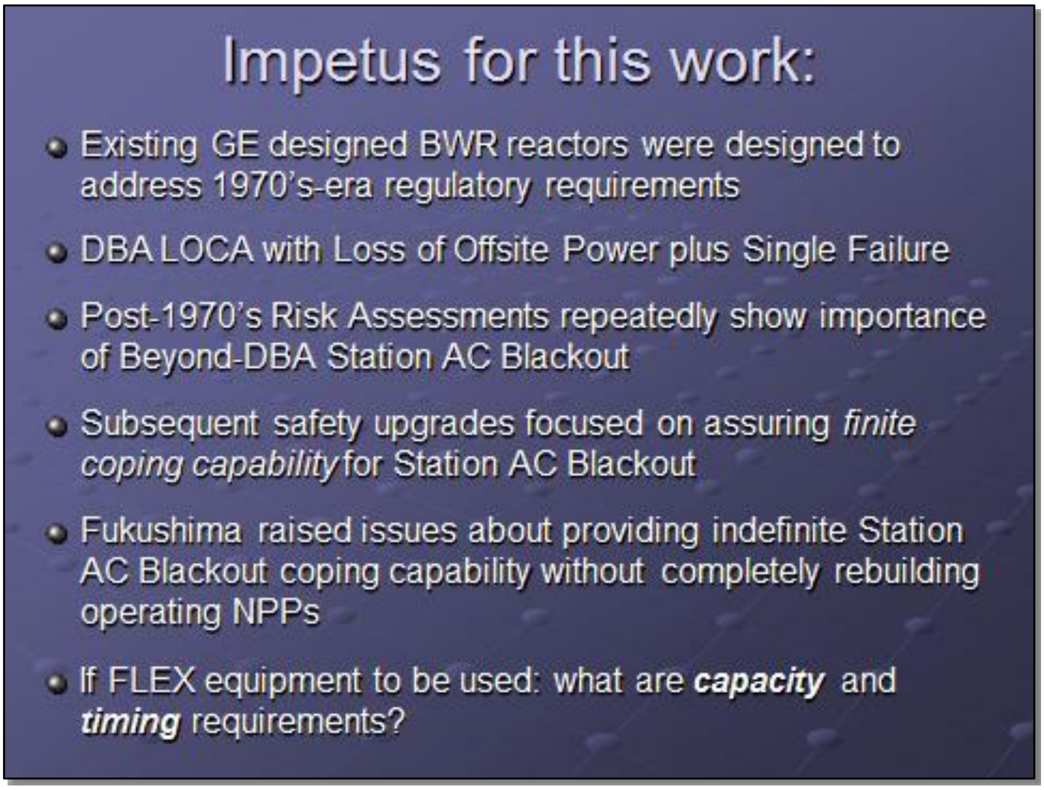


Figure 2 – Successful Mitigation Strategy for Seismic SBO using FLEX Equipment



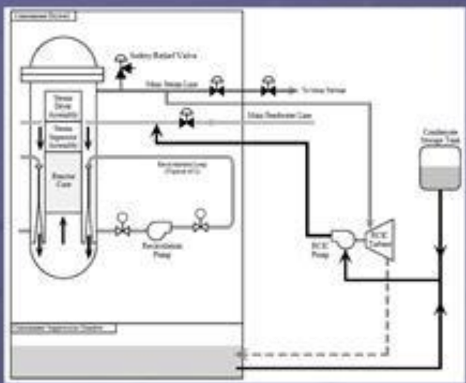

Timing Criteria for Supplemental BWR Emergency Response Equipment
Dr. John H Bickel
Evergreen Safety & Reliability Technologies, LLC
Evergreen, Colorado, 80439 USA


Impetus for this work:
Existing GE designed BWR reactors were designed to address 1970's-era regulatory requirements
DBA LOCA with Loss of Offsite Power plus Single Failure
Post-1970's Risk Assessments repeatedly show importance of Beyond-DBA Station AC Blackout
Subsequent safety upgrades focused on assuring finite coping capability for Station AC Blackout
Fukushima raised issues about providing indefinite Station AC Blackout coping capability without completely rebuilding operating NPPs
If FLEX equipment to be used: what are capacity and timing requirements?

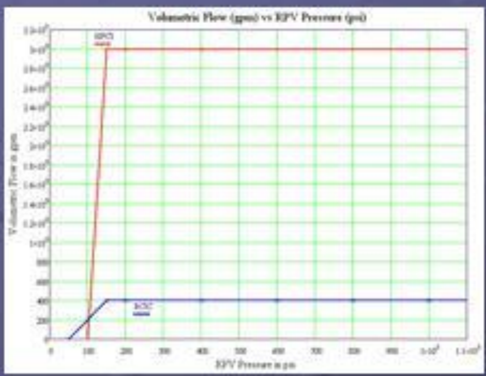
Analysis Assumptions:

- 1970's-era BWR-4 with Mark I containment
- 2000 MW thermal output
- Standard ECCS features:
  - 2x fast-starting emergency diesel generators
  - 2x 250VDC Batteries (7-8hr), 2x 125VDC Batteries (5.5-5.7hr)
  - 2x electric driven Core Spray Pumps
  - 2x electric driven Low Pressure Coolant Injection/RHR Pumps
  - 8x Safety/Relief Valves discharging to Suppression Pool
  - 1 steam driven High Pressure Coolant Injection Pump
  - 1 steam driven Reactor Core Isolation Cooling Pump
- Beyond DBA Emergency Response features:
  - Fire Water/FLEX pump cross-connection to RHR piping
  - High Pressure Containment Vent from Suppression Pool

Steam Driven RCIC Pump



High/Low Pressure Makeup:

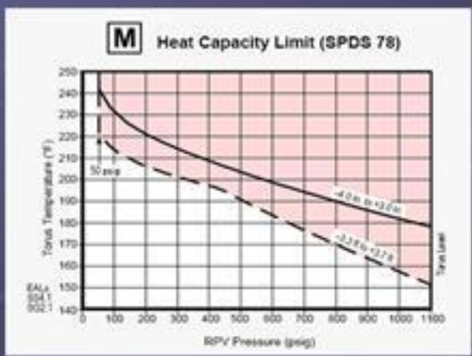


High Pressure Makeup Pumps

Low Pressure Makeup Pumps

Key timing, operability limits:

- HPCI/RCIC require:
  - 125VDC and 250VDC
  - reactor steam pressure above minimum turbine operating limits
- S/RVs require:
  - 125VDC or 250VDC,
  - N_2 gas pressure
  - Drywell temperature <325°F (S/RV qualification temperature)
  - Drywell pressure < 90 psi (N_2 pressure)
- Fire Water/FLEX Pumps and Portable Battery Charger require:
  - Fuel Supply
- Hard Pipe Containment Vent require:
  - 125VDC or 250VDC
  - N_2 gas



As Suppression Pool heats up, RPV must be depressurized

Conduct of the Analysis:

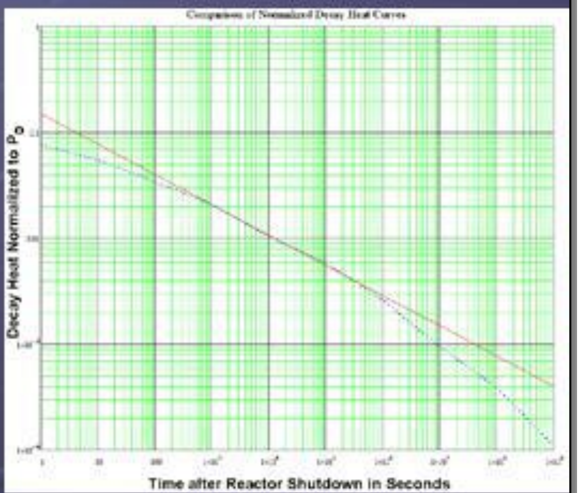
- ~80 MAAP4.0.6 long term simulations
- Small, Med., Large LOCA, RCP seal failure with SBO
- Postulated emergency response equipment success/failure
- Fire Water, Condensate Storage Tanks:
  - Non-Seismic event – no loss of integrity
  - Seismic event – assumed to fail
- Analysis used to determine maximum coping time to:
  - Restore AC power without core damage
  - Install alternate makeup water connection to RHR piping
  - Restore Battery Charging
  - Replenish bottled N_2 gas, fuel

Minimum FLEX pump requirements:

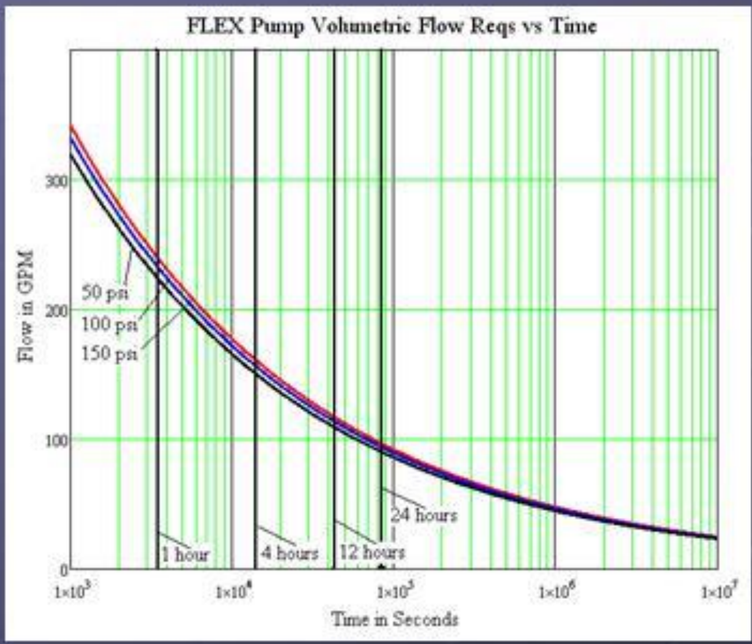
- ANS Std. 5.1 (2005) Decay Heat Model used
- Log-Log curve fit:
  $P(t) = (0.15)\ P_0\ t^{-0.286}$
- Makeup flow to match core boiloff computed:

$$W(t) = \frac{P(t)\ v_f\ (448.8gpm/ft3/sec)}{h_{fg}}$$

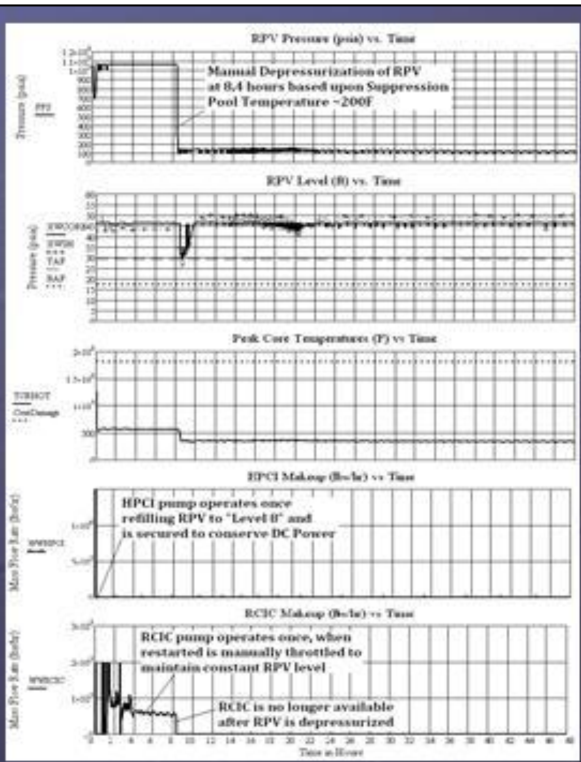
- Evaluated for various pressure, time regions

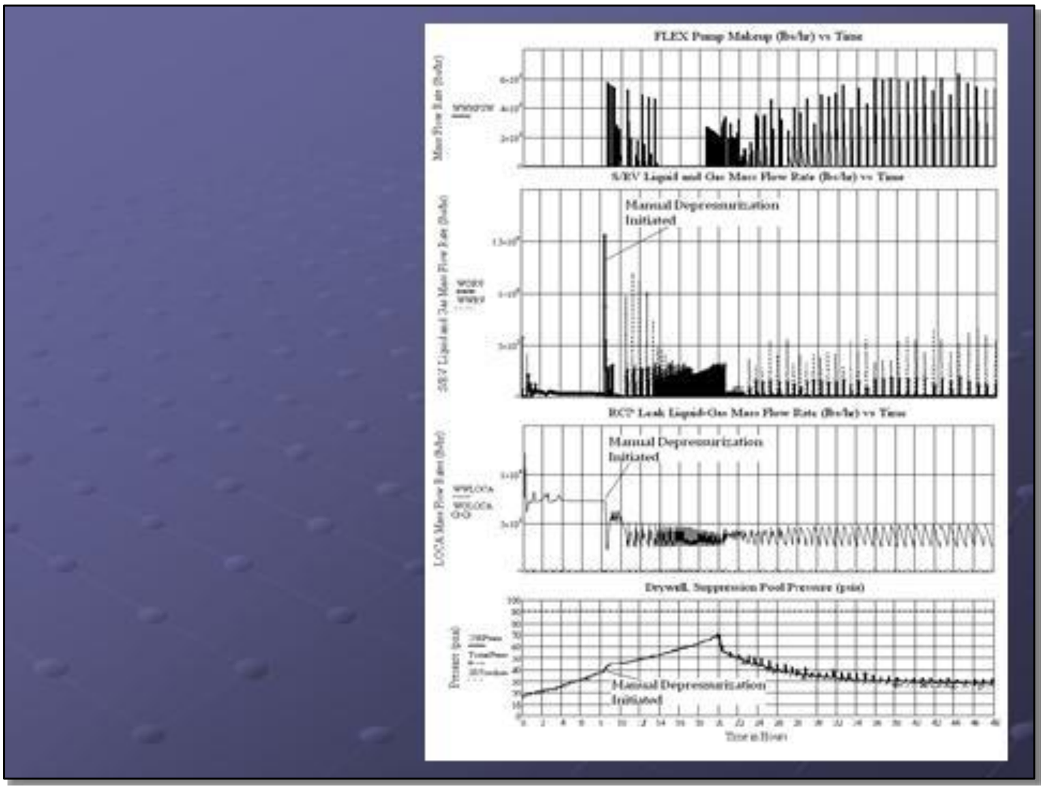


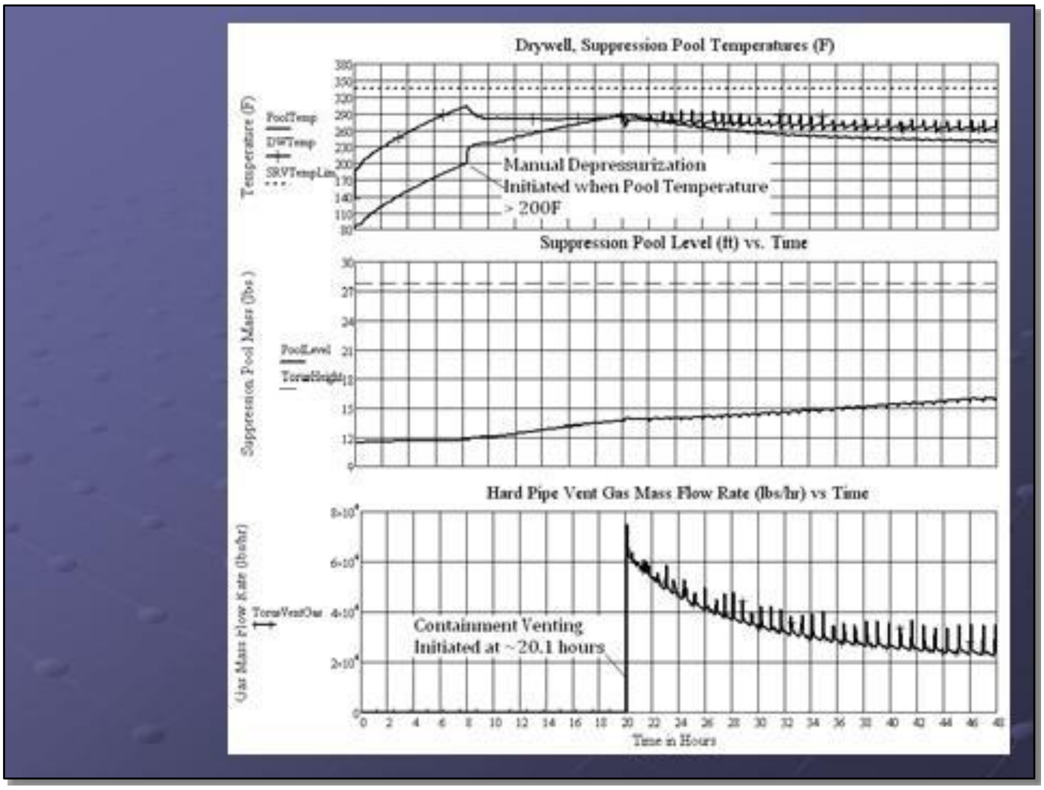
Minimum FLEX pump requirements:

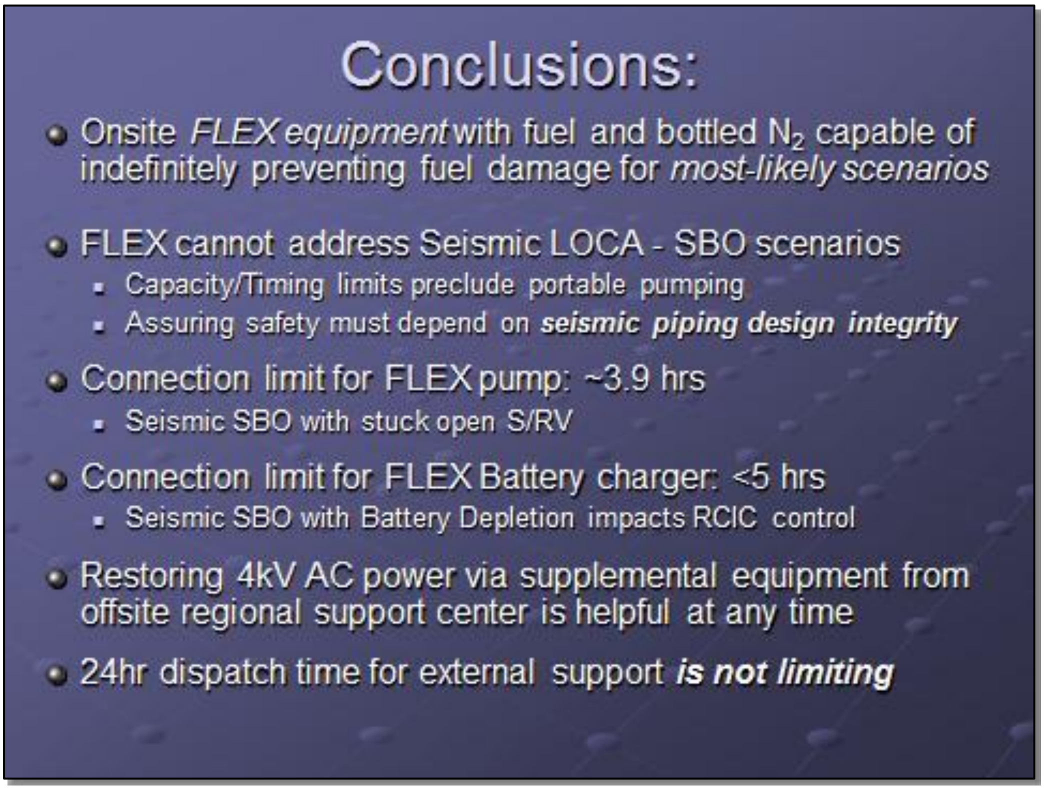


Successful mitigation of Seismic SBO using FLEX equipment




FLEX Pump Makeup (lbs/hr) vs Time
S/RV Liquid and Gas Mass Flow Rate (lbs/hr) vs Time
Manual Depressurization Initiated
RCP Leak Liquid-Gas Mass Flow Rate (lbs/hr) vs Time
Manual Depressurization Initiated
Drywell, Suppression Pool Pressure (psia)
Manual Depressurization Initiated
Time in Hours


Drywell, Suppression Pool Temperatures (F)
Temperature (F)
PoolTemp
DWTemp
SRVTempLim
Manual Depressurization Initiated when Pool Temperature > 200F
Suppression Pool Level (ft) vs. Time
Suppression Pool Mass (lbs)
PoolLevel
TorusHeight
Hard Pipe Vent Gas Mass Flow Rate (lbs/hr) vs Time
Gas Mass Flow Rate (lbs/hr)
TorusVentGas
Containment Venting Initiated at ~20.1 hours
Time in Hours


Conclusions:
Onsite FLEX equipment with fuel and bottled N_2 capable of indefinitely preventing fuel damage for most-likely scenarios
FLEX cannot address Seismic LOCA - SBO scenarios
Capacity/Timing limits preclude portable pumping
Assuring safety must depend on seismic piping design integrity
Connection limit for FLEX pump: ~3.9 hrs
Seismic SBO with stuck open S/RV
Connection limit for FLEX Battery charger: <5 hrs
Seismic SBO with Battery Depletion impacts RCIC control
Restoring 4kV AC power via supplemental equipment from offsite regional support center is helpful at any time
24hr dispatch time for external support is not limiting

Resilience improvements to UK nuclear power plants

Eur Ing Kevin Pepper B.Eng (Hons) C.Eng MIET
Office for Nuclear Regulation, United Kingdom

Abstract

Following the events at Fukushima, the Office for Nuclear Regulation (ONR), the UK nuclear safety regulator, undertook a series of reviews into the resilience of UK nuclear power plants to severe events. These reviews highlighted a number of areas in relation to electrical infrastructure where it considered licensees should review their arrangements, considering both onsite and offsite infrastructure as well as the ability to recover following a complete loss of site infrastructure.

In response, UK licensees have been exploring four parallel approaches to improving the resilience for each of their sites. Firstly, through modifications on-site such as enhancements to the installed diesel generators and related systems. Secondly through improvements to the resilience of essential instrumentation to Station Black Out events. Thirdly, through the provision of off-site backup equipment that can be deployed to any site following a severe event. Finally, the provision of event qualified connection points on site to enable timely restoration of long term essential electrical supplies and cooling to key systems. This last item gives a central focus to the issues of switchboard availability and the resilience of the whole network to large potentially common cause internal and external hazards.

This paper will discuss the electrically related findings of the ONR reviews, explore the reasoning behind those decisions, and describe the approaches being taken by UK licensees.

1. Introduction

Each Nuclear Power Plant (NPP) around the world takes an overview of its arrangements typically every ten years and reassess their plant as part of a periodic safety review process. Significant events such as those at Chernobyl in 1986 and Fukushima in 2011 act as additional triggers for the global nuclear industry to take a step back and reassess if the systems and processes in place remain appropriate.

The problems encountered on site at Fukushima Daiichi were the result of two extreme events; seismic and flooding. Whilst the electrical onsite generators were available to start and provided electrical power following the earthquake, the tsunami resulted in flooding of areas which resulted in the loss of functionality of switchboards and diesel generators. Unfortunately whilst some switchboards and some diesel generators remained available, there were no means to route power from surviving generators through switchboards to essential safety systems. It is important therefore to consider that the effects of the Fukushima events are not really about loss of diesels generators or loss of switchboards but rather the loss of the ability to supply power to essential safety functions. This is important because providing more diverse diesel generators may not help in a future event unless the whole essential electrical systems can be considered robust.

This paper summarises the reviews that have been undertaken in the United Kingdom (UK), providing some insight into the recommendations that have been made by the UK nuclear regulator, the Office for Nuclear Regulation, before providing some examples of actions being taken by the UK industry in its response.

2. Reviews overseen by ONR in the year following the events at Fukushima

In the United Kingdom (UK), immediately following the events, the Chief Nuclear Inspector of the Office for Nuclear Regulation (ONR) was requested by the UK Government to undertake a review of the events and the implications on the UK Nuclear Industry. This led to the publication of an interim report[1] in May 2011, where twenty three recommendations were made – some directed at licensees and some at UK Government and some at ONR itself. A final report[2] was published in September 2011, which took into account developing understanding as to what had occurred at Fukushima, and included an additional six recommendations. Of the total, two were focussed specifically at electrical systems ; IR-17 and IR-18.

In parallel, the Stress Test process was developed by the European Nuclear Safety Regulators Group (ENSREG) on behalf of the European Council and in December 2011, ONR assessed the UK NPP licensees own assessments against this specification and compiled the UK National Report. From the stress test review[3], nineteen stress test findings were placed on licensees where ONR considered that either the licensees' own considerations for further review or enhancement were critically important or ONR did not consider they went far enough. Four findings (STF-8 – STF-11) related to electrical systems. In addition, ONR requested non-NPP licencees and prospective NPP licensees (i.e. those linked to new NPP construction) to participate in a similar process for their sites. In May 2012, ONR assessed and reported this review[4].

3. ONR Recommendations and Findings

The follow section presents the recommendations and findings related to the power electrical aspects from each of the ONR's reports and provides insight into why it came to those conclusions.

3.1 Recommendation IR-17: The UK nuclear industry should undertake further work with the National Grid to establish the robustness and potential unavailability of off–site electrical supplies under severe hazard conditions.

Whilst loss of grid is considered a frequent event at all UK licensed sites and all licensees must have appropriate arrangements in place to ensure safe shutdown, cooling/and containment , it remains preferable to source electrical power from the offsite grid, providing such supplies remain stable and secure. It is recognised that the UK transmission network has changed over the last twenty years from the nationalised industry that existed when construction of the last nuclear power plant was started. Whilst grid reliability remains above 99.99%[5], with a changing generation mixture and major asset replacement of the transmission network underway, it was considered appropriate that licensees, with the co-operation of the

[1] Japanese earthquake and tsunami: Implications for the UK nuclear industry – Interim Report. Office for Nuclear Regulation, ONR-FR-REP-11-002 Revision 1, May 2011

[2] Japanese earthquake and tsunami: Implications for the UK nuclear industry - Final Report. Office for Nuclear Regulation, ONR-FR-REP-11-002 Revision 2, September 2011

[3] European Council "Stress Tests" for UK Nuclear Power Plants, National Final Report. Office for Nuclear Regulation, December 2011

[4] "Stress Tests" for UK non-Power Generating Nuclear Facilities, Final Report. Office for Nuclear Regulation, May 2012

[5] National Electricity Transmission System Performance Report 2012-2013, National Grid plc

transmission system operators, should review how robust the network and its ability to restore supplies are today.

3.2 Recommendation IR-18: The UK nuclear industry should review any need for the provision of additional, diverse means of providing robust sufficiently long-term independent electrical supplies on sites, reflecting the loss of availability of off-site electrical supplies under severe conditions.

The potential for long term loss of offsite power was highlighted in the events at Fukushima. This recommendation was placed on UK licensees to consider whether in light of a reassessment of potential severe hazards, additional backup supplies should be provided.

3.3 Finding STF-8: Licensees should further investigate the provision of suitable event- qualified connection points to facilitate the reconnection of supplies to essential equipment for beyond design basis events.

The events at Fukushima highlighted the potential desire following an extreme event to connect mobile generators and pumps. The connection and operation of such equipment was recognised as being difficult in conditions such as those experienced in Fukushima. This finding reflected that access around the plant following an extreme event may be very difficult. Where additional connection points to electrical systems are being proposed, this finding ensured that licensees considered their robustness against the extreme events being considered.

3.4 Finding STF-9: Licensees should further investigate the enhancement of stocks of essential supplies (cooling water, fuel, carbon dioxide, etc.) and extending the autonomy time of support systems (e.g. battery systems) that either provide essential safety functions or support emergency arrangements.

Licensees impose operational minimum capacities for fuel and water tanks on-site based upon the requirements to maintain a minimum mission time for the system in accordance with the safety case. The stress test analysis confirmed that a 72 hour minimum operation was acheiveable on these systems. Reflecting the desire to reduce the reliance on offsite support, this finding placed an action on licensees to consider whether extensions to the mission times were practicable..

3.5 Finding STF-10: Licensees should identify safety-significant prime mover-driven generators and pumps that use shared support systems (including batteries, fuel, water and oil) and should consider modifying those prime movers systems to ensure they are capable of being self-sufficient.

Fukushima serves as a reminder to the nuclear industry of the potential wide-reaching effects of common cause failures. ONR requested licensees to review all their safety significant prime-mover systems to identify any shared systems. A loss of a support system could affect the ability of multiple safety systems to perform their duty. Where such issues were identified, then licensees were requested to consider separating the systems.

3.6 Finding STF-11: Licensees should further consider resilience improvements to equipment associated with the connection of the transmission system to the essential electrical systems (EES) for severe events.

This reflected that IR-17 placed an action on licensees to review with the Transmission System Operators (TSO), the reliability and integrity of the power transmission systems, whilst other IRs and the STFs ensured that the essential on-site electrical systems were as resilient so far as is reasonably practicable. This finding ensured that licensees adequately considered improvements to the resilience of electrical equipment, such as station transformers, which connect the two systems together.

4. Licensees' Actions

All licensees have adopted a two fold response : i) immediate actions to improve the inherent resilience of the sites; and ii) long term reviews. Immediate actions have included plant walkdowns to ensure that the current arrangements such as intact or operable fire barriers, seismic housekeeping, relocation of portable equipment which could be subject to flooding, etc, are adequately enforced,.

UK, licensees set themselves a target deadline for completion of the reviews, associated with the above recommendations and findings, along with the majority of any resulting invasive implementations of the three year anniversary following the events at Fukushima, namely March 2014.

ONR will shortly be formally assessing licensees final reports on the actions implemented and the justification provided for closing out each of the recommendation and findings. However, through early engagement with licensees and monitoring of the implementation of actions taken, we understand the approaches they are taking; these can be best summarised in the case of operational power plants by the following four approaches :

1. Additional on-site emergency equipment

- Provision of small portable generators stored in a robust location to be used to support targeted instrumentation and pumps
- Additional portable de-watering pumps
- Excavators and debris removal equipment
- Satellite telephones for resilient communication to offsite locations

2. Modifications on site to existing installations to provide additional resilience

- Provision of additional flood barrier surrounding Dungeness B
- Dam boards to protect essential buildings
- Review of flood protection of cable and pipework penetrations to essential buildings
- Installation of Passive Autocatalytic Recombiners at Sizewell B

3. Provision of offsite backup equipment to be deployed to site following a severe event

- Provision of Pumps, Generators, Instrumentation, Emergency Control and Communications equipment located at strategic offsite locations
- Emergency Response Centre for Sizewell B
- Provision of suitable vehicles to transport equipment to site over rough terrain

4. Provision of event qualified connection points to support the backup equipment and longer term restoration
- Identification of essential systems requiring restoration (water, CO_2, electrical)
  - Identification of resilient connection points against postulated hazards with significant margins
- Suitably routed and resilient connections

Summary

The problems encountered on site at Fukushima Daiichi were the result of two extreme events; seismic and flooding. It is important to note that the effects of the Fukushima events are not about the loss of diesels generators or loss of switchboards but were a combination of both these factors that lead to the loss of the ability to supply power to essential safety functions. This is an important point since additional diesel generators on their own may not solve the problem.

The Office for Nuclear Regulation in the UK has undertaken a series of assessments of UK NPPs with the co-operation of the UK licensees. These highlighted a number of areas where ONR recommended UK licensees should consider further review. UK NPP licensees have taken the lessons learned from Fukushima and combined with the activities taken to address ONR recommendations are taking action to improve the resilience of the UK nuclear power plants. This is being achieved through both modifications on-site and the provision of off-site backup equipment.

Office for Nuclear Regulation

Resilience Improvements to UK Nuclear Power Plants

Eur Ing Kevin Pepper CEng MIET

Background

- Initiating event
- Reviews / Assessment undertaken by ONR
- Recommendations / Findings
- Actions being taken by Licensees

Office for Nuclear Regulation

Initiating Event

- Fukushima event of 11 March 2011
  - Severe seismic event
  - Severe flooding event
- Loss of ability to supply power to essential safety functions
  - Generation
  - Switchboards
  - DC support systems

Office for Nuclear Regulation

ONR Reviews and Assessments

- "Japanese earthquake and tsunami: Implications for the UK nuclear industry"
  - Interim Report (May 2011)
  - Final Report (September 2011)
- "European Council "Stress Tests" for UK nuclear power plants – National Final Report " (December 2011)

Office for Nuclear Regulation

Recommendations and Findings

- Six areas for consideration in respect of electrical systems identified from these reports
- Two Recommendations
  - Derived from the Interim Report
- Four Stress Test Findings
  - Derived from the European Council Report

Office for Nuclear Regulation

Recommendation IR-17

The UK nuclear industry should undertake further work with the National Grid to establish the robustness and potential unavailability of off–site electrical supplies under severe hazard conditions.

Office for Nuclear Regulation

Recommendation IR-17

- Reflecting changes
  - network ownership
  - generation mix
- Consider the events system is resilient against
- Consider the mitigating action that could be taken and how well rehearsed this is

Office for Nuclear Regulation

Recommendation IR-18

The UK nuclear industry should review any need for the provision of additional, diverse means of providing robust sufficiently long-term independent electrical supplies on sites, reflecting the loss of availability of off-site electrical supplies under severe conditions.

Office for Nuclear Regulation

Recommendation IR-18

- Following reassessment of sites against severe events
- Consider if additional diverse on-site electrical backup supplies are required
- Could be targeted at specific functions – pond cooling, alternative indication centres, etc.

Office for Nuclear Regulation

Stress Test Finding STF-8

Licensees should further investigate the provision of suitable event-qualified connection points to facilitate the reconnection of supplies to essential equipment for beyond design basis events.

Office for Nuclear Regulation

Stress Test Finding STF-8

- Facilitate connection to systems important to safety that may be difficult to access during or following an event
- For external connections important to consider :
  - Events during/after which they need to be available
  - Sufficient margin against the hazard being considered

Office for Nuclear Regulation

Stress Test Finding STF-9

Licensees should further investigate the enhancement of stocks of essential supplies (cooling water, fuel, carbon dioxide, etc.) and extending the autonomy time of support systems (e.g. battery systems) that either provide essential safety functions or support emergency arrangements.

Office for Nuclear Regulation

Stress Test Finding STF-9

- Review the appropriateness of minimum operational levels in light of
  - Access and supply difficulties post event
  - Nature of the system being supplied
  - Resilience of the storage

Office for Nuclear Regulation

Stress Test Finding STF-10

Licensees should identify safety-significant prime mover-driven generators and pumps that use shared support systems (including batteries, fuel, water and oil) and should consider modifying those prime movers systems to ensure they are capable of being self-sufficient.

Office for Nuclear Regulation

Stress Test Finding STF-10

- Recognising the potential for Common Cause Failure to affect diverse plant
- Ensure that independence of essential supply equipment is maximised

Office for Nuclear Regulation

Stress Test Finding STF-11

Licensees should further consider resilience improvements to equipment associated with the connection of the transmission system to the essential electrical systems (EES) for severe events.

Office for Nuclear Regulation

Stress Test Finding STF-11

- Review the resilience of the connection between the transmission network and essential on-site electrical system

Office for Nuclear Regulation

Licensees' Actions

- Both NPP licensees in the UK have taken:
  - Immediate actions
  - Undertaken reviews and improvements long term
- NPPs imposed a deadline of three years after the events at Fukushima for the longer term reviews and majority of improvements to be completed

Office for Nuclear Regulation

Licensee Short Term Actions

- Examples of actions include :
  - Deployment to sites of additional debris removal equipment
  - Provision of additional portable generators
  - Relocation of support equipment to higher ground
  - Walkdowns to ensure fire and seismic housekeeping in order

Office for Nuclear Regulation

Licensee Long Term Actions

- Additional onsite emergency equipment
- Modifications on site to existing installations
- Provision of offsite backup equipment to be deployed to site following a severe event
- Provision of event qualified connection points to support the backup equipment and longer term restoration

Office for Nuclear Regulation

Additional onsite emergency equipment

- Provision of small portable generators stored in a robust location to be used to support targeted instrumentation and pumps
- Additional portable de-watering pumps
- Excavators and debris removal equipment
- Satellite telephones for resilient communication to offsite locations

All images courtesy of EDF Energy Nuclear Generation Ltd

Office for Nuclear Regulation

Modifications on site to existing installations

- Provision of additional flood barrier surrounding Dungeness B
- Dam boards to protect essential buildings
- Review of flood protection of cable and pipework penetrations to essential buildings
- Installation of Passive Autocatalytic Recombiners at Sizewell B

Office for Nuclear Regulation

Provision of additional flood barrier surrounding Dungeness B

Office for Nuclear Regulation

Dam boards to protect essential buildings

Office for Nuclear Regulation

Installation of Passive Autocatalytic Recombiners at Sizewell B

Office for Nuclear Regulation

Provision of offsite backup equipment to be deployed to site following a severe event

- Provision of Pumps, Generators, Instrumentation, Emergency Control and Communications equipment located at strategic offsite locations
- Dedicated Emergency Response Centre for Sizewell B
- Provision of suitable vehicles to transport equipment to site over rough terrain

Office for Nuclear Regulation


Provision of offsite backup Equipment
Nuclear Regulation


Strategic Offsite Locations
Office for
Nuclear Regulation

Provision of event qualified connection points to support the backup equipment and longer term restoration

- Identification of essential systems requiring restoration (water, CO_2, electrical)
- Identification of resilient connection points against postulated hazards with significant margins
- Suitably routed and resilient connections

Office for Nuclear Regulation

Provision of Resilient Electrical Connection

Office for Nuclear Regulation

Summary

- ONR has undertaken a number of reviews of UK resilience to extreme events at the request of:
  - UK Government
  - European Council
- In relation to electrical systems, ONR identified a number of recommendations and findings
- UK licensees have and continue to take action to ensure their sites and systems are robust against a range of extreme events

Office for Nuclear Regulation

Any Questions?

Email : kevin.pepper@onr.gsi.gov.uk

Office for Nuclear Regulation

Emergency Mitigating Equipments – Post Fukushima Actions at Canadian Nuclear Power Plants – Portable AC Power Sources

J. Vucetic and R. Kameswaran
Canadian Nuclear Safety Commission, Canada

Abstract

In response to the Fukushima Daiichi NPP accident in 2011, the Canadian Nuclear Safety Commission set up a Task Force to evaluate operational, technical and regulatory implications on Canadian NPPs. While accepting that the risk from beyond-design-basis accidents (BDBA) at Canadian NPPs is very low, the Task Force identified a number of areas where additional improvements or confirmatory assessments would further enhance safety.

As a result, a set of 36 Fukushima Action Items (FAIs) were assigned to the licensees.

This paper focuses on the FAI related to electrical power system enhancements to address a total loss of all AC Power leading to a possibility of loss of heat sinks (i.e. Station Blackout). This required the licensees to implement the following:

- Additional back up power supplied by portable diesel generator(s) to allow key instrumentation and control equipment and key electrical loads to remain operable;
- Provisions for a storage and timely transportation and connection of the portable generator(s) to the applicable units ;
- Provisions for testing of the portable generator;
- Provisions for fuelling of portable generators;
- Provisions such as panels, receptacles, and connectors to quickly deploy the portable generators to plant system, and separate feeder cables route to avoid a common mode failure;
- Load shedding strategy to extend the existing station's battery life to ensure that the connection of portable generators can be completed before the batteries are depleted;
- Provisions to supply water to steam generators and Irradiated Fuel Bay using portable pumps;

The paper will also provide a brief description of Electrical power systems of the Canadian NPPs designed to satisfy the high safety and reliability requirements for nuclear systems, which are based on the following:

- 2 group design philosophy (Group 1 and Group 2 Electrical Power Systems)
- 2 separate groups of onsite emergency generators (Class III Standby generators and Emergency Power generators)
- 4-7 days' supply of fuel for standby and emergency generators,
- The capability to transfer power between units in a multi-unit plant

1. Introduction

Canada has five Nuclear Power Plants (NPPs) in three provinces that houses 22 CANDU reactors; 20 located in Ontario at three multi-unit stations ; Pickering, Darlington and Bruce. There are also single-unit CANDU stations in Gentilly, Québec and Point Lepreau, New Brunswick. All currently operating reactors are CANDU (Canadian Deuterium –uranium) reactors.

Following the Fukushima Daiichi nuclear accident, the Canadian Nuclear Safety Commission (CNSC) requested all the Canadian Nuclear Power Plants (NPPs) to conduct a review of the initial lessons learned from Fukushima, under subsection 12(2) of the General Nuclear Safety and Control Regulations. In April 2011, the CNSC convened a task force to review the licensees' responses to the 12(2) request and evaluate the operational, technical and regulatory implications of the Fukushima Daiichi nuclear accident for the Canadian NPPs. While acknowledging that the probability of a beyond-design-basis accident (BDBA) at Canadian NPPs is very low, the Task Force identified a number of areas where additional improvements would further enhance safety. To address the Task Force recommendations, the CNSC developed a draft CNSC Action Plan. The document established a four-year plan, for both licensees and CNSC staff, to strengthen reactor defence in depth, enhance emergency response, improve regulatory oversight and crisis communication capabilities, and enhance international collaboration.

In parallel to the task force the President of the CNSC established an External Advisory Committee (EAC) to review the CNSC's process in responding to the Fukushima crisis and in developing proposed changes to its processes and regulatory framework. The EAC concluded that the process followed by the CNSC in response to the accident was appropriate, and identified a number of complementary areas for further enhancements.

CNSC Staff Action Plan was developed taking into consideration the comments received from the public and stakeholders on the CNSC Fukushima Task Force (FTF) Report. The CNSC Staff Action Plan identified a number of actions to address the Task Force Report recommendations. The actions are grouped in the following three categories:

– Strengthening reactor defence in depth
– Enhancing emergency response
– Improving regulatory framework and processes

This paper discusses the findings, and recommendations of the FTF with respect to the strengthening of defence in depth of CANDU Electrical Power Systems (EPS).

2. CANDU Electrical Power Systems Design

CANDU EPS is designed to satisfy the high safety and reliability requirements of the nuclear power plants. Notably, this is achieved through grouping and separation.

2.1 Group Separation

The concept of grouping and separation of safety related systems has been integral to CANDU plants. This concept provides physical and functional separation of safety related systems to ensure that common cause events do not impair the capability to perform essential safety functions. In this concept, the plant can be shut down, decay heat removed, and the plant conditions monitored independently from systems and components of either one of two groups, known as Group 1 and Group 2. The EPS is separated into Group 1 and Group 2 in accordance with the two groups' separation philosophy. Group 2 power is qualified to operate following the design basis common-mode events.

2.2 Division Separation

The design provides two electrically independent and physically separated power distribution divisions. One is designated odd, the other even. The two divisions provide power to redundant station loads and prevent failures or damage of one divisions cascading to the other.

2.3 Classes of Power

There are four distinct classes of power, namely Class IV, III, II and I, as well as Emergency Power Supply. Class IV, III, II and I are Group 1 supplies while Emergency Power Supply is Group 2 power.

The Class IV power system is an AC power that supplies the unit auxiliary loads during normal plant operation. The Class IV power can be supplied from the turbine generator or from the off-site power and may be subject to long term interruptions. Under certain circumstances the loads may be transferred from one source to others. The class IV distribution arrangement is a radial dual bus scheme (i.e. Class IV is split into two divisions; even and odd. CANDU turbine generators units are designed to survive 100 % load rejection from the external grid and continue to supply their own house load. Most of the CANDU reactors are capable of quickly reducing reactor power to 60 % of full power, holding at reduced power, and then returning more slowly to full power using their adjuster rods. The reactors have provisions to dump the steam to condenser and can remain at 60 % full power indefinitely ready for reconnection to the grid or for an orderly shut down. The unit electrical output would be held to around 10-15 % full power to supply the house loads.

Class III power is an AC system that is normally supplied from the Class IV system. Upon loss of Class IV power it is automatically supplied from on-site stand-by generators (SGs) under the control of the emergency transfer scheme (ETS). Each SG is capable of black starting and supplying the Class III requirements. The SGs are provided with an on-site fuel oil supply. Uninterruptible control power required for switching and monitoring following loss of Class IV and until Class III restoration is provided from Class I and II.

Class II is an AC system which supplies uninterruptible AC power to the essential loads, which cannot tolerate power interruptions that may occur in the Class III system. The Class II power is normally supplied from Class I batteries through inverters with alternate supply from the Class III system.

The Class I is a DC system which supplies uninterruptible DC power to the essential auxiliary services. Class I power is normally supplied from Class III power through rectifiers and is backed up by batteries to ensure uninterruptible supply to Class I and Class II loads. The overall system requirement is that if AC supplies fail than the battery will supply the emergency loads without interruption for the required time. Batteries are capable of providing uninterruptible power to the full Class II and Class I loads for a minimum period of 40 minutes following a total loss of Class III and IV power. After this time, all class I and II loads will be lost if class III power cannot be restored. Table – 1 summarizes the attributes of classes of power.

Table 1 – Classes of power in a CANDU Nuclear Power Plant

RELIABILITY	Class IV	• Normal Alternating Current (AC) – Supplied from turbine generator and/or grid
	Class III	• AC system – Normally supplied from Class IV – Upon loss of Class IV, from Standby generator
	Class II	• AC System – Normally supplied form Class I DC system – Can be supplied from Class III
	Class I	• DC system – Normally supplied from Class III via rectifiers – Backup battery supply

2.4 The Emergency Power Supply

Emergency Power Supply is a separate power system consisting of its own on-site power generation and AC and DC power distribution, including batteries. Emergency Power Supply is the Group 2 power. The purpose of Emergency Power Supply is to provide power to selected nuclear safety-related loads following a common-mode incident such as earthquake, should all the Group 1 supplies fail. The whole Emergency Power Supply is seismically qualified to withstand a design basis earthquake. Two Emergency Power Generators (EPGs) are provided, each capable of black starting and supplying the minimum power requirements for safe plant shutdown. The EPGs are required to be manually started within 30 minutes of the occurrence of a common-mode event. Figure 1 Block diagram illustrating typical separation of Class I, II, III and IV electrical systems into independent divisions with a separate emergency power supply.

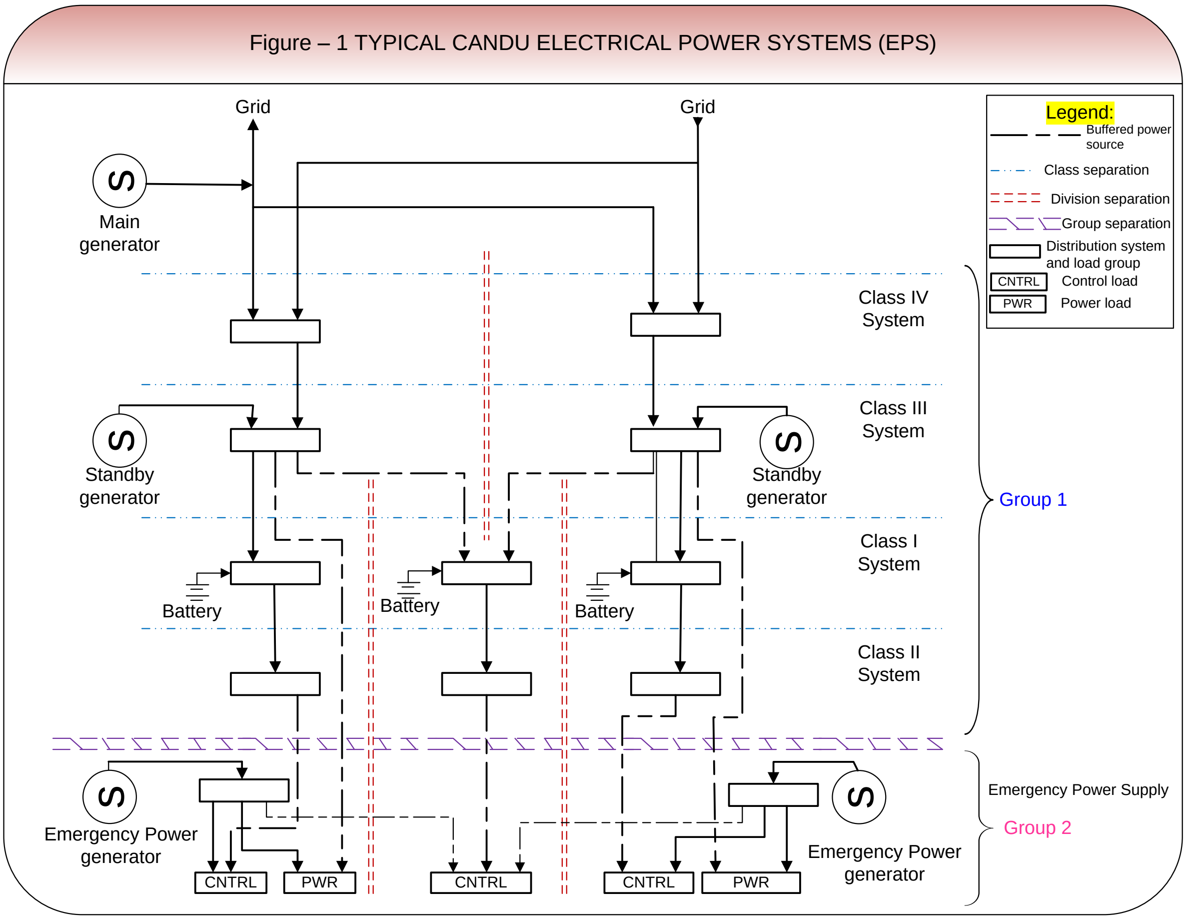


Figure – 1 TYPICAL CANDU ELECTRICAL POWER SYSTEMS (EPS)

3. Lessons learned from Fukushima

The lessons learnt from Fukushima required the licensees to analyze station capability to respond to the Station Blackout (SBO).The CNSC also reviewed the level of preparedness of Canadian NPPs to respond to a sustained SBO event. Immediately after the Fukushima event, the CNSC staff performed walkdowns at Canadian NPPs to verify the licensees' emergency preparedness for external hazards and severe accidents so that the CNSC could reassure the Commission and Canadian public that certain aspects that had contributed to the events in Japan had been specifically verified. One of the aspects verified was availability of backup power.

3.1 Fukushima Task Force Findings

A major class of beyond-design-basis accidents are those involving a loss of all heat sinks. The most challenging of these are caused by loss of electrical power. The Fukushima Daiichi accident was of this type and was the focus of the CNSC Fukushima Task Force (FTF).

One of the focus areas of FTF review was strengthening reactor defence in depth. In the event of a loss of all normal, backup and emergency AC power the batteries are the only electrical stored energy source available. However, they will be depleted in approximately 40 minutes. After that time, most control and instrumentation functions such as reactor start up monitoring, containment parameter monitoring, lighting, motorized valve operation etc, will be lost unless an alternative power source is established well before the batteries are depleted.

3.2 Fukushima Action Items

The CNSC Task Force found that licensees should explore options to extend the duration of power supplies to instrumentation and control equipment that may be needed to mitigate beyond-design-basis accidents, including severe accidents. Consequently, all licensees have performed an evaluation to determine if the 40 minute mission time for batteries can be extended to at least 8 hours. This time is required between total loss of AC power and connection of additional power sources i.e. the portable generators.

Fukushima Action Item (FAI) 1.10 required all licensees to investigate means of extending the availability of power for key instrumentation and control (I&C) needed in accident management actions following a loss of all AC power.

FAI 1.11 required all licensees to procure, as quickly as possible, emergency mitigating equipment (EME) and other resources that could be stored offsite and brought onsite to mitigate a severe accident. EME consists of portable generators, portable UPS, cables, receptacles, panels, portable diesel driven pumps and fire hoses.

3.3 Implementation of Action Items

Deliverables of FAI 1.10 implementation required the licensees to evaluate the requirements and capabilities of electrical power for key instrumentation and control (I&C). Licensees were asked to identify practicable upgrades that would extend the availability of key I&C, if needed. Licensees were asked to present a plan and schedule for deployment of identified upgrades. A target of 8 hours without the need for offsite support was required.

Deliverables of FAI 1.11 implementation required the licensees to provide a plan and schedule for procurement of emergency equipment and other resources that could be stored offsite and brought onsite to mitigate a severe accident.

To comply with the CNSC requirements the following actions were performed by the licensees:

– Operational guides were developed for shedding of non-priority Class 1 and 2 loads to extend the battery discharge time.

– Station specific list of priority loads was developed which should powered by portable generators[6] / portable uninterruptable power supplies (UPS)

– Calculated the extended life of the batteries after load shedding to ensure that it exceeds the time required to deploy and connect the portable generators.

– Procured and deployed portable generators / portable UPS. The size and number of portable generators/UPS is site specific. In addition to the above, the panels, receptacles, and cable/connectors to quickly deploy the portable generators to unit systems are also site specific.

[6] Some stations have provisions to rapidly deploy Portable UPS for key I&C followed by the AC portable generators.

- Confirmed through tests/drills that there is sufficient time to invoke the load shedding strategy and extend the battery life prior to deploying, connecting and operating the portable generators / portable UPS.
- Developed a number operational and maintenance guidelines for deployment of EME equipment.
- Developed and provided training for the Emergency Response Team personnel.
- Built EME storage facility near the station to house the EME equipment.
- The lessons learned during the tests/drills were used to improve the emergency response time during a total loss of AC power event

4. Conclusion

Fukushima Task Force review acknowledged that the probability of a BDBA at a Canadian NPPs is very low. However CNSC staff identified a number of areas where additional improvements would further enhance safety. Implementation of the action items has strengthened the defence in depth. Among other improvements this has resulted in an enhancement of the already robust CANDU EPS. It has been confirmed that the essential safety functions such as control, cool, contain and monitor will be maintained during a SBO event. Fukushima events led the CNSC to consider enhancing the regulatory requirements of EPS which includes requirement for Alternate AC power. This requirement has been included in the draft REGDOC 2.5.2 which will replace the current regulatory document RD-337.

References:

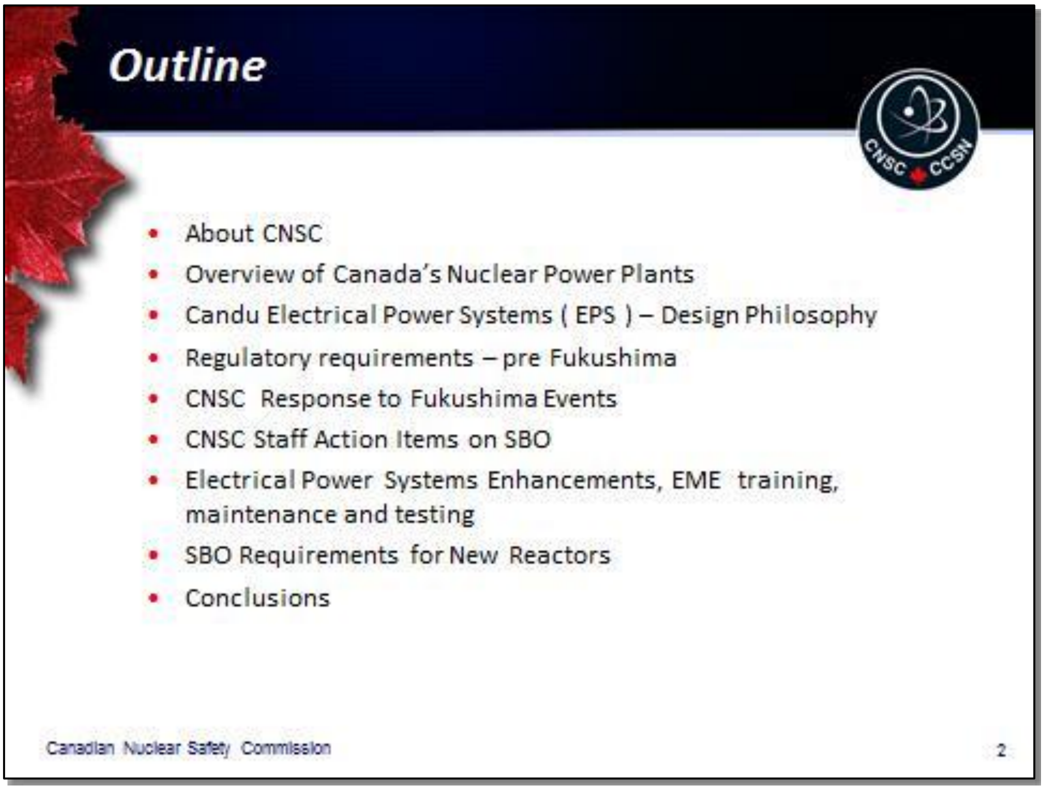
1. CNSC Fukushima Task Force Report, CNSC INFO-0824
http://nuclearsafety.gc.ca/pubs_catalogue/uploads/October-2011-CNSC-Fukushima-Task-Force-Report_e.pdf

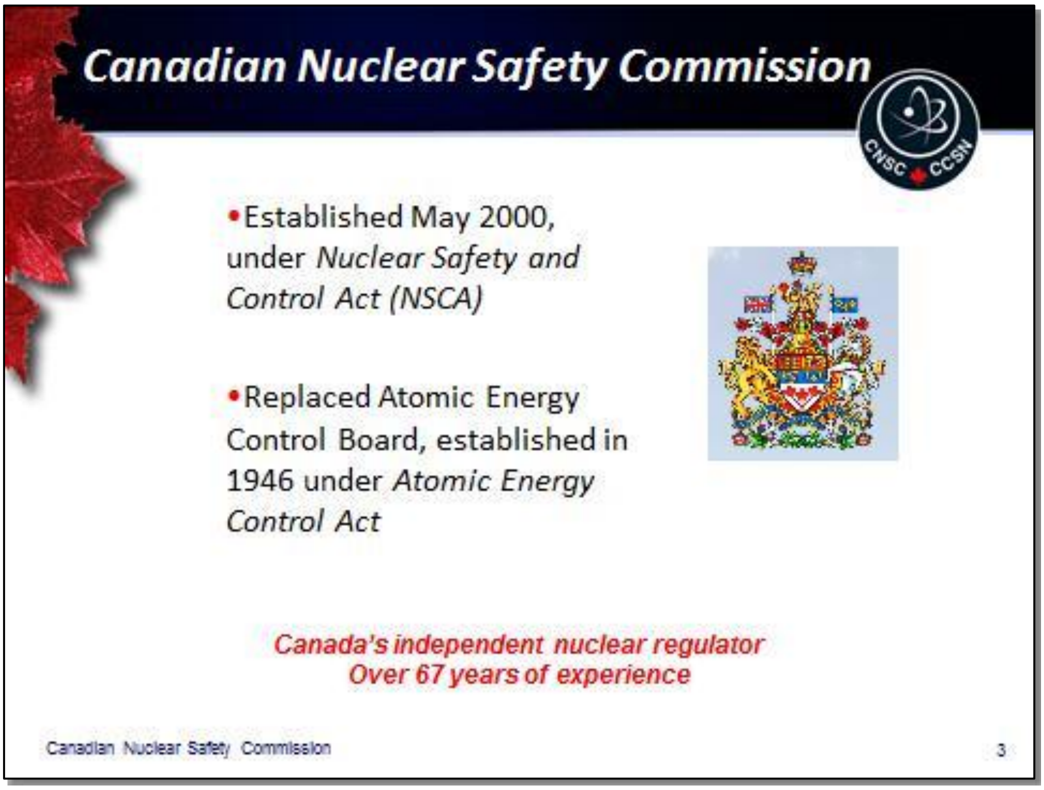
2. CNSC Management Response to the CNSC Fukushima Task Force Recommendations, INFO-0825, http://nuclearsafety.gc.ca/pubs_catalogue/uploads/October-2011-Management-Response-to-Fukushima-Task-Force-Report_e.pdf

3. CNSC Staff Action Plan on the CNSC Fukushima Task Force Recommendations INFO-0828
http://www.nuclearsafety.gc.ca/pubs_catalogue/uploads_unapproved/REVISED-INFO-0828-Draft-CNSC-Staff-Action-Plan-on-Fukushima-Dec-2011_e.PDF

4. CNSC REGDOC-2.5.2 Physical design: design of reactor Facilities: Nuclear Power plants (Draft) [Former RD-337]
http://nuclearsafety.gc.ca/pubs_catalogue/uploads/RD-337_e.pdf

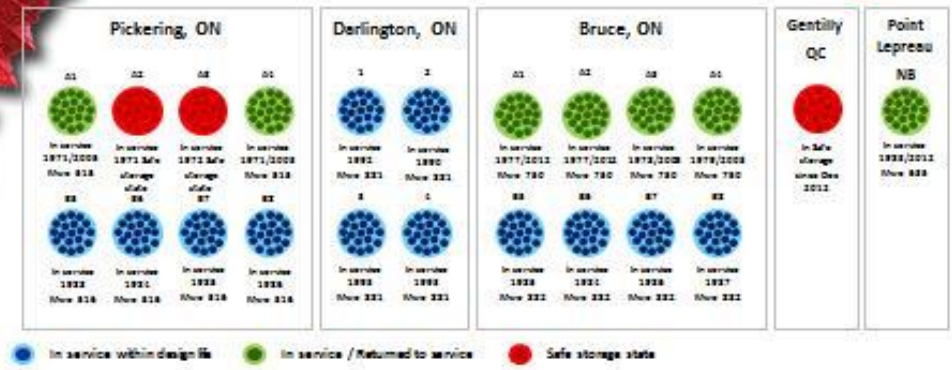

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire
CNSC CCSN
Emergency Mitigating Equipments
Post Fukushima actions at Canadian NPPs
Portable AC power sources
Presented by Jasmina Vucetic
nuclearsafety.gc.ca
Presented at the CSNI International Workshop on Robustness of Electrical Systems of NPPs in Light of the Fukushima Dai-Ichi Accident
Paris, April 1-3, 2014
Canada


Outline
CNSC CCSN
About CNSC
Overview of Canada's Nuclear Power Plants
Candu Electrical Power Systems (EPS) – Design Philosophy
Regulatory requirements – pre Fukushima
CNSC Response to Fukushima Events
CNSC Staff Action Items on SBO
Electrical Power Systems Enhancements, EME training, maintenance and testing
SBO Requirements for New Reactors
Conclusions
Canadian Nuclear Safety Commission
2


Canadian Nuclear Safety Commission
CNSC CCSN
•Established May 2000, under *Nuclear Safety and Control Act (NSCA)*
•Replaced Atomic Energy Control Board, established in 1946 under *Atomic Energy Control Act*
Canada's independent nuclear regulator
Over 67 years of experience
Canadian Nuclear Safety Commission
3


CNSC Mission
CNSC CCSN
• To regulate the use of nuclear energy and materials so that the health, safety and security of Canadians and the environment are protected, and to implement Canada's international commitments on the peaceful use of nuclear energy.
• Canada's nuclear watchdog
Canadian Nuclear Safety Commission
4

Canada's Nuclear Power Plants



- 5 Stations in 3 Provinces
- 22 CANDU Reactors

Canadian Nuclear Safety Commission 5

Pickering Nuclear Power Plant

- Multi-unit station (8 units)
- Six units in operation
- Units #2 and #3 under safe storage

Canadian Nuclear Safety Commission 6

Bruce Nuclear Power Plant

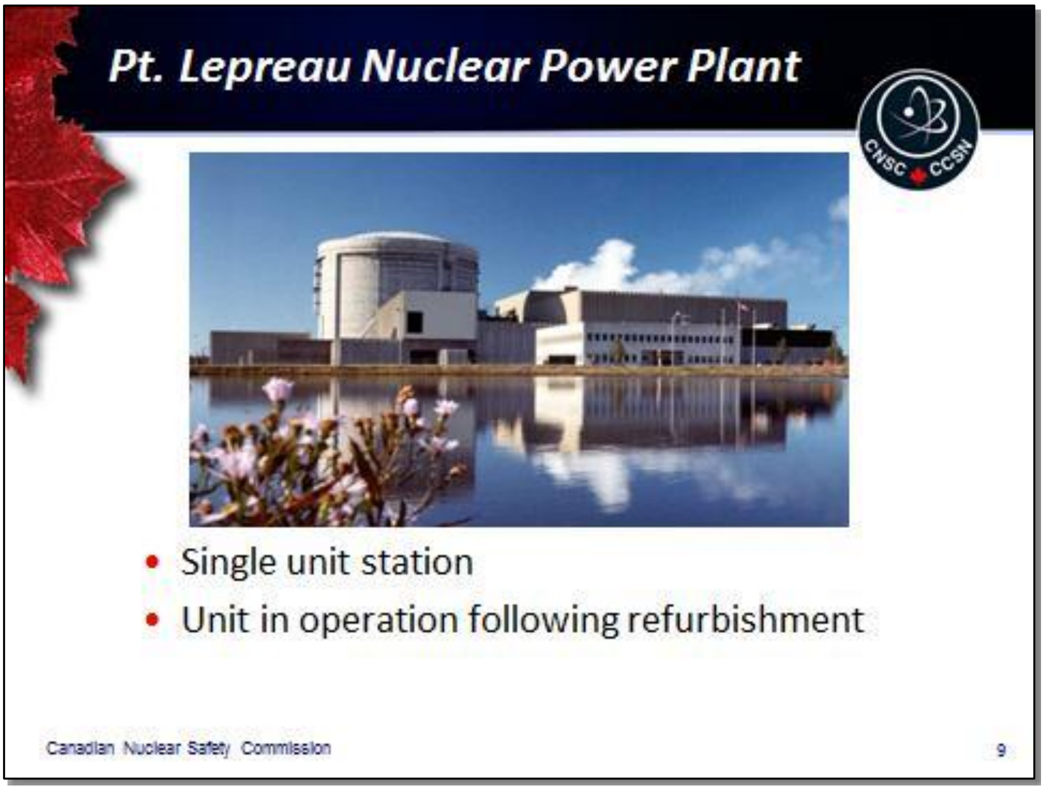
- Multi-unit station
- 2X4 Units (Bruce – A and Bruce – B)
- All units in operation

Canadian Nuclear Safety Commission 7

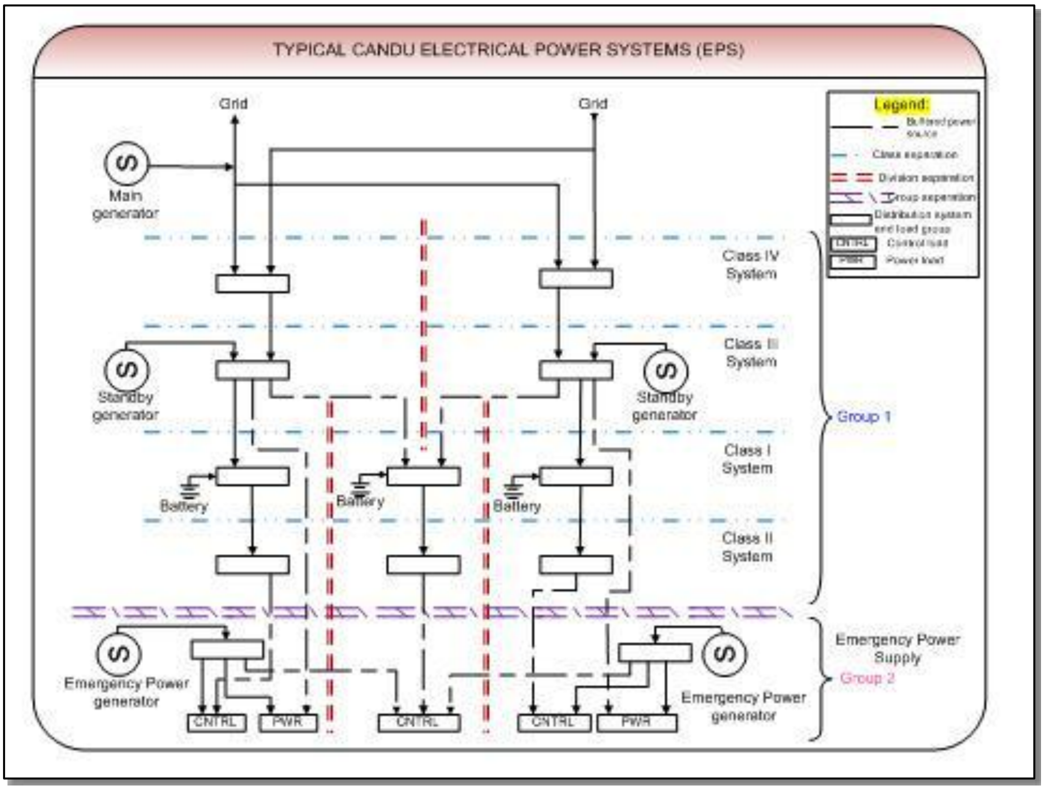
Darlington Nuclear Power Plant

- Multi-unit station (4 units)
- All units in operation

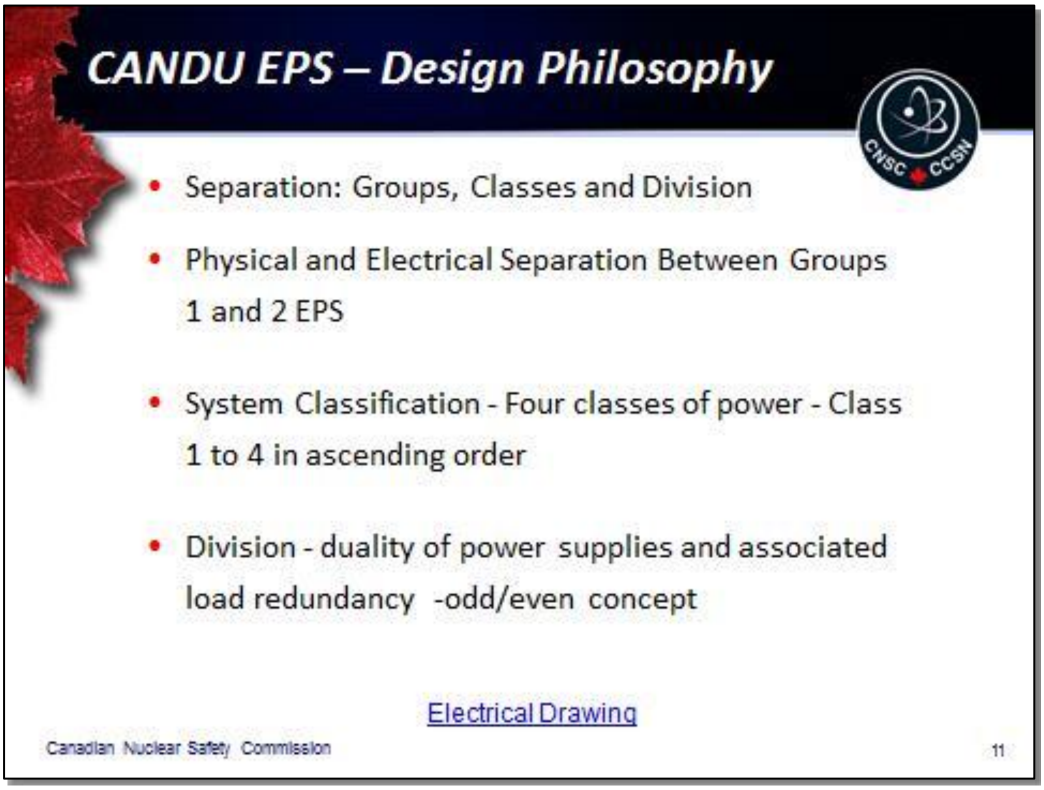
Canadian Nuclear Safety Commission 8

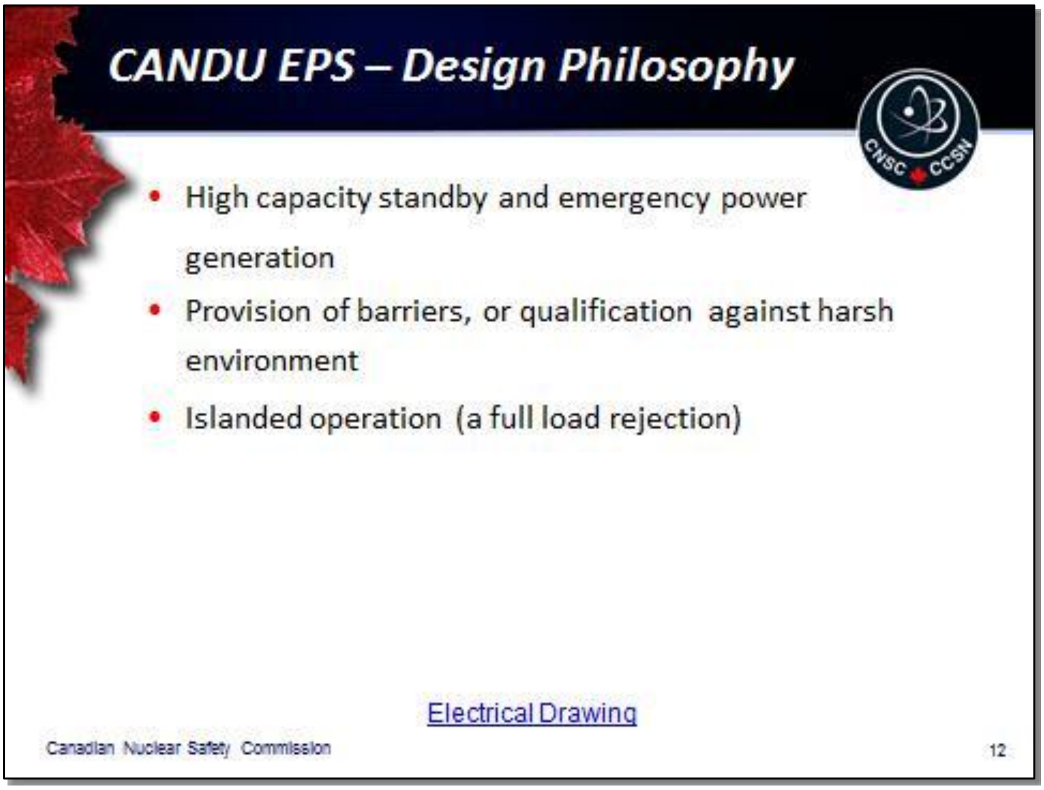


Pt. Lepreau Nuclear Power Plant
CNSC CCSN
• Single unit station
• Unit in operation following refurbishment
Canadian Nuclear Safety Commission
9



TYPICAL CANDU ELECTRICAL POWER SYSTEMS (EPS)
Grid
Grid
Main generator
Legend:
Class IV System
Class III System
Class I System
Class II System
Standby generator
Standby generator
Battery
Battery
Battery
Group 1
Emergency Power Supply
Group 2
Emergency Power generator
Emergency Power generator
CNTRL
PWR
CNTRL
CNTRL
PWR


CANDU EPS – Design Philosophy
CNSC CCSN
• Separation: Groups, Classes and Division
• Physical and Electrical Separation Between Groups 1 and 2 EPS
• System Classification - Four classes of power - Class 1 to 4 in ascending order
• Division - duality of power supplies and associated load redundancy -odd/even concept
Electrical Drawing
Canadian Nuclear Safety Commission
11


CANDU EPS – Design Philosophy
CNSC CCSN
• High capacity standby and emergency power generation
• Provision of barriers, or qualification against harsh environment
• Islanded operation (a full load rejection)
Electrical Drawing
Canadian Nuclear Safety Commission
12

CANDU EPS – Classes of power

RELIABILITY

Class IV	• Normal Alternating Current (AC) –Supplied from turbine generator and/or grid
Class III	• AC system –Normally supplied from Class IV –Upon loss of Class IV, from Standby generator
Class II	• AC System –Normally supplied form Class I DC system –Can be supplied from Class III
Class I	• DC system –Normally supplied from Class III via rectifiers –Backup battery supply

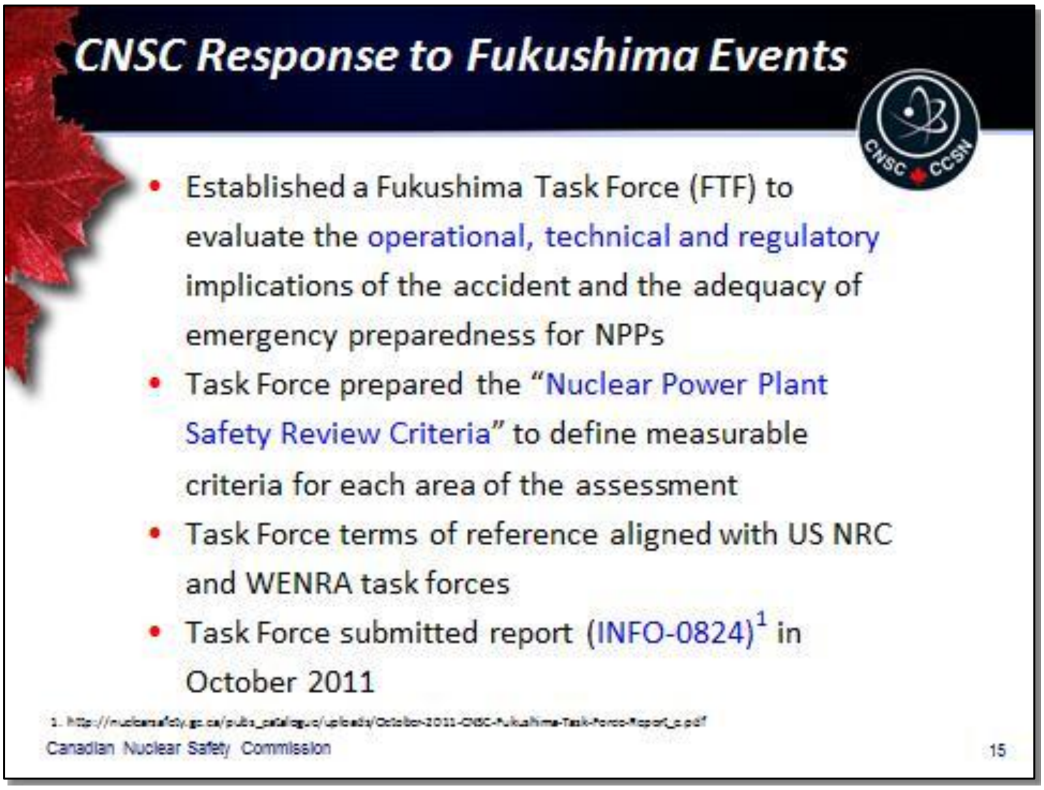
Electrical Drawing

Canadian Nuclear Safety Commission 13

Regulatory requirements - Pre Fukushima

- Loss of Class IV - analyzed in Safety Reports as part of Design Basis Accidents (DBA)
- Station Blackout (SBO) was considered a Beyond Design accident (BDBA) with an extremely low probability of occurrence
- No explicit requirements for SBO response
- Some stations analyzed loss of Class IV combined with loss of Class III power. No failure predicted
- The lessons learnt from Fukushima required licensees to analyze station capability to respond to SBO.

Canadian Nuclear Safety Commission 14


CNSC Response to Fukushima Events
CNSC CCSN
Established a Fukushima Task Force (FTF) to evaluate the operational, technical and regulatory implications of the accident and the adequacy of emergency preparedness for NPPs
Task Force prepared the "Nuclear Power Plant Safety Review Criteria" to define measurable criteria for each area of the assessment
Task Force terms of reference aligned with US NRC and WENRA task forces
Task Force submitted report (INFO-0824)1 in October 2011
1. http://nuclearsafety.gc.ca/pubs_catalogue/uploads/October-2011-CNSC-Fukushima-Task-Force-Report_e.pdf
Canadian Nuclear Safety Commission
15


CNSC Response to Fukushima Events
CNSC CCSN
CNSC management committed to implement FTF recommendations in a timely and transparent manner (INFO-0825)1
CNSC established an External Advisory Committee (EAC)2, to provide an independent assessment of response to the Fukushima Daiichi incident
The CNSC Integrated Action Plan3 was based on the findings and recommendations of the FTF Report and EAC as well as comments from public and stakeholders
Specific CNSC Staff Action Plan developed (INFO-0828)4
1. CNSC Management Response to Fukushima Task Force Report
2. External Advisory Committee Final Report
3. Fukushima Task Force CNSC Integrated Action Plan
4. CNSC Staff Action Plan on Fukushima
Canadian Nuclear Safety Commission
16

CNSC Regulatory Documents

- INFO-0824, INFO-0828 & REGDOC-2.5.2

Canadian Nuclear Safety Commission 17

Fukushima Action Items on SBO

- FAI – 1.10

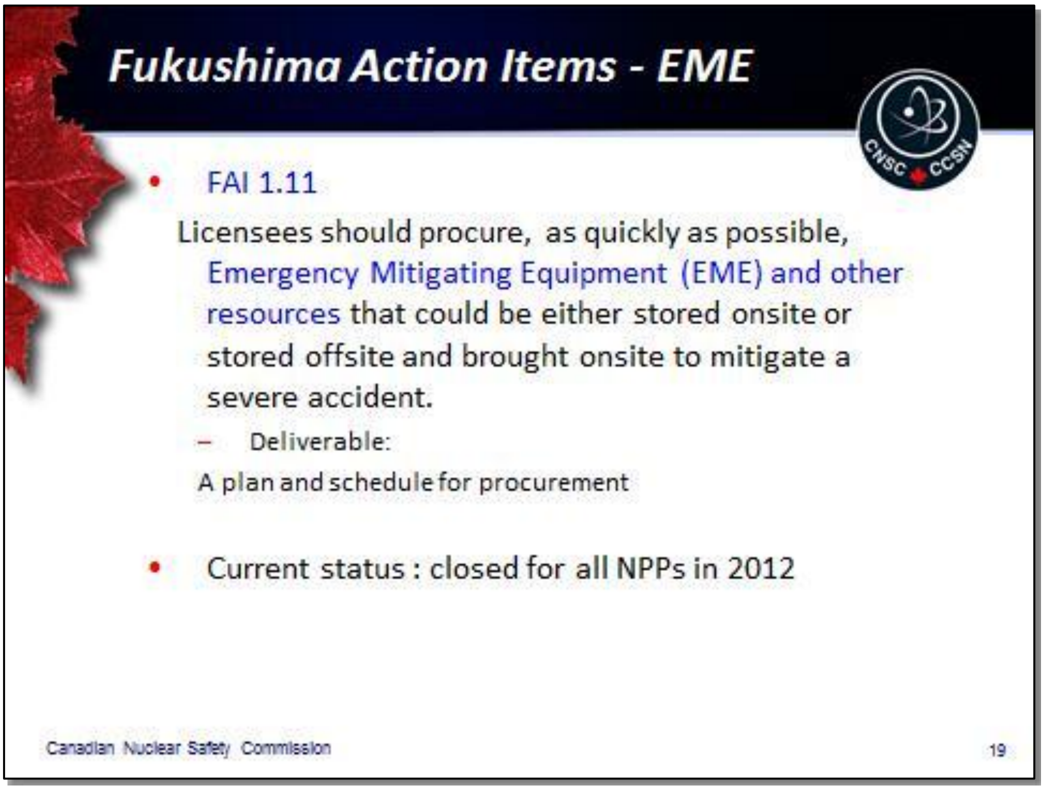
  Licensees should investigate means of extending the availability of power for key instrumentation and control (I&C) needed in accident management actions following a loss of all AC power

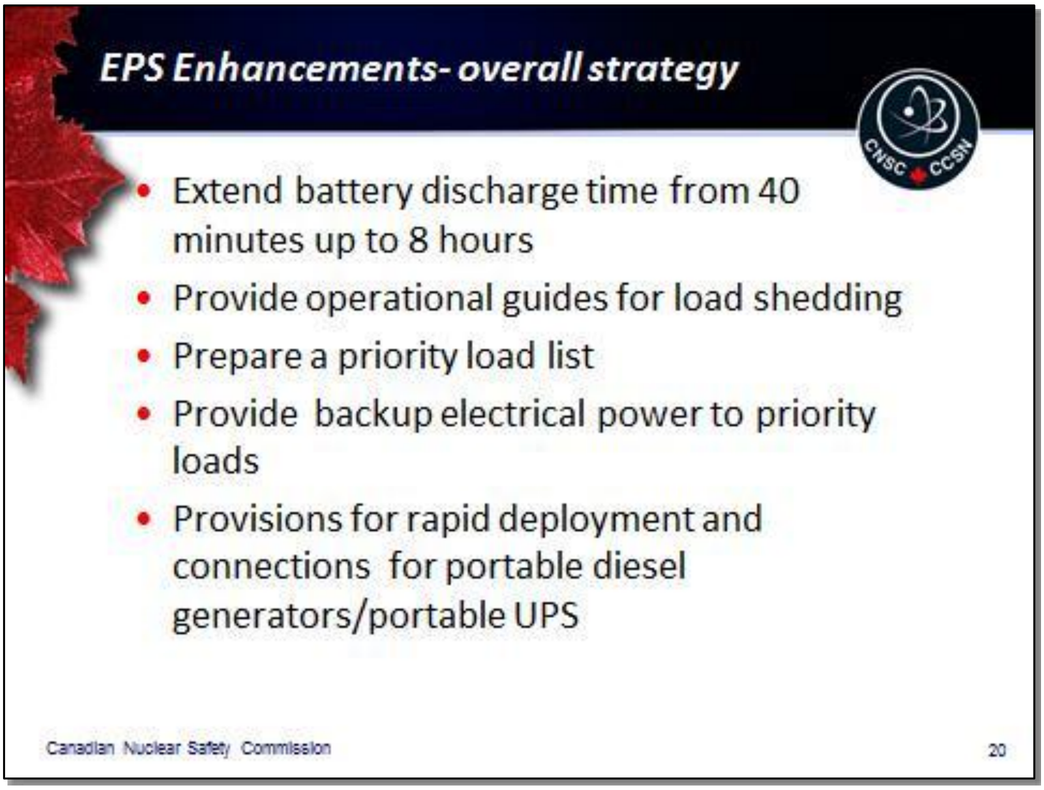
  - Deliverables:

  1. An evaluation of the requirements and capabilities for electrical power for key I&C. The evaluation should identify practicable upgrades that would extend the availability of key I&C, if needed.
  2. A plan and schedule for deployment of identified upgrades. A target of eight hours without the need for offsite support should be used.

- Current status: closed for all NPPs in 2012

Canadian Nuclear Safety Commission 18


Fukushima Action Items - EME
CNSC CCSN
FAI 1.11
Licensees should procure, as quickly as possible, Emergency Mitigating Equipment (EME) and other resources that could be either stored onsite or stored offsite and brought onsite to mitigate a severe accident.
Deliverable:
A plan and schedule for procurement
Current status : closed for all NPPs in 2012
Canadian Nuclear Safety Commission
19


EPS Enhancements- overall strategy
CNSC CCSN
Extend battery discharge time from 40 minutes up to 8 hours
Provide operational guides for load shedding
Prepare a priority load list
Provide backup electrical power to priority loads
Provisions for rapid deployment and connections for portable diesel generators/portable UPS
Canadian Nuclear Safety Commission
20

EME Training

- A training needs analysis conducted
- Station-specific Emergency Mitigating Equipment Guides (EMEGs) produced
- The EME training delivered to all ERT personnel who will be involved in emergency response
- Drills conducted to test the response effectiveness
- Focus on improving the capability to respond in time during the SBO event

Canadian Nuclear Safety Commission 21

New regulatory requirements

- REGDOC 2.5.2 Design of Reactor Facilities: Nuclear Power Plants supersede RD-337-2008
- Electrical Power System requirements has been expanded in REGDOC 2.5.2
- Provision for mitigating the complete loss of on-site and off-site AC power are required
  - onsite portable, transportable or fixed power sources, or/ and
  - offsite portable or transportable power sources

Canadian Nuclear Safety Commission 22


Emergency Mitigating Equipment
CNSC CCSN
CAT
Bruce Power
100 kW Generators
Canadian Nuclear Safety Commission
23


Emergency Mitigating Equipment
CNSC CCSN
Bruce Power
MOBILE OPERATIONS CENTRE
Mobile Operations Centre
Canadian Nuclear Safety Commission
24

Emergency Mitigating Equipment

Panel for 400kW AC generators

Canadian Nuclear Safety Commission

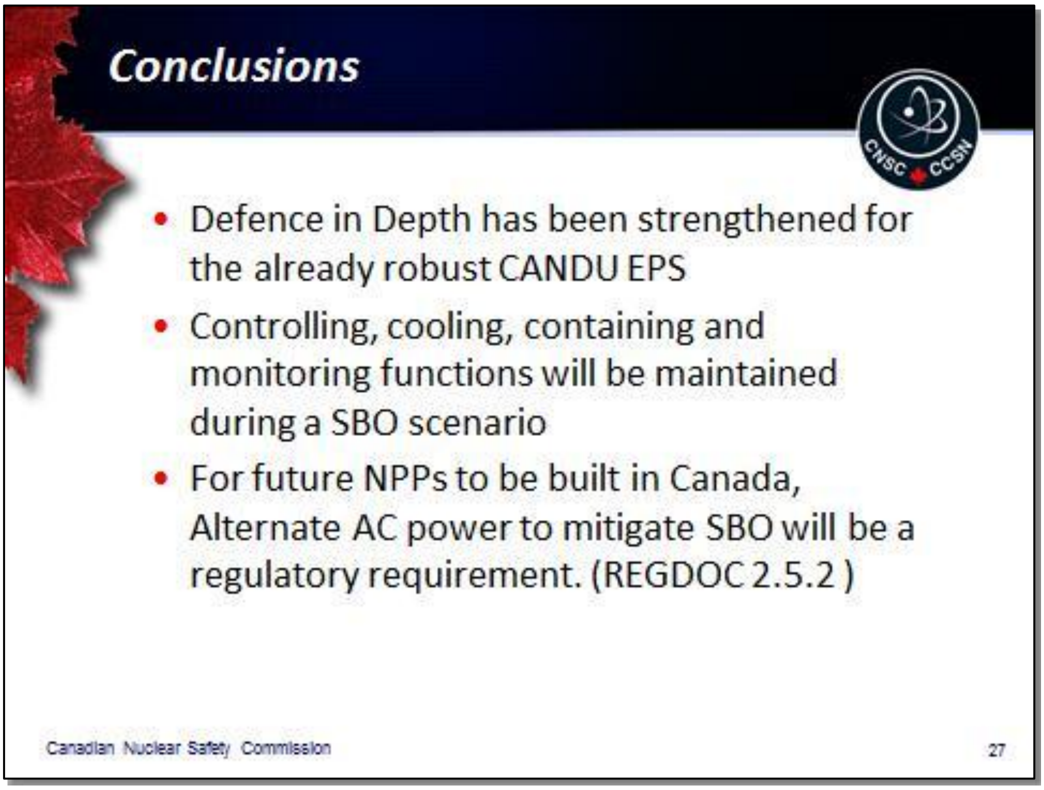
25

Emergency Mitigating Equipment

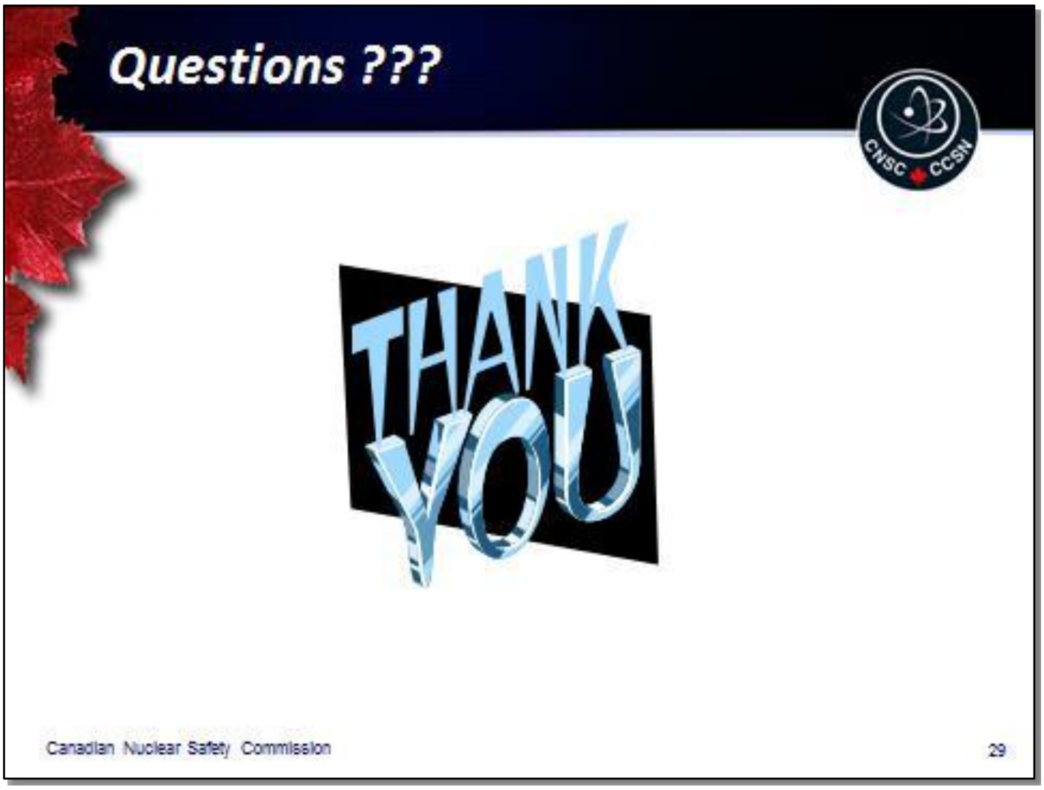
400 kW AC Generator

Canadian Nuclear Safety Commission

26


Conclusions
CNSC CCSN
• Defence in Depth has been strengthened for the already robust CANDU EPS
• Controlling, cooling, containing and monitoring functions will be maintained during a SBO scenario
• For future NPPs to be built in Canada, Alternate AC power to mitigate SBO will be a regulatory requirement. (REGDOC 2.5.2)
Canadian Nuclear Safety Commission
27


CNSC Video presentation on SBO
CNSC CCSN
For those interested, this CNSC video shows the progression of an accident scenario involving a total station blackout at a Canadian nuclear power plant.
http://www.youtube.com/watch?v=vggzl9OngaM&feature=player_detailpage
Canadian Nuclear Safety Commission
28


Questions ???
CNSC CCSN
THANK YOU
Canadian Nuclear Safety Commission
29

Fundamental design bases for independent core cooling in Swedish nuclear power reactors

Tomas Jelinek
Swedish Radiation Safety Authority, Sweden

Abstract

New regulations on design and construction of nuclear power plants came into force in 2005. The need of an independent core cooling system and if the regulations should include such a requirement was discussed. The Swedish Radiation Safety authority (SSM) decided to not include such a requirement because of open questions about the water balance and started to investigate the consequences of an independent core cooling system.

The investigation is now finished and SSM is also looking at the lessons learned from the accident in Fukushima 2011. One of the most important measures in the Swedish national action plan is the implementation of an independent core cooling function for all Swedish power plants. SSM has investigated the basic design criteria for such a function where some important questions are the level of defence in depth and the acceptance criteria. There is also a question about independence between the levels of defence in depth that SSM have included in the criteria. Another issue that has to be taken into account is the complexity of the system and the need of automation where independence and simplicity are very strong criteria. In the beginning of 2014 a memorandum was finalized regarding fundamental design bases for independent core cooling in Swedish nuclear power reactors. A decision based on this memorandum with an implementation plan will be made in the first half of 2014.

Sweden is also investigating the possibility to have armed personnel on site, which is not allowed currently. The result from the investigation will have impact on the possibility to use mobile equipment and the level of protection of permanent equipment.

In this paper, SSM will present the memorandum for design bases for independent core cooling in Swedish nuclear power reactors that was finalized in March 2014[7] that also describe SSM´s position regarding independence and automation of the independent core cooling function.

1. Summary

This memorandum describes the Swedish Radiation Safety Authority's (SSM) proposal for the fundamental design bases for *Independent core cooling* in Swedish nuclear power plants. The object of this function is to increase the level of resilience against certain events based on the results of the stress tests that have been carried out, as well as on earlier investigations regarding *Independent core cooling.*

[7] Proposal regarding fundamental design bases for independent core cooling in Swedish nuclear power reactors, T. Jelinek, 7 March 2014, SSM 2014-122-3.

2. Object and scope

The object of this memorandum is to briefly describe the design bases required in order to define the properties for *Independent core cooling.* These include design basis events, safety classification, residual heat removal, diversification, etc.

3. Background

The need to **i**ncrease the reliability of core cooling in a nuclear power reactor by introducing an independent function was brought up already when drafting the Swedish Nuclear Power Inspectorate (SKI) regulation SKIFS 2004:2 (corresponding to the present SSMFS 2008:17) from the beginning of the 2000s. The object of the new system was to during an H5 event (total loss of all non-battery-backed emergency systems, SBO, H5 is similar to PC6) add water for 24 hours to the reactor pressure vessel through connecting a water reservoir located outside of the reactor containment. The pumping of water would have to be activated independently of the reactor protection system, and also have separate power feed. For this reason, an early draft version of the proposed new regulation SKIFS 2004:2 contained the following proposed rule:

"In order to reduce the risk of core meltdown and reactor vessel melt through, it should be possible to add water to the reactor pressure vessel by connecting an independent water reservoir located outside of the reactor containment. Activation of pumping should be possible independently of the reactor protection system, and it should also have separate power feed."

The knowledge base, especially regarding negative effects of introducing this kind of function, was judged as insufficient for deciding on a regulation at that stage. SKI therefore came to the conclusion that further investigation was necessary. This further investigation was finalized in March 2009[8]. The need for independent core cooling received further attention after the Forsmark 1 event on 25 July 2006, as well as the serious events at the Fukushima Dai-ichi nuclear power plant.

After the Fukushima events, the European Council required at the end of March 2011 that stress tests were to be performed at all operating nuclear power plants in Europe. The Swedish national action plan to the EU[9] is part of these stress tests and it was developed with a view to dealing with deficiencies identified during the stress tests. Two issues are described in the action plan: T3.LA.2[10] and T2.LA.[11] that deal with independent core cooling. According to the action plan, analyses/investigations of the issues shall be finalized at the end of 2014 regarding T3.LA.2, and in 2015 regarding T2.LA.2.

This memorandum accounts for the fundamental design bases that can be of interest to observe when designing and constructing the independent core cooling.

---

[8] Investigation of independent core cooling systems for reducing the risk of core melt and vessel melt through in Swedish reactors, W. Frid, 16 March 2009, SSM 2008/354.

[9] Swedish Radiation Safety Authority, "Swedish action plan for nuclear power plants, Response to ENSREG's request", 29 December 2012.

[10] T3.LA.2 – Define the design bases for an independent core cooling system

[11] T2.LA.2 – Define design bases for alternate cooling and alternate residual heat removal

3 Proposed design bases

A number of fundamental design bases for *Independent core cooling* are presented here. Further design bases may be added while working on solutions.

3.1 Design basis events

The primary object of *Independent core cooling* is to prevent the reactor core from melting down, that is, to keep a coolable core geometry that belongs to defence in depth level 3 according to the WENRA countries' common view on the structure of defence in depth. The reason for choosing defence in depth level 3 is that major uncertainties in analyses of core melt sequence make it difficult to verify when and how vessel melt through takes place, which would be the case if the *Independent core cooling* would be set at defence in depth level 4. In defence in depth level 4 it is acceptable to have a reactor core that has lost its coolable core geometry. To set the *Independent core cooling* at defence depth level 3 also means that there is a more natural connection to the new design basis events stated below, against which the resilience must be strengthened according to the national action plan for the stress tests:

- Protracted loss of AC power and present steam generated motor power for at least 72 hours (*ELAPSP – Extended Loss of AC Power and Steam Power).*
- Protracted loss of ultimate heat sink for at least 72 hours (*LUHS – Loss of normal access to Ultimate Heat Sink*)

The ELAPSP event is an extension of ELAP, where loss of present steam generated motor power has been added.

All units at a site must be assumed to be exposed to ELAPSP or LUHS at the same time.

The design basis events need not be combined with other *independent* initiating events. Whenever other events are the result of this initiating event, e.g. loss of coolant in the present primary system in a PWR, this shall be taken into account in the analyses. Furthermore, it is not necessary to apply ELAPSP and LUHS at the same time

The extreme outer impact that shall be taken into account for the *Independent core cooling* is constituted by all the external conditions that could affect the core cooling at the plant. These conditions shall be identified, including possible links and interdependencies. The outer impact that cannot constitute a physical threat to the plant or which is estimated to be extremely improbable can be excluded. External events that in combination with other risks have the potential to constitute a threat to the plant must not be excluded. For all events that cannot be excluded, risk assessments shall be made using deterministic as well as probabilistic analyses. When assessing the risks, site specific data and conditions should be used. All events and the conditions that they lead to shall be taken into account if the frequency is 10^{-6} per year or higher.

The justification for choosing 10^{-6} per year or higher is that the safety functions shall be designed for external conditions that are more frequent than 10^{-5} per year. Should the state of the plant require *Independent core cooling*, a probable scenario would then be that an external condition has arisen with such a degree of severity that the present safety functions have not been able to deal with the event. Should the *Independent core cooling* system be unable to handle a more challenging initiating event or combinations of external events than the ones of today, the safety advantage would be uncertain in relation to extreme external events beyond design. Therefore the *Independent core cooling* should be designed for external events with a significantly lower frequency than 10^{-5} per year. This consequently means designing for greater snow loads, stronger winds, higher water level, etc.

The design basis events (ELAPSP and LUHS) shall be combined with all extreme external conditions that lead to situations that hereon are referred to as *Extreme conditions.*

Extreme conditions shall be evaluated for all operational states. To merely consider power operation is not compatible with the insights that the PSA analyses provide. Furthermore, acceptance criteria in event class 4 shall primarily be applied.

The duration of the ELAPSP and LUHS events is the minimum of the length of time needed in order to take necessary actions to counter these events under *Extreme conditions.* 72 hours is the minimum length of time to be used for the design bases.

3.2 Residual heat removal

The filtered pressure relief of the consequence mitigating systems for severe accidents must not be credited for residual heat removal in the design of the *Independent core cooling*, even if it can be shown that the capability of the system to fulfil its task (to filter the discharge) in an H5 event (core meltdown) is not affected.

The justification for this is that the various levels of defence in depth must be independent. Another argument is that the filters are the very last protection against major discharges due to a severe accident, and should be dedicated to defence in depth level 4. Even from a probabilistic perspective, introducing independent residual heat removal implies a reduction of risk. Should an accident occur all systems available shall of course be used, including systems that have not been credited in the safety analysis.

3.3 Safety classification

In the general advice for Section 21 of SSMFS 2008:17, it is stated that safety classification should follow the principles given in ANSI/ANS-51.1-1983 regarding pressurized water reactors and ANSI/ANS-52.1-1983 regarding boiling water reactors. (It should be noted that general advice is not binding for neither government authorities nor individuals; however, it is normally assumed that the requirement of the regulation is met provided that the recommended standard has been followed.) The indicated standards, 51.1 and 52.1, have however been withdrawn by the American standardization organization, to be replaced in 2011 with ANSI/ANS-58.14-2011 regarding criteria for safety classification. In the old standards from 1983 as well as in the new one from 2011, the classification is primarily based on the function that the equipment must fulfil in connection with “Design Basis Events (DBE)”.

The events that the independent core cooling function is meant to handle constitute an extension compared to “DBE”, which was not addressed in the old standards since the defence in depth structure at the beginning of the 1980s was not the same as today. On the other hand, a new safety class is introduced in 58.14, labelled “A” (“non-safety-related with augmented requirements”), to which functions that need to be performed in connection with “special events” beyond DBE are clearly classified. This also resembles the kind of classification that the IAEA uses, where equipment of importance for safety is separated into “safety systems” and “safety related items”. The latter is defined as equipment of importance for safety that is not part of a safety system, see the IAEA Safety Glossary. (Unfortunately the concept “safety related” is used with another meaning in the IAEA terminology compared to the US. The concept “safety-related” in American terminology is rather comparable to the IAEA’s “safety system”.) Furthermore the

IAEA has in its SSR-2/1 (from 2012) chosen to define the concept “safety feature for design extension conditions” in order to further describe this category of the equipment at a plant.

In the view of SSM, from a functional classification perspective and with the above in mind, the independent core cooling should be categorized in a specific safety class equivalent to the IAEA’s guidelines and ANSI/ANS-58.14, with the purpose of clarifying which specific requirements should be valid for all equipment, as well as defining the distinction in relation to “operationally classed?? equipment”. The additional equipment for independent core cooling shall, based on this platform, be attributed the requirements on quality assurance and operability that, at an acceptable level, ensure that the equipment can perform the function required during the *Extreme conditions* that are expected to prevail when the equipment is credited.

3.4 Separation and diversification

Independent core cooling must be functionally and physically separated vis-à-vis systems and components that are used at the other levels of the defence in depth, as well as against existing systems and components of the defence in depth level that is to be reinforced as far as concerns water reservoir, power feed, I&C as well as isolation valves.

Exceptions can be made for separation against the diversified parts of the safety function. This exception implies that the *Independent core cooling* in the future can be a subset for fulfilling the diversification requirements according to Section 10 of SSMFS 2008:17 for the safety functions’ core and containment spray as well as residual heat removal.

3.5 Redundancy

It is not necessary to fulfil the single failure criteria for the *Independent core cooling*. This cooling system is viewed as a supplement and backup in relation to existing systems and components in defence in depth level 3.

3.6 Simplicity in the functional framework and the use of electricity for power supply

The ambition is to achieve simplicity in the functional framework. This implies a lower probability of faults being built in or introduced in connection with maintenance, refurbishing or rebuilding work. A transparent system is also more straightforward to manage and should consequently be simpler to sustain or restart during *Extreme conditions.*

Electricity for power supply to safety features revealed deficiencies in robustness against extreme events in Fukushima. This is due to that it is very difficult to encapsulate electrical equipment (problems of cooling, condensation, flooding, etc.). Electrical materials are also difficult to make robust against electromagnetic fields and power surges. Despite early availability in Fukushima of electric power generators, it was not possible to operate safety objects, due to moisture and salt water intrusion. An external direct-drive motor pump is probably easier to get back and be made to work (connected to the pipeline to the reactor tank) than getting an external motor-generator function to operate an independent electrically driven pump. This needs to be investigated and taken into account when designing the independent core cooling function.

3.7 Manual and/or automatic initiation/control

It should be possible to start *Independent core cooling* and monitor it close to the object/locally and from the main control room. It should also be possible to have optional manual initiation directly on components, i.e. required local manoeuvrability on pumps, inboard and outboard/isolation valves, etc.

The manual initiation and operation of the *Independent core cooling* must be ready for activation by using simple and transparent equipment under *Extreme conditions*. A requirement is imposed on manual initiation of all components in the *Independent core cooling* in order to ensure this independence as far as possible.

Automatic initiation is not necessary provided that the acceptance criteria can be met with reasonable time for consideration in the event of *Extreme* conditions.

Simplicity shall be the objective; for example, control in the form of complicated electronics or sequential control should be avoided.

Necessary information to the operators concerning process parameters so as to enable comprehension and performance of the function's initiation and operation should be as straightforward and transparent as possible and be independent of routine information.

3.8 Mobile equipment

It is not permitted to credit heavy external equipment within 72 hours. If heavy external equipment is credited after 72 hours, it must be demonstrated as being available and capable of being transported and connected under *Extreme conditions*. For instance, in order to credit the onsite grid after 72 hours, it must be demonstrated that it is available in connection with *Extreme conditions*.

Mobile equipment set up onsite in advance may be used no earlier than after 8 hours if it can be demonstrated as being available and functional in connection with *Extreme conditions*.

3.9 Safety margins

The system is to be dimensioned allowing for good safety margins in its design since the extent and nature of the conditions that the system must be capable of withstanding are linked with considerable uncertainties.

3.10 Requirements imposed on physical protection

Certain key assumptions for a security force, for example pertaining to issuing weapons and principal organisers, are currently being investigated by the Ministry of the Environment

In the autumn of 2013, an updated design bases threat description was approved implying what events the facilities must be capable of withstanding. Based on the threat description in addition to other potential protective measures, the licensees have the possibility of designing the *Independent core cooling* (bunkered) together with the protection of the rest of the facility in a way so that the requirements imposed under SSMFS 2008:12 are fulfilled. The part of the *Independent core cooling* whose task is residual heat removal may have other design assumptions in terms of physical protection if the time aspect allows for crediting of external physical protection.

On the basis of this memorandum and an impact assessment, SSM is planning to take a decision on implementation of *Independent core cooling*. In connection with this decision, SSM will also give guidance for licensee analyses of the capability of a possible security force to withstand antagonistic threats, including assumptions on antagonists' possible entry and use of explosives in the facility, particularly on the independent core cooling.

3.11 While awaiting a final solution

Installation of permanent equipment takes a long time. Consequently, there is a need for earlier protection that does not fully meet the requirements. These solutions may become a part of the final solution.

Strål
säkerhets
myndigheten
Swedish Radiation Safety Authority

Fundamental design bases for independent core cooling in Swedish nuclear power reactors

Tomas Jelinek
Swedish Radiation Safety Authority

Tomas Jelinek
2015-01-13
Sida 1

Presentation layout

- Historical background
- Proposed design bases

Tomas Jelinek
2015-01-13
Sida 2

Background 1(5)

The need to increase the reliability of core cooling in a nuclear power reactor by introducing an independent function was brought up already from the beginning of 2000 when drafting the new regulation SSMFS 2008.17.

At the event "total loss of all non-battery-backed emergency systems, SBO, add water for 24 hours to the reactor pressure vessel through connecting a water reservoir located outside of the reactor containment".

Tomas Jelinek
Sida 3

Background 2(5)

The pumping of water would have to be activated independently of the RPS, and have separate power feed. An early draft version of the present regulation SKIFS 2008:17 contained the following proposed rule:

"In order to reduce the risk of core meltdown and reactor vessel melt through, it should be possible to add water to the reactor pressure vessel by connecting an independent water reservoir located outside of the reactor containment. Activation of the pumping should be possible independently of the RPS, and it should also have separate power feed."

Tomas Jelinek
Sida 4

Background 3(5)

The knowledge base, especially regarding negative effects of introducing this kind of function, was judged as insufficient for deciding on a regulation at that stage. SSM therefore came to the conclusion that further investigation was necessary.

Tomas Jelinek
2015-01-13
Side 5

Background 4(5)

Forsmark 1 event 2006

The need for independent core cooling received further attention after the Forsmark 1 event on 25 July 2006. The Forsmark 1 event showed that a high degree of *redundancy* and *separation* do not automatically mean high safety with robustness in construction and defence in depth, primary because of the *electrical dependencies* that are very difficult to eliminate.

A decision was close in the beginning of 2011.

Tomas Jelinek
2015-01-13
Side 6

Background 5(5)

Fukushima made SSM postpone the decision, to learn from the accident for the design bases for independent core cooling.

Stresstest

The Swedish national action plan to the EU is to handle deficiencies identified during the stress tests.

The issues described in the action plan are:

- T2.LA.2 – Define design bases for alternate cooling and alternate residual heat removal.
- T3.LA.2 – Define the design bases for an independent core cooling system.

Tomas Jelinek
2015-01-13
Sida 7

Design bases events1(3)

The design bases events are:

- Loss of AC power and present steam generated motive power for at least 72 hours (*ELAPSP – Extended Loss of AC Power and Steam Power)*.
- Loss of ultimate heat sink for at least 72 hours (*LUHS – Loss of normal access to Ultimate Heat Sink*).

The ELAPSP event is an extension of ELAP, where loss of present steam generated motive power has been added.

Tomas Jelinek
2015-01-13
Sida 8

Design bases events 2(3)

Extreme conditions

The design basis events (ELAPSP or LUHS), combined with extreme external conditions, more frequent than per year 10^{-6} per year.

Tomas Jelinek
2015-01-13
Sida 9

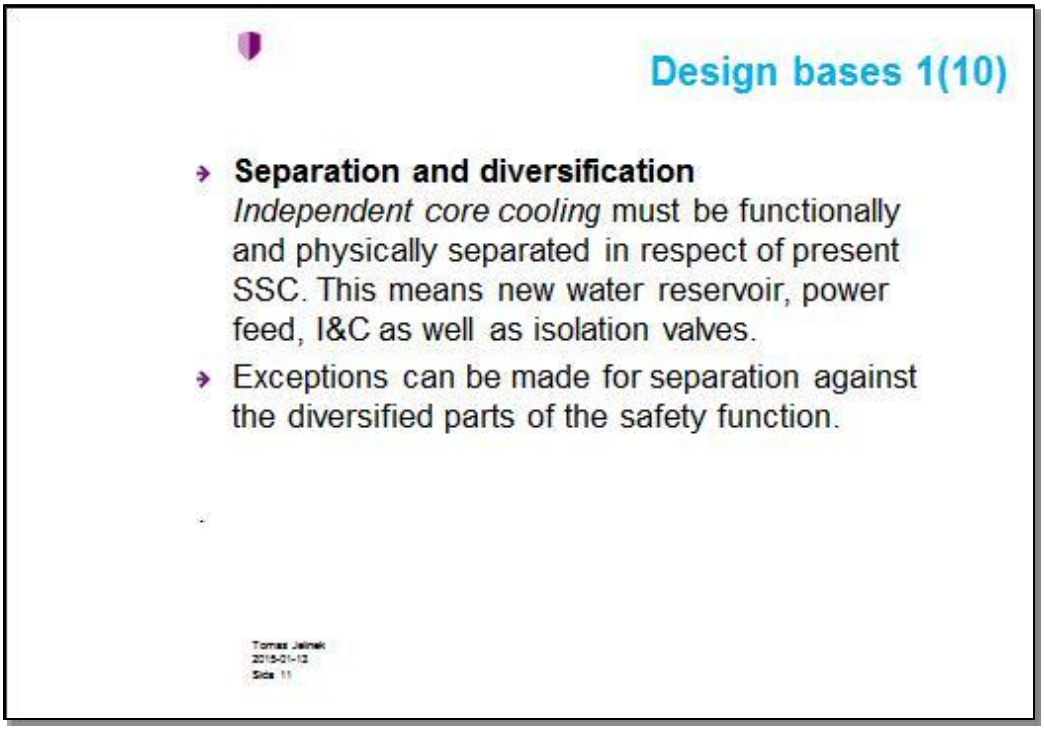
Design bases events 3(3)

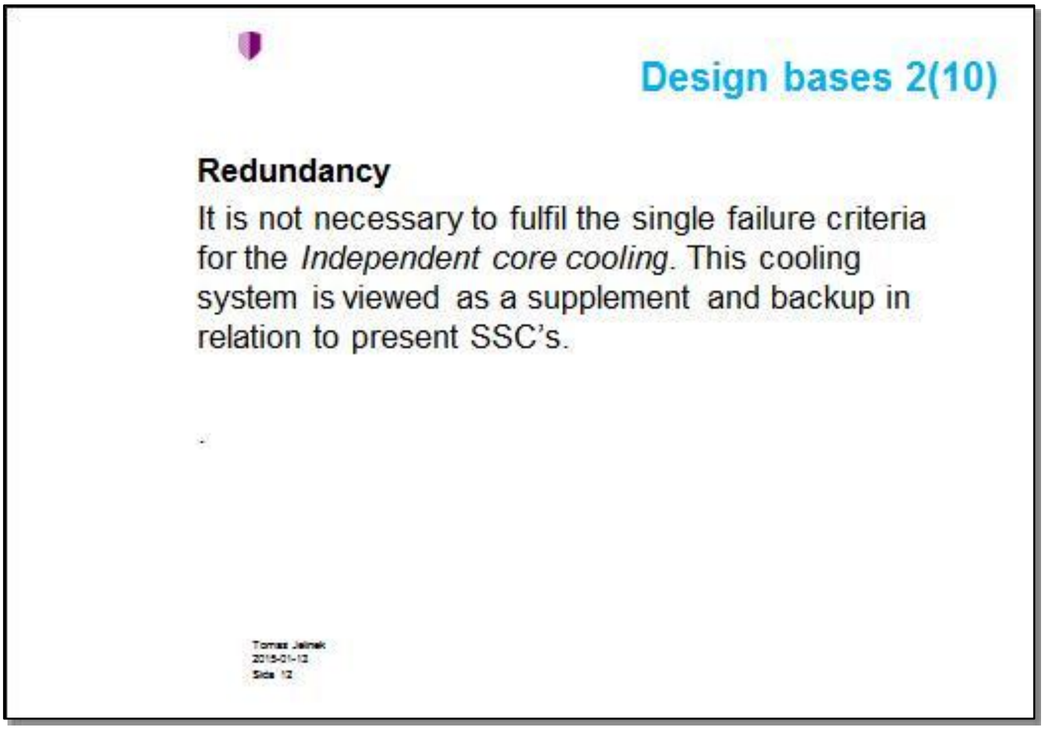
Justification of 10^{-6} per year

Should the *Independent core cooling* be required, a probable scenario is an external condition with such a degree of severity that the present safety functions have not been able to deal with the event.

The *Independent core cooling* should be designed for external events with a significantly lower frequency than 10^{-5} per year (10^{-5}=design base for present safety functions). This consequently means designing for greater snow loads, stronger winds, higher water level, etc.

Tomas Jelinek
2015-01-13
Sida 10


Design bases 1(10)
Separation and diversification
Independent core cooling must be functionally and physically separated in respect of present SSC. This means new water reservoir, power feed, I&C as well as isolation valves.
Exceptions can be made for separation against the diversified parts of the safety function.


Design bases 2(10)
Redundancy
It is not necessary to fulfil the single failure criteria for the Independent core cooling. This cooling system is viewed as a supplement and backup in relation to present SSC's.

Design bases 3(10)

Residual heat removal

The present filtered pressure relief of the consequence mitigating systems (introduced 1987) for severe accidents must not be credited for residual heat removal in the design of the *Independent core cooling*.

Operational states

All operational states must be considered, not only power operation.

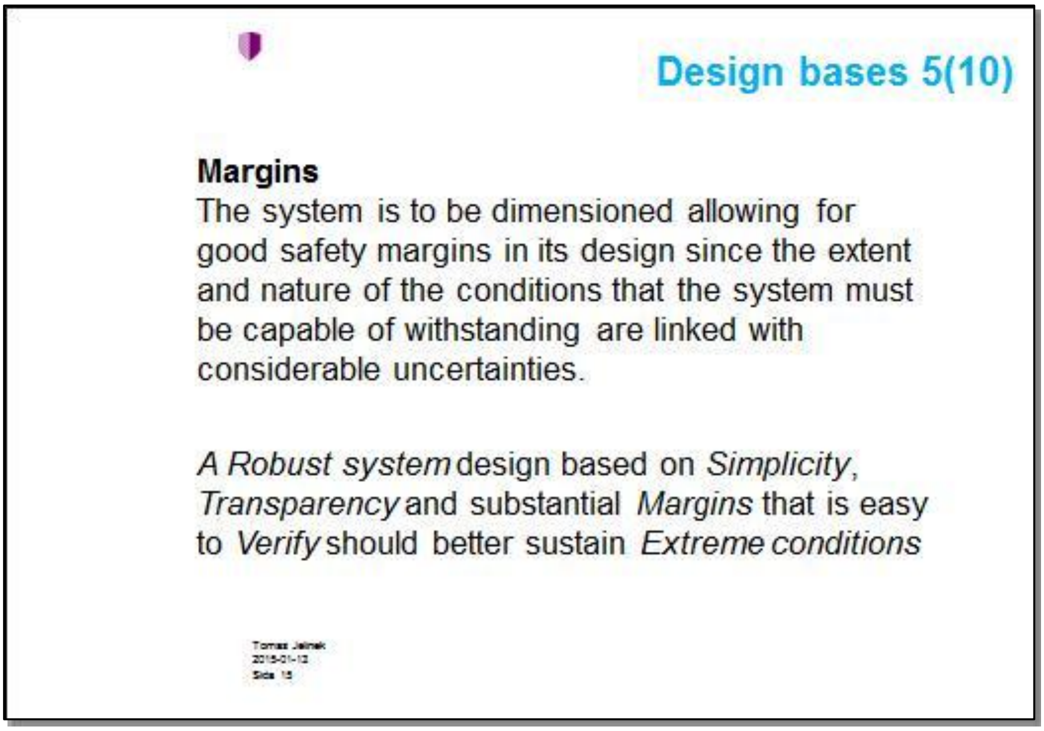
Tomas Jelinek
2015-01-13
Sida 13

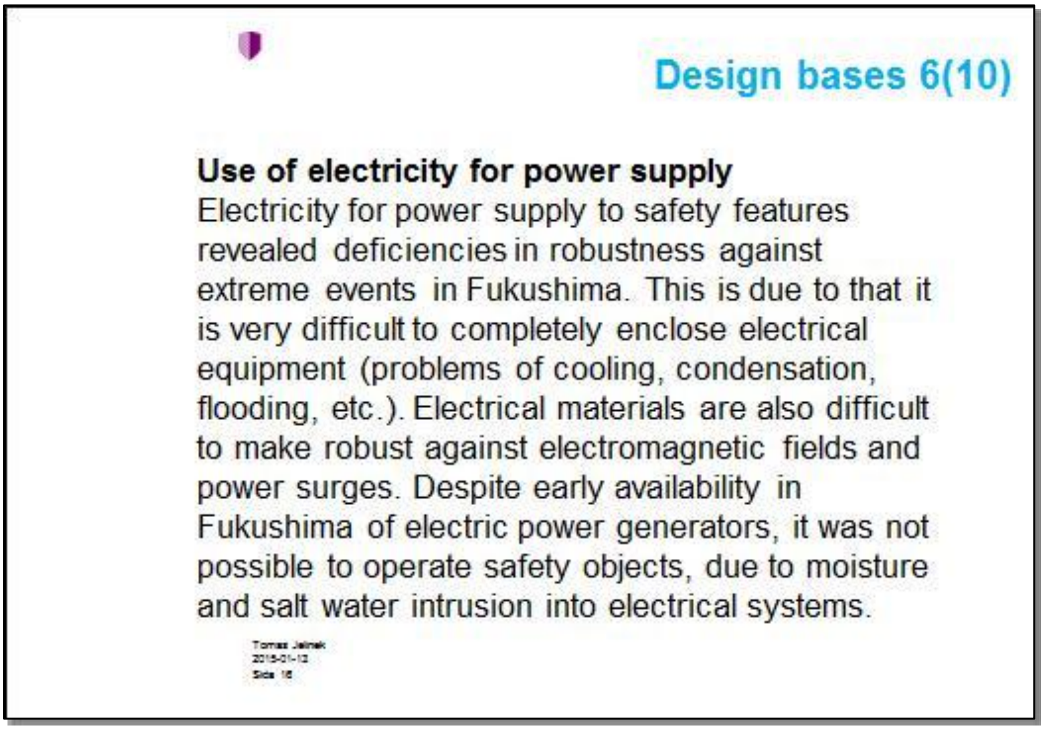
Design bases 4(10)

Simplicity, Transparency and Verifiability

The ambition is to achieve simplicity in design. This should result in a lower probability of faults being introduced in design or in connection with maintenance, refurbishing or rebuilding work. A simple system is also more transparent and should therefore be more straightforward to verify and manage.

Tomas Jelinek
2015-01-13
Sida 14


Design bases 5(10)
Margins
The system is to be dimensioned allowing for good safety margins in its design since the extent and nature of the conditions that the system must be capable of withstanding are linked with considerable uncertainties.
A Robust system design based on Simplicity, Transparency and substantial Margins that is easy to Verify should better sustain Extreme conditions


Design bases 6(10)
Use of electricity for power supply
Electricity for power supply to safety features revealed deficiencies in robustness against extreme events in Fukushima. This is due to that it is very difficult to completely enclose electrical equipment (problems of cooling, condensation, flooding, etc.). Electrical materials are also difficult to make robust against electromagnetic fields and power surges. Despite early availability in Fukushima of electric power generators, it was not possible to operate safety objects, due to moisture and salt water intrusion into electrical systems.

Design bases 7(10)

Use of electricity for power supply, con't
An external direct engine driven pump is probably easier to get back and be made to work (connected to the pipeline to the reactor tank) than getting an external motor-generator function to operate an electrically driven pump.

Historical probability data of steam generated motive power shows even lower probability than equivalent electrical pumps.

Thus this needs to be investigated and taken into account, when designing the *Independent core cooling*.

Tomas Jelinek
2015-01-13
Sida 17

Design bases 8(10)

Manual and/or automatic initiation/control 1(2)
Requirement is imposed on manual initiation and monitoring of the *Independent core cooling*. All components required for *Independent core cooling* function should be manually manoeuvrable.

These requirements ensure the independency of failure in automation, electrical disturbances, auxiliary systems failure, fire, and other consequences of extreme events as far as possible.

Tomas Jelinek
2015-01-13
Sida 18

Design bases 9(10)

Manual and/or automatic initiation/control con´t

Automatic initiation is not a requirement if the acceptance criteria can be met during *Extreme conditions*.

Simplicity and *Transparency* shall be the objectives; for example, control in the form of complicated electronics or sequential control should be avoided.

Necessary information to the operators should be as straightforward and *Transparent* as possible and be independent of routine information.

Tomas Jelinek
2015-01-13
Sida 19

Design bases 10(10)

Safety classification

Independent core cooling shall be classified in a sub-group under "Items important to Safety" as defined by IAEA glossary. Requirements on quality assurance and operability shall ensure that the equipment can perform the function required during the *Extreme conditions*. The normal functional design requirements imposed by classification of electrical and control equipment in Class 1E is necessarily not fully applicable and may also need to be supplemented.

Tomas Jelinek
2015-01-13
Sida 20

While awaiting a final solution

Installation of permanent equipment takes a long time. Consequently, there is a need for earlier protection that does not fully meet the requirements. These solutions may become a part of the final solution

Tomas Jelinek
2015-01-13
Side 21

Ultimate Electrical Means for Severe Accident and Multi Unit Event Management

Xavier Guisez
Electrabel GDF Suez

Abstract

Following the Multi Unit Severe Accident that occurred at Fukushima as a result of the tsunami on 11 March 2011, the European Council decided to submit its Nuclear Power Plants to a Stress Test. In Belgium, this Stress Test, named BEST (BElgian Stress Test), was successfully concluded at the end of 2011. Nevertheless, Electrabel decided, in agreement with the Authorities, to start a beyond design basis action plan, with the goal to mitigate the consequences of a Beyond Design Basis Accident and a Multi Unit Event. Consequently, this has lead to an improvement of the robustness of its Nuclear Power Plants.

Considering the importance of electrical power supply to a nuclear power plant, a significant part of this action plan consisted of setting up a mobile, 'plug and play' method for the electrical power supply to some major safety systems. In order to install this ultimate power supply, three factors were retained as essential. First, important reactor monitoring instrumentation is preserved. Second, core cooling is provided at all times. Finally, systems are easily made operational within a very short delay of time.

During normal operation and Design Basis Events, core cooling is provided by High Voltage equipment. However, during high stress circumstances, it is too complex to realize connections on this equipment. Therefore, analysis was performed to realize core cooling with, easier to handle, Low Voltage equipment. These systems are powered by several GenSets, especially designed and manufactured for this application.

The outcome of this project are easy to use, ultimate means, that supply electric power to important safety systems in order to drastically reduce the risk of core damage, during a beyond design basis event. Additionally, for all ultimate means, procedures and training modules were developed for the operators.

Need for Electrical Power Supply

The purpose of a nuclear power plant is to produce electrical power. Therefore, a nuclear power plant has many similarities to other electrical generating facilities. However, there is one major difference to this comparison. Unlike a conventional power plant, a nuclear power plant still produces an important amount of thermal energy following an emergency stop. This amount of energy is enough to cause severe damage to the installation with possible result of radioactive release to the environment. Therefore it is essential for a nuclear power plant, to remove this residual thermal energy by adequate cooling systems. Although it is possible to use this heat to drive cooling pumps or fans, these systems have their limitations. In the end, there is always an electrical energy source needed for cooling the reactor core. As ironical as it may seem, although a nuclear power plant is constructed to produce electricity, supply of electricity to the plant is an absolute necessity to ensure the safety.

Electrical Design

Before discussing the electrical design of Doel Nuclear Power Plants, it is important to have an idea of the design basis and its key safety features. Table 1 gives an overview of the nuclear installations at the site of Doel.

	Type	Thermal Power (MWth)	First Criticality	Reactor Building	Steam Generator Replacement	Design
Doel 1	PWR (2 loop)	1312	1974	Double Containment (steel and concrete)	2009	Westinghouse
Doel 2	PWR (2 loop)	1312	1975	Double Containment (steel and concrete)	2004	Westinghouse
Doel 3	PWR (3 loop)	3064	1982	Double Containment (concrete with liner and concrete)	1993	Framatome
Doel 4	PWR (3 loop)	3000	1985	Double Containment (concrete with liner and concrete)	1997	Westinghouse

Table 1: Basis Design Nuclear Installations at Doel

At the time, in Belgium, the nuclear regulatory framework was still 'under development'. Therefore it was agreed to use the American regulation as a reference and all Belgian Nuclear Units were designed accordingly. Additionally, in accordance with the Belgian regulation concerning the protection of population against ionizing radiation and because of the high population density, some specific key safety features were integrated in the general design:

- All Reactor Buildings have a Double Containment separated by an interspace held at slightly lower than ambient pressure. The purpose is to collect and filter the possible radioactive gases released in case of an accident and to discharge it at sufficient height, according the topography of the environment.
- In 1975 the Belgian Authorities decided that the design of the Nuclear Power Plants had to consider additional external hazards, regardless the American regulation. This demand resulted in a second level of safety systems, functionally independent and physically separated from the 'common' first level of protection systems dedicated to internal hazards. Moreover, the nature of these hazards required this second level of protection systems to be bunkerized. The purpose of this second level is protection against external hazards such as airplane crashes, explosion, etc.
- The site of Doel has two possibilities of ultimate cold source. Next to the river there are three cooling ponds, each containing about 30.000 m^3 of water.
- Units Doel 3 and Doel 4 have an extra common emergency diesel generator.

The site of Doel is connected with the external grid via multiple connections. The external main source is assured by five 380kV-lines. All four nuclear units are connected with this 380kV grid via multiple busbars. A second external power source is provided by a 150kV grid, connected with the units via a double busbar system. This 150kV supply is assured by two high voltage lines. In case of complete Loss Of Offsite Power (LOOP), meaning the simultaneous loss of both high voltage supplies, the plant transfers to island mode, only providing electrical power to its own auxiliaries. When at least one entity successfully transfers to island mode, it is possible to make the connection with the other power plants, in this way supplying electrical power to the auxiliaries.

When the unit cannot transfer to island mode a redundant number of safety and emergency diesel generators will provide electrical power to the nuclear safety related auxiliaries. In case of complete loss of external and internal power critical I&C systems are powered via batteries. Figure 1 shows an overview of the electrical design of Doel 3 and Doel 4.

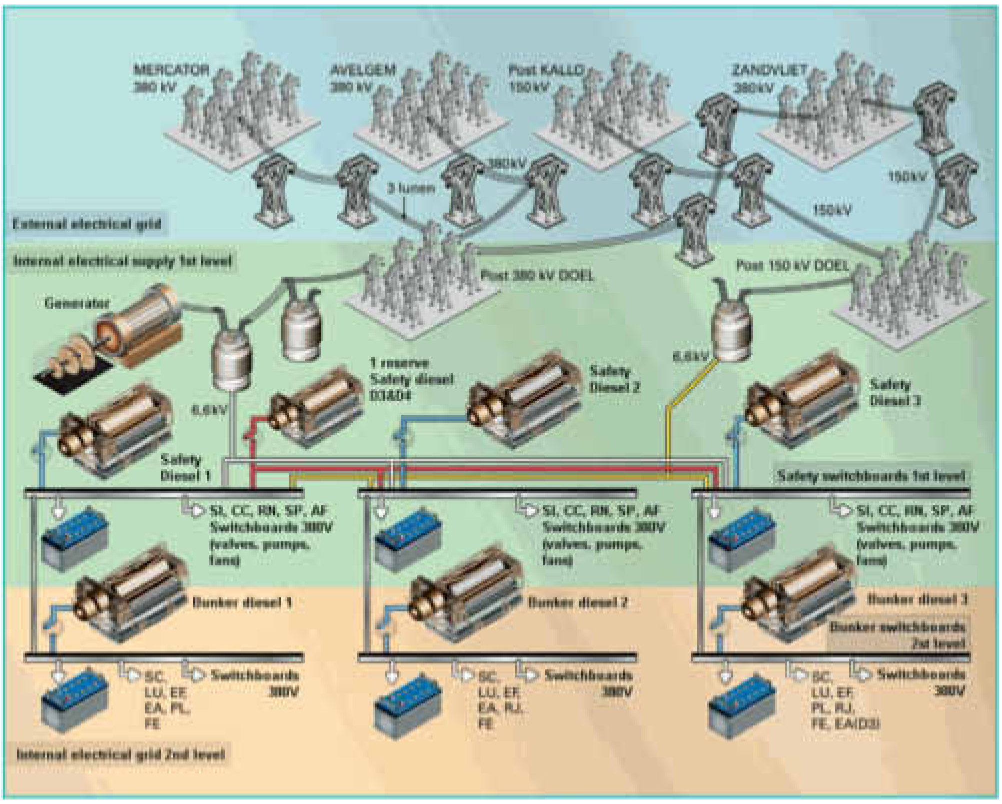


Figure 12: Electrical Design Doel 34 [1]

These multiple safety levels show to what extent the site of Doel was already, by the original design, protected against the complete loss of electrical power supply. This points out that occurrence of this scenario is highly unlikely.

Non Conventional Equipment

Despite the abundant safety power systems, described in the previous paragraph, Electrabel agreed, in the framework of the Belgian Stress Tests, to implement an action plan. The purpose was to bring the robustness and defence in depth to an even higher level. Installation of Non Conventional Equipment (NCE), among others, is part of that action plan.

The considered hazards are an extreme seismic event and site flooding. The envelope scenario retained for defining the Non Conventional Equipment is the "complete station blackout", meaning:

- Loss of both high voltage power supply (380kV and 150kV)
- Failure of island mode
- Loss of all first level diesel generators
- Loss of all second level diesel generators

This scenario only leaves batteries, turbine pumps, by gravity transferable cooling water and finally, the Non Conventional Equipment at the site's disposal.

Extreme Seismic Event

In case the complete station blackout is the result of an extreme seismic event, it is considered that the NCE will only be used after the occurrence of this event. Therefore the seismic specification prescribes that these equipments must withstand the earthquake structurally and need to be functional after the earthquake. In contrast to the first and second level safety equipment, the NCE are not qualified for operation during the seismic event.

In order to define the seismic specification for the NCE a Seismic Margin Assessment (SMA) was performed resulting in a acceleration spectrum more severe than the one used for the design criteria of the nuclear units. The resulting spectrum is shown in Figure 2.

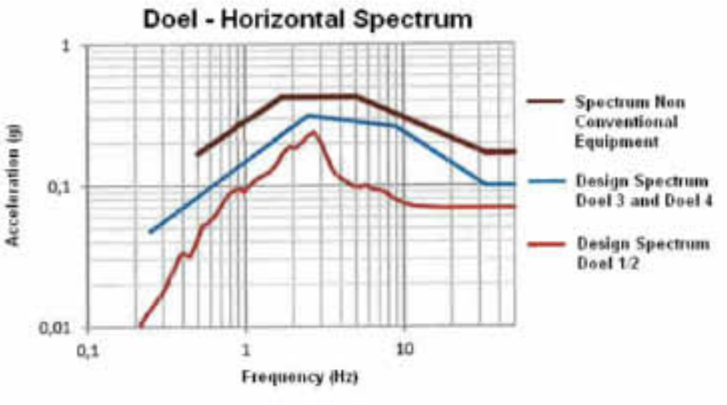


Figure 13: NCE seismic spectrum

Flooding

During the Belgian Stress Tests following cases were considered to assess flooding coping capability:

- Water (river) surge in combination with severe weather circumstances with a period of occurrence of one in ten thousand years.
- Dike breach at high water level.

Since the nuclear site is located higher than the surrounding polders, only temporarily flooding is possible, before the water drains off to the lower located area. Conservative calculations showed no more than a few tens of centimetres of water level are expected on site.

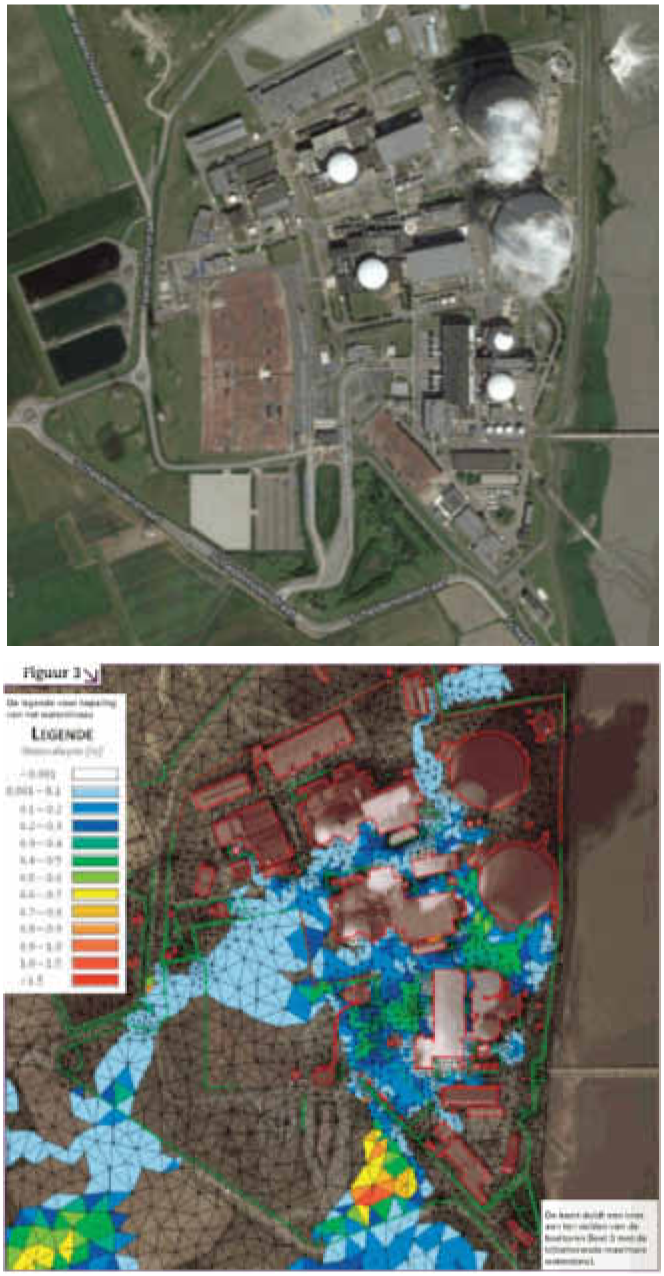


Figure 14: Site flooding calculation [1]

Design

The accident at Fukushima Nuclear Power Plant has emphasized the great difficulty to restore electrical power to vital equipment once the standard equipment and installations are damaged and unusable [3]. At Doel Nuclear Power Plant, this would not be any different, considering most of the necessary equipment for core cooling is connected to the 6kV buses and therefore inherently complex to replace by alternatives in high human stress circumstances.

Even for low voltage equipment, like I&C, it is nearly out of the question to restore power supply, on short notice, without adequate components, tools, procedures and thorough training of the operators. Hence, the Non Conventional Means are expected to meet some predefined constraints to improve the robustness and defense in depth of the nuclear units. First, the method needs to be user friendly meaning an easy, straightforward and safe way of installation. Providing electrical power high voltage installations (e.g. pumps, fans, etc.) would give large opportunities to manage severe accidents, however the poor handiness due to heavy weights of cables and connections bring about considerable limitations. Therefore it was decided to limit the scope to low voltage installations.

At each nuclear unit an electrical low voltage grid and power supply system, as shown in Figure 4 was installed. The system consists of a ‘plug and play’ system which connects a diesel generator, via a prefabricated loose cable, to a seismically installed grid. This grid distributes the electricity to switchboards installed at the entrance of the safety trains, housing the safety related switchboards. These switchboards normally distribute the electrical power coming from the high voltage grid, via a high to low voltage transformer, to the low voltage load (I&C, valves, compressor, pumps, etc.). When the Non Conventional Equipment are used, these safety related switchboards distribute the electrical energy from the mobile diesel generator to the load. In order to do this, additional switchgears were installed. These non conventional switchgears do not connect with the inner bus bar of the switchboard, but have a connection plug on the front panel of the switchgear cabinet. Via loose prefabricated cables, connection is made to the non conventional grid.

The whole system is designed to make it impossible for the operator to get in contact with conductive electrical parts. Operator procedures are written for correct and safe line up of the non conventional power supply and each operator team receives periodically, theoretical and practical training on the Non Conventional Equipment. This results in well trained operators and makes sure that procedures are tried out, increasing the quality of implementation. Since no connection is made with the inner bus bar of the existing safety related switchboards, no false parallel resulting in short circuit is possible during testing of the equipment.

The above described installation is considered as an ultimate level of protection. Considering the design of the Belgian Nuclear Power Plants including two independent levels of safety systems, one could call this Non Conventional Equipment the ‘third level safety system’.

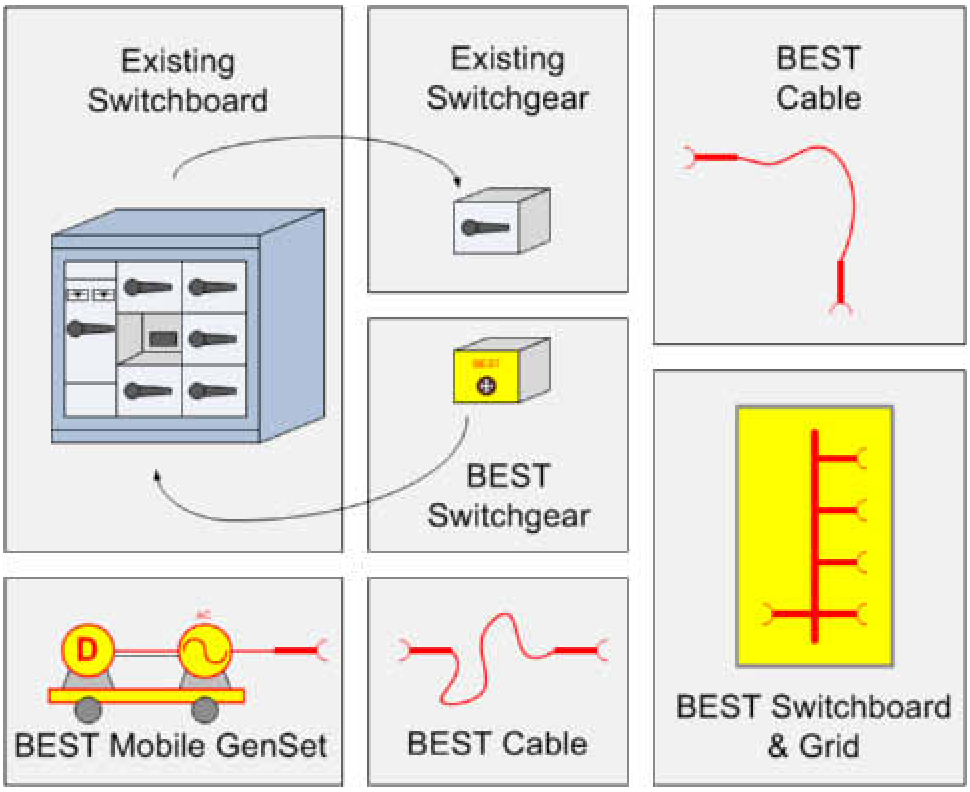


Figure 15: BEST Electrical Installation

Installed protections on Non Conventional Electrical Equipment

In general, when equipment is constructed, the design is such to protect the equipment in case parameters are out range. Therefore trip setpoints are set conservative towards the protection of the equipment itself. In nuclear applications, the first goal is not to protect the safety related equipment but, as a priority, to protect the environment against radioactive release. In case of a nuclear power plant, this means protecting the reactor core against overheating after shutdown. Therefore it is essential to exclude tripping of safety related equipment when there is no real absolute need to. Three cases are considered:

1. Setpoint is chosen too conservative towards protection of the equipment itself.
2. Spurious actuation of the protection.
3. The protection setpoint is drifting (e.g. due to temperature variation) and initiates a trip of a safety related equipment while all parameters are still in acceptable range.

The first two cases can be overcome by adequate design. First, the setpoints of the protections initiating the trip of an electrical component are preferred to be chosen more conservative towards protection of the reactor. Second, preventing an unnecessary trip because of spurious actuation is generally done by 2/3 and 2/4 logic. Avoiding the third case is done by a combination of adequate design and periodical testing.

Because of its use in very extreme and highly unlikely circumstances, the Non Conventional Equipment installation is designed to have a minimal set of protections. The non conventional electrical grid is not protected against overload (thermal protection), however only contains short circuit (magnetic) protection with respect for electrical selectivity. The diesel generator is equipped with a number of protections such as high cooling water temperature, low oil pressure, low fuel level, overload, etc. yet these protections are mainly installed to protect the generator set during testing. Each protection can be bypassed in case of emergency. In this way a generator trip, because of spurious protection signal, can be avoided or overruled. As mentioned higher, in conventional reactor instrumentation and control systems two out of three or two out of four logics are used to overcome this issue. This was not included in the design of the Non Conventional Equipment.

Conclusion

Electrical power is essential for a nuclear power plant. Although highly unlikely, in case of complete station blackout, it is recommended to have an action plan available to repower safety critical systems. Therefore Doel Nuclear Power Plant installed a seismic qualified electrical grid, powered by specific designed mobile diesel generators. This Non Conventional Equipment can be used in extreme beyond design circumstances, to repower vital electronics, pumps, compressors, etc. In high human stress circumstances this prefabricated system, along with specific severe accident procedures, can drastically reduce the outcome of a severe multi unit nuclear accident.

References

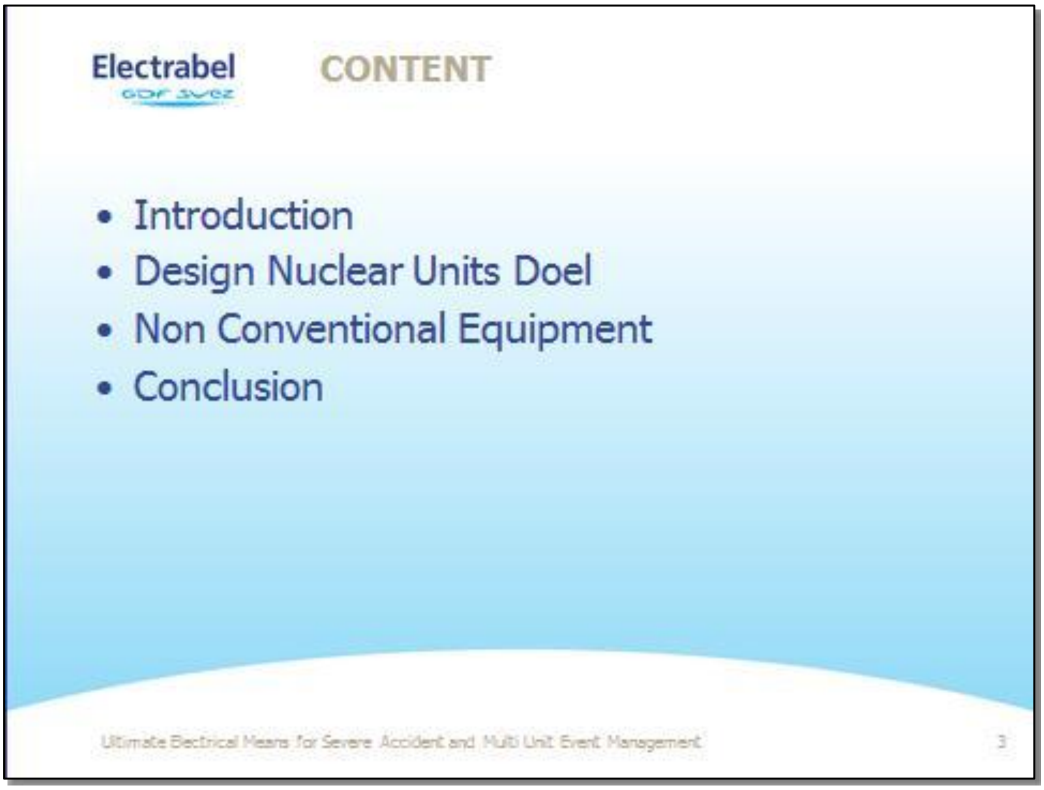
[1] *Kerncentrale Doel rapport weerstandstesten – Bijkomende veiligheidsherziening van de installaties (2011, October 31)*. Retrieved February 20, 2014, from http://www.electrabel.com

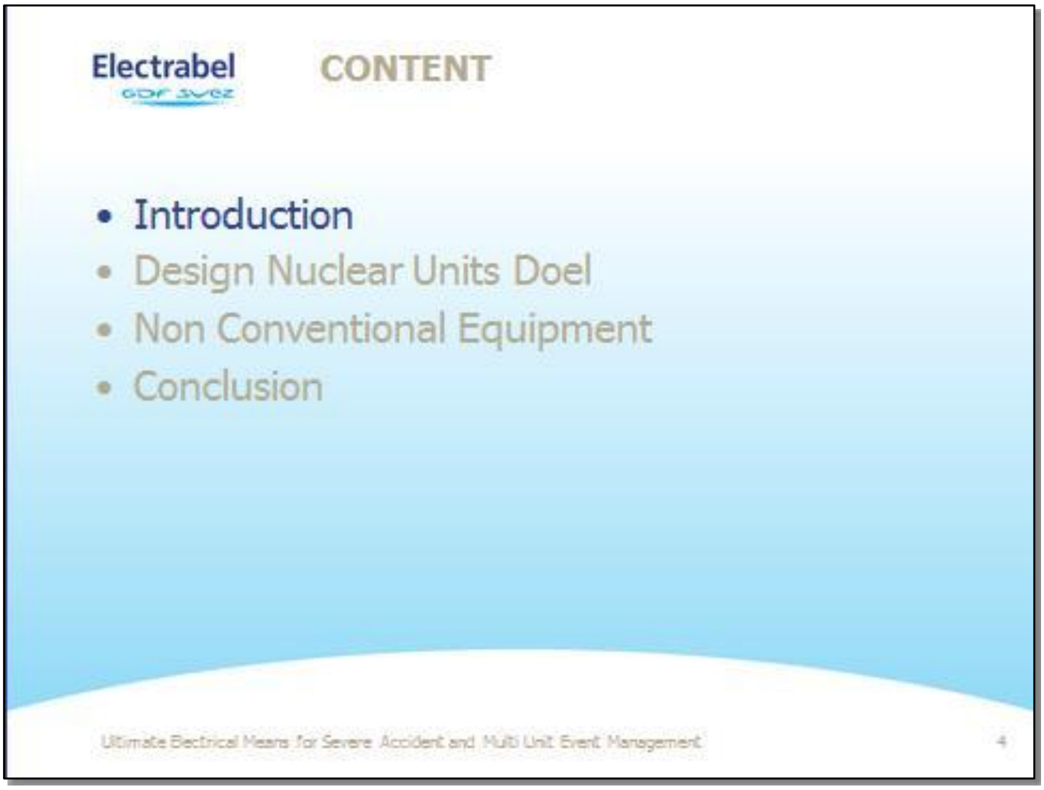
[2] *Post-Fukushima Daiichi Nuclear Accident – Lessons Learned (2013, August).* WANO Significant Operating Experience Report 2013-2 Rev 1

[3] *Fukushima Nuclear Accident Interim Report: Effects of the Earthquake and Tsunami on the Fukushima Daiichi and Daini Nuclear Power Stations, especially on electric and I&C systems and equipments (2011, July 27 @IEEE Nuclear Power Engineering Committee)*. Tokyo Electric Power Company: Akira Kawano


Electrabel
GDF SUEZ


Electrabel
GDF SUEZ
ULTIMATE ELECTRICAL MEANS FOR SEVERE ACCIDENT AND MULTI UNIT EVENT MANAGEMENT
Xavier Guisez
ROBELSYS workshop
Paris 1 – 4 April 2014
2


Electrabel
GDF SUEZ
CONTENT
• Introduction
• Design Nuclear Units Doel
• Non Conventional Equipment
• Conclusion
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
3


Electrabel
GDF SUEZ
CONTENT
• Introduction
• Design Nuclear Units Doel
• Non Conventional Equipment
• Conclusion
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
4

Electrabel
GDF SUEZ

INTRODUCTION

Electrabel

Electrabel is a limited company whose headquarters office is located in Brussels, Belgium. It is part of GDF SUEZ, a world leader in energy and the environment, which owns 100% of it. The company is active in the **production of electricity** and in the **selling of electricity, natural gas and energy services** to **retail and business** customers.

Electrabel
GDF SUEZ

INTRODUCTION

Key Figures

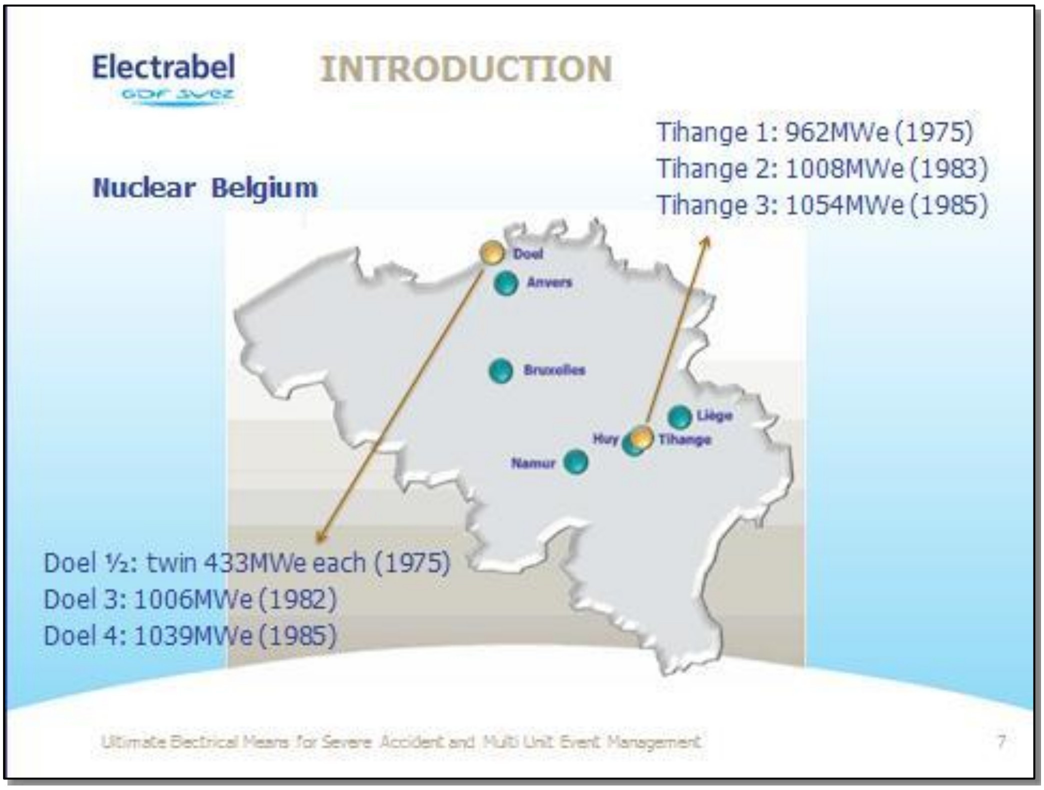
Key figures for 2012, Electrabel in Belgium

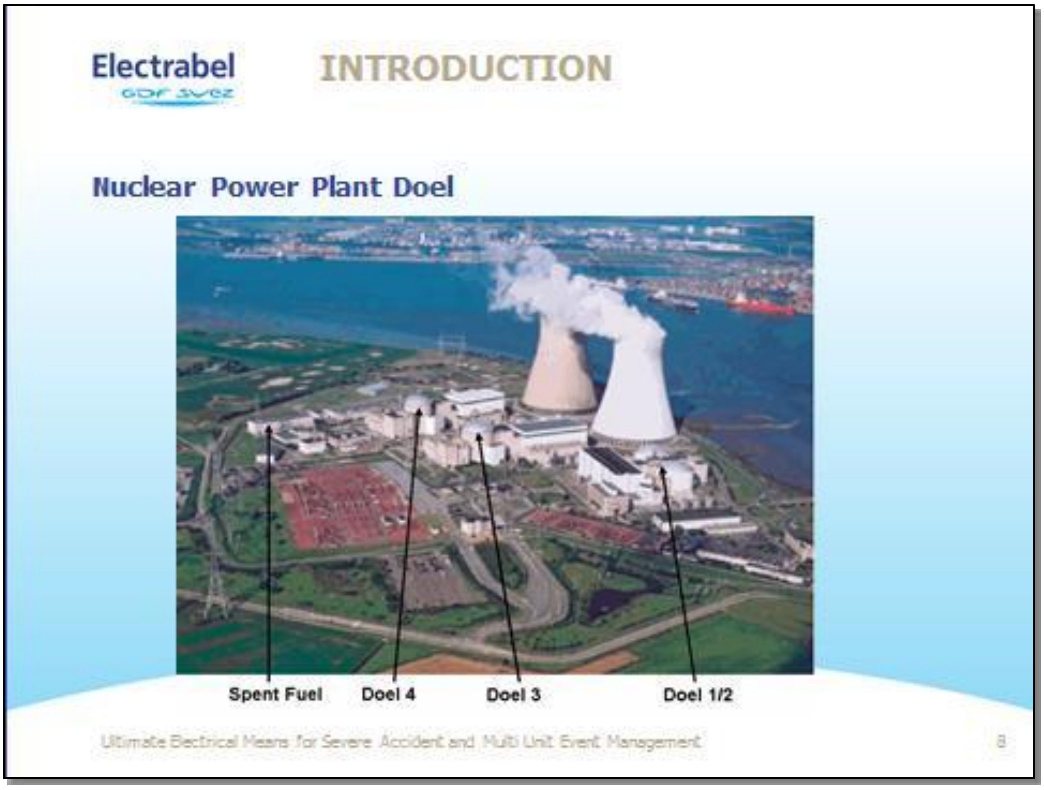
	Total	Renewable energy share	Share without carbon emissions	Staff
Generating capacity	9.9 GW	5.0%	58.0%	5 429
Generation	42.6 TWh	5.1%	65.5%	

Renewable energy capacity	489 MW
Carbon emissions	168 g/KWh

	Total	Electric power	Natural gas	Electrical power + natural gas
Sales	107.3 TWh	56.6 TWh	50.7 TWh	
Customers	3.1 million	1.44 million	0.11 million	1.54 million

The generation (capacity) figures relate to the Electrabel share.


Electrabel
GDF SUEZ
INTRODUCTION
Nuclear Belgium
Tihange 1: 962MWe (1975)
Tihange 2: 1008MWe (1983)
Tihange 3: 1054MWe (1985)
Doel
Anvers
Bruxelles
Liège
Huy
Tihange
Namur
Doel ½: twin 433MWe each (1975)
Doel 3: 1006MWe (1982)
Doel 4: 1039MWe (1985)
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
7


Electrabel
GDF SUEZ
INTRODUCTION
Nuclear Power Plant Doel
Spent Fuel
Doel 4
Doel 3
Doel 1/2
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
8

Electrabel GDF SUEZ

CONTENT

- Introduction
- **Design Nuclear Units Doel**
- Non Conventional Equipment
- Conclusion

Electrabel GDF SUEZ

DESIGN NUCLEAR UNITS DOEL

Basis design

	Type	Thermal Power (MWth)	First Criticality	Reactor Building	Steam Generator Replacement	Design
Doel 1	PWR (2 loop)	1312	1974	Double Containment (steel and concrete)	2009	Westinghouse
Doel 2	PWR (2 loop)	1312	1975	Double Containment (steel and concrete)	2004	Westinghouse
Doel 3	PWR (3 loop)	3064	1982	Double Containment (concrete with liner and concrete)	1993	Framatome
Doel 4	PWR (3 loop)	3000	1985	Double Containment (concrete with liner and concrete)	1997	Westinghouse
SCG	-	-	-	-	-	Tractebel Engineering

Electrabel GDF SUEZ

DESIGN NUCLEAR UNITS DOEL

Key safety features

- Double containment reactor building
- Two independent levels of emergency systems
  - ✓ First level: internal accidents
  - ✓ Second level: external hazards (bunkerized)
- Two possibilities of ultimate heat sink
  - ✓ River
  - ✓ Cooling ponds
- Extra common emergency diesel generator (Doel 34)

Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 11

Electrabel GDF SUEZ

DESIGN NUCLEAR UNITS DOEL

Electrical Design

- 5 x 400kV lines
- 2 x 150 kV lines (enough capacity for auxiliaries of 4 plants)
- Doel 1 & Doel 2
  - ✓ (4 + 1 spare) x first level emergency diesel generators
  - ✓ 2 x second level emergency diesel generators
  - ✓ Battery backed safety buses for I&C
  - ✓ 2 x non nuclear safety related diesel generators
- Doel 3 & Doel 4
  - ✓ 3 x first level emergency diesel generators
  - ✓ 3 x second level emergency diesel generators
  - ✓ Battery backed safety buses for I&C
  - ✓ 2 x non nuclear safety related diesel generators
  - ✓ 1 x common reserve emergency diesel generator

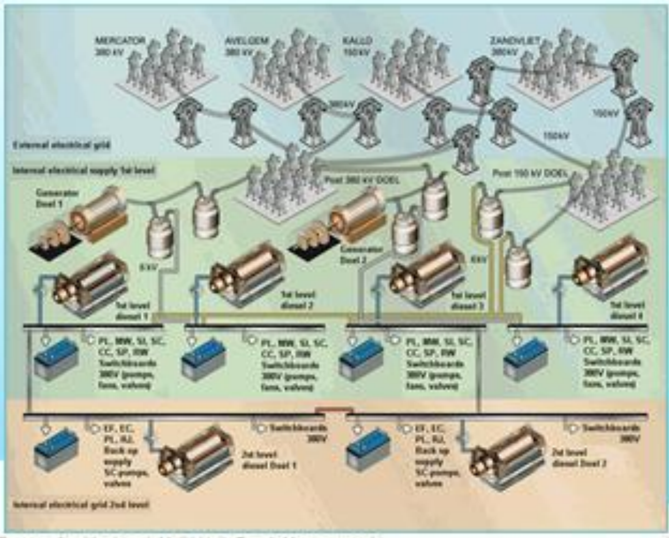
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 12

Electrabel
GDF SUEZ

DESIGN NUCLEAR UNITS DOEL

Electrical Design

Doel 1 & Doel 2



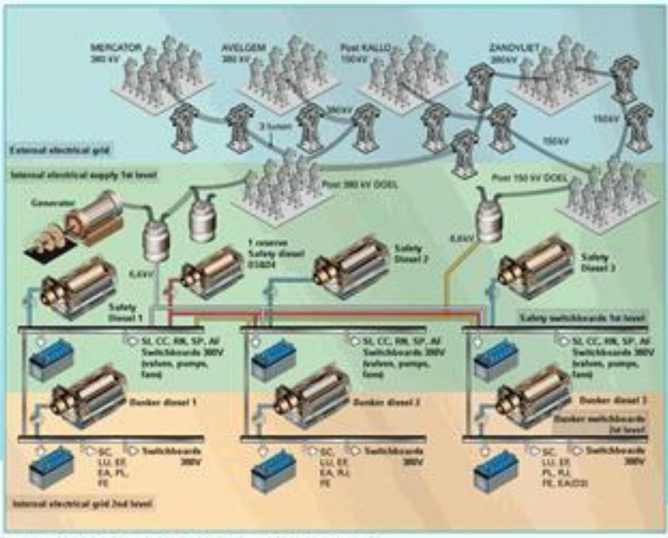
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 13

Electrabel
GDF SUEZ

DESIGN NUCLEAR UNITS DOEL

Electrical Design

Doel 3 & Doel 4



Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 14

Electrabel
GDF SUEZ

CONTENT

- Introduction
- Design Nuclear Units Doel
- Non Conventional Equipment
- Conclusion

Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 15

Electrabel
GDF SUEZ

NON CONVENTIONAL EQUIPMENT

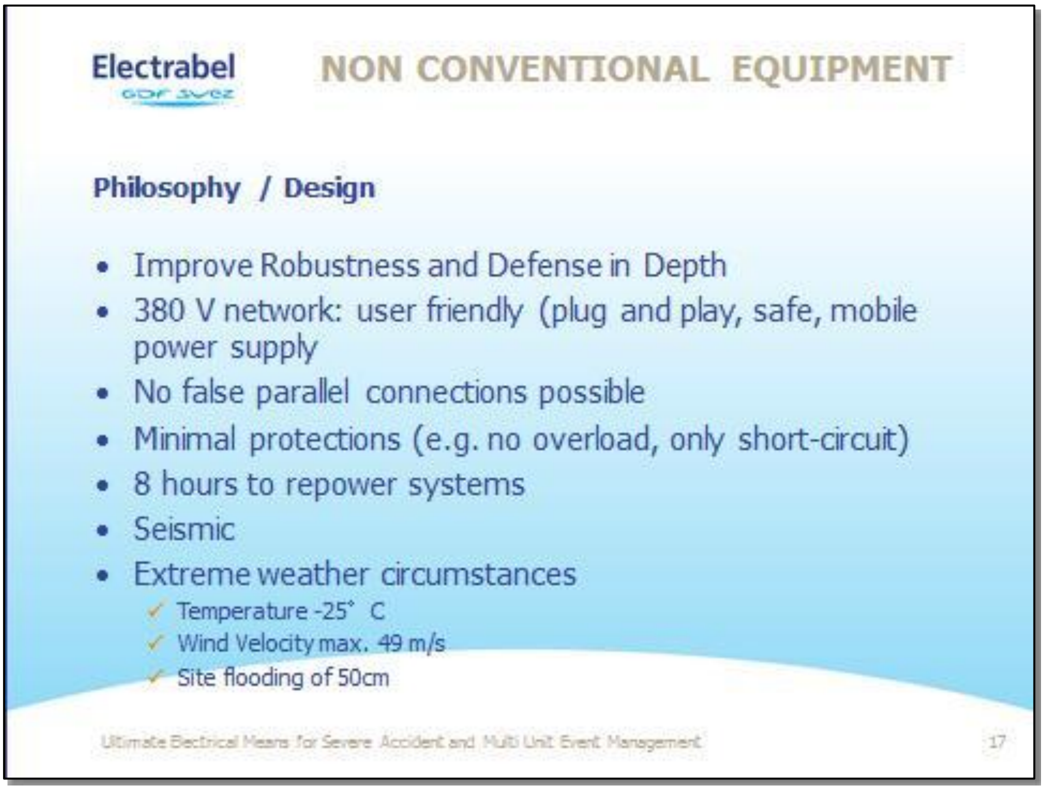
Action Plan

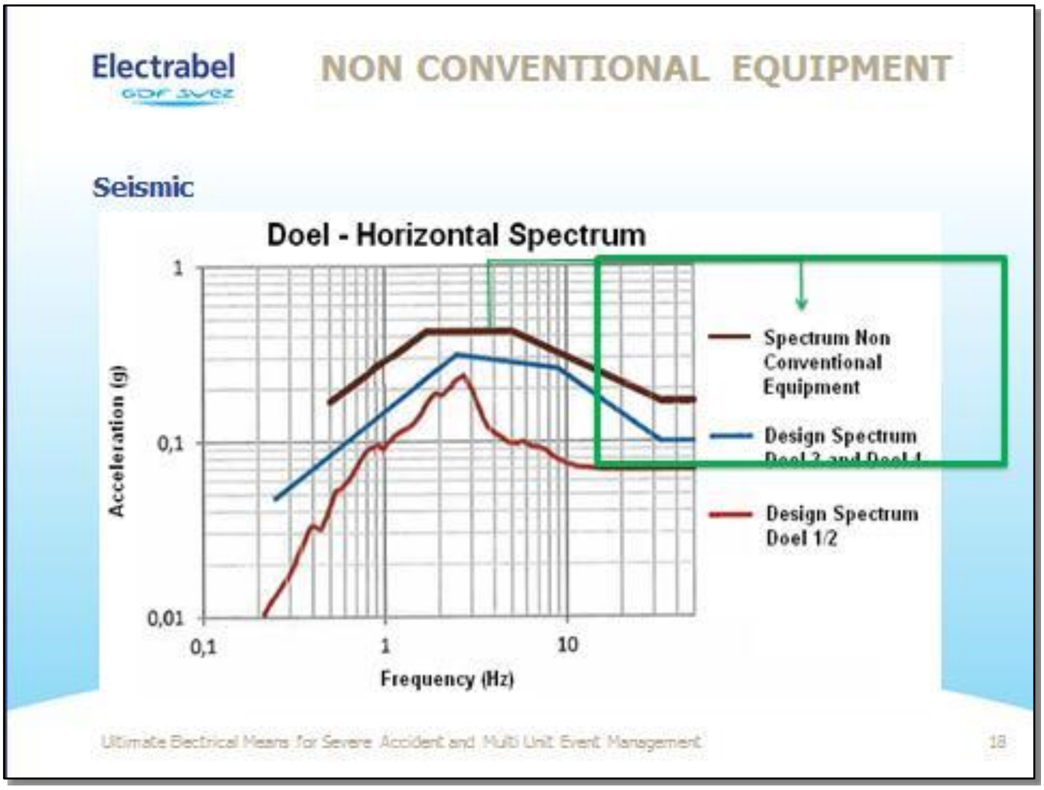
- In the framework of the Belgian Stress Tests, Electrabel agreed to implement an action plan.

➡ Purchase of mobile generator sets and installation of an independent electrical grid with easy connection to safety equipment to mitigate the effects of a severe accident and/or multi unit event, is part of that action plan.

https://www.electrabel.com/en/corporate/company-news/topics/resistance-test

Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 16

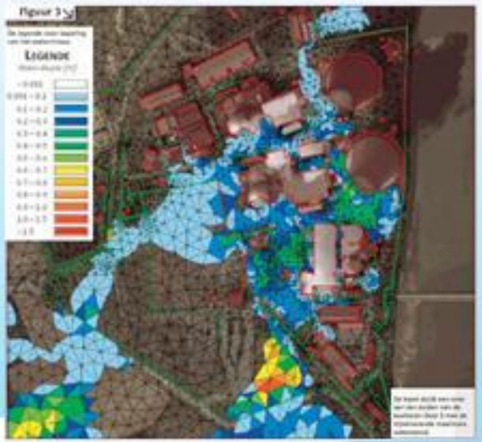

Electrabel
GDF SUEZ
NON CONVENTIONAL EQUIPMENT
Philosophy / Design
• Improve Robustness and Defense in Depth
• 380 V network: user friendly (plug and play, safe, mobile power supply
• No false parallel connections possible
• Minimal protections (e.g. no overload, only short-circuit)
• 8 hours to repower systems
• Seismic
• Extreme weather circumstances
✓ Temperature -25° C
✓ Wind Velocity max. 49 m/s
✓ Site flooding of 50cm
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
17


Electrabel
GDF SUEZ
NON CONVENTIONAL EQUIPMENT
Seismic
Doel - Horizontal Spectrum
1
0,1
0,01
Acceleration (g)
0,1
1
10
Frequency (Hz)
Spectrum Non Conventional Equipment
Design Spectrum
Design Spectrum Doel 1/2
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
18

Electrabel
GDF SUEZ

NON CONVENTIONAL EQUIPMENT

Flooding

Cooling ponds

Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 19

Electrabel
GDF SUEZ

NON CONVENTIONAL EQUIPMENT

Powered Systems

- Safety Valves
  - ✓ To isolate SI-accumulators (avoid non-condensable gases in primary circuit)
    - Jeopardizing Natural Circulation and Residual Heat removal
  - ✓ Actuation of Pressurizer Relief Valves (Avoid High Pressure Core Ejection)
  - ✓ Open Steam Generator Relief Valves (accelerated primary cooling)
- Air Compressor
  - ✓ Pneumatic Operated Relief Valves

Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 20

Electrabel GDF SUEZ

NON CONVENTIONAL EQUIPMENT

Powered Systems

- Safety Related Ventilation
  - ✓ Limit/Control ambient temperature
- CVCS-pumps (380V)
  - ✓ Water inventory in primary circuit
- Rectifiers/Inverters
  - ✓ Instrumentation and control

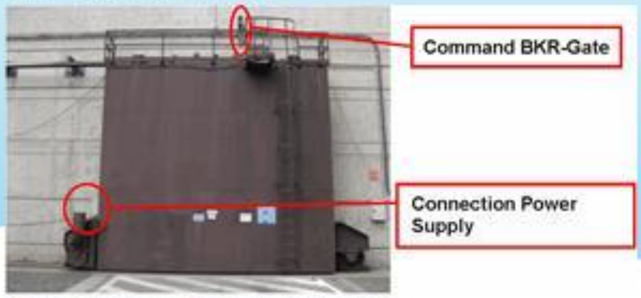
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 21

Electrabel GDF SUEZ

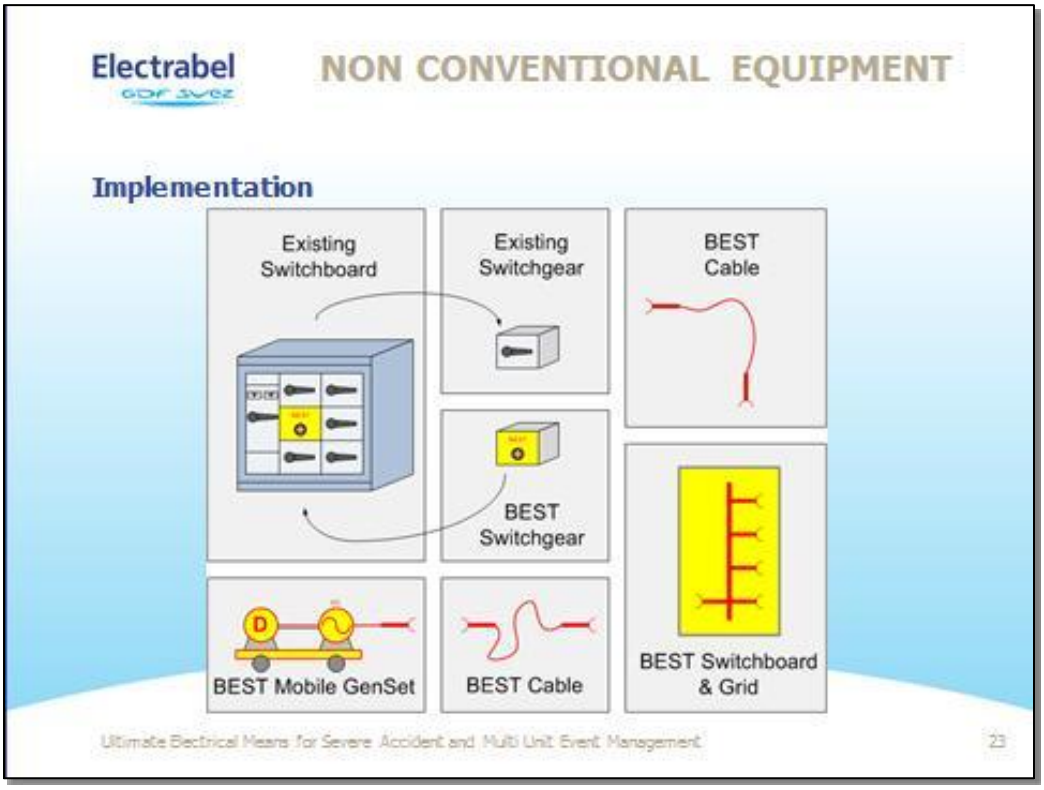
NON CONVENTIONAL EQUIPMENT

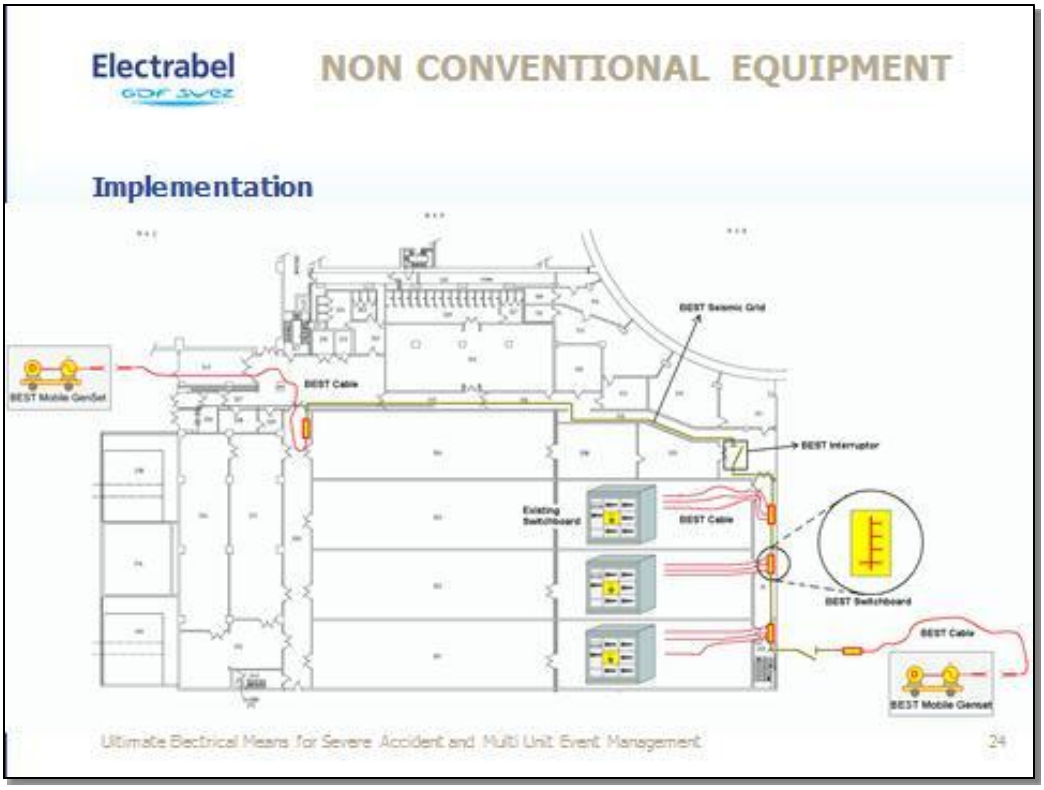
Powered Systems

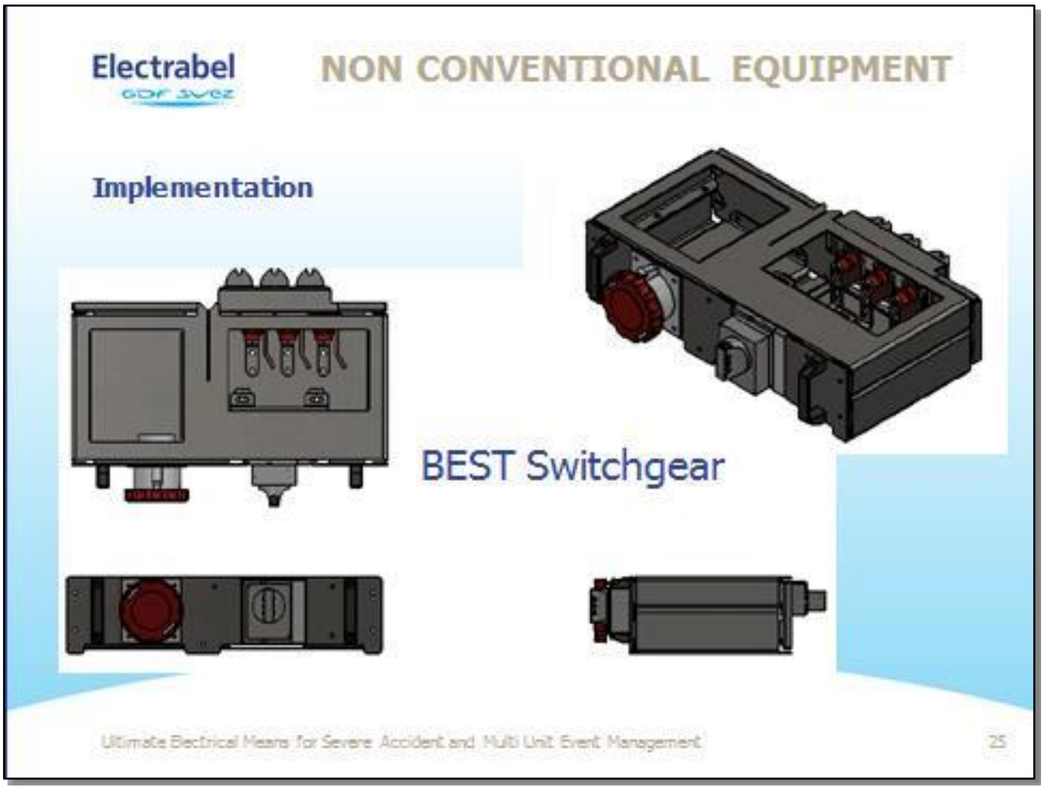
- Emergency infrastructure
- Reinforced doors to bunkerized buildings
  - ➡ Access to Non Conventional Grid



Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 22


Electrabel
GDF SUEZ
NON CONVENTIONAL EQUIPMENT
Implementation
Existing Switchboard
Existing Switchgear
BEST Cable
BEST Switchgear
BEST Mobile GenSet
BEST Cable
BEST Switchboard & Grid
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
23


Electrabel
GDF SUEZ
NON CONVENTIONAL EQUIPMENT
Implementation
BEST Seismic Grid
BEST Mobile GenSet
BEST Cable
BEST Interruptor
Existing Switchboard
BEST Cable
BEST Switchboard
BEST Cable
BEST Mobile Genset
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
24


Electrabel
GDF SUEZ
NON CONVENTIONAL EQUIPMENT
Implementation
BEST Switchgear
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
25


Electrabel
GDF SUEZ
NON CONVENTIONAL EQUIPMENT
Implementation
BEST
BEST
BEST Grid
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
26

Electrabel GDF SUEZ

NON CONVENTIONAL EQUIPMENT

Implementation

Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 27

Electrabel GDF SUEZ

NON CONVENTIONAL EQUIPMENT

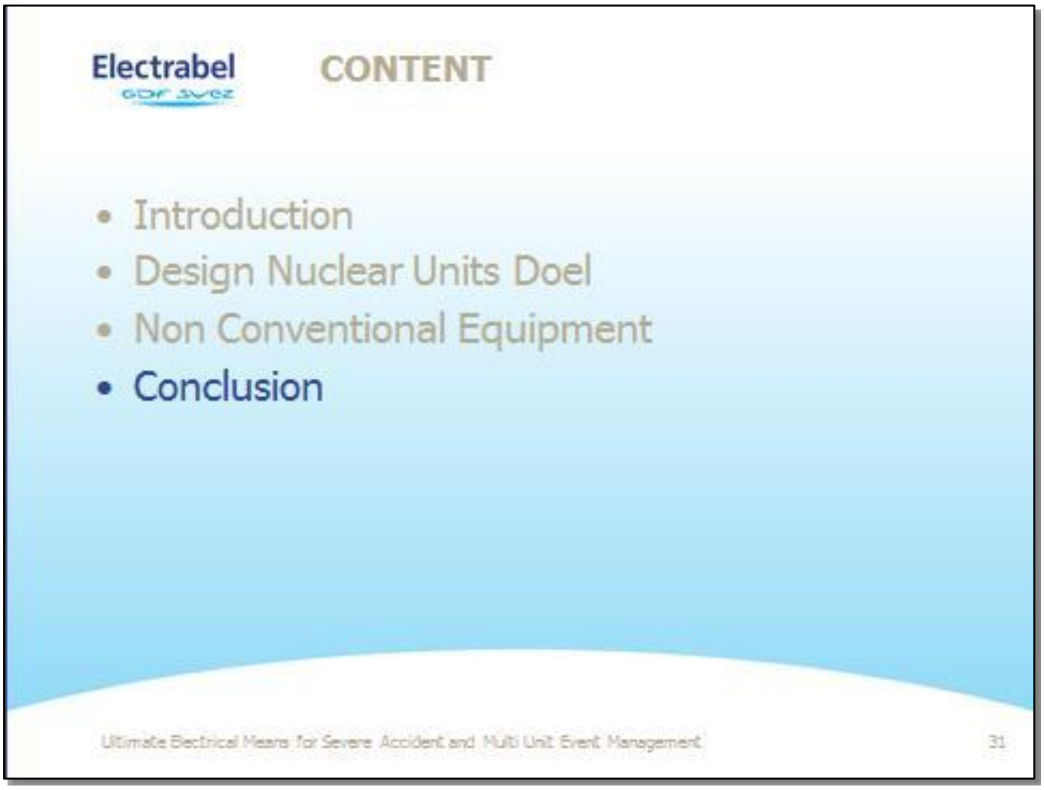
Design GenSets

- Operable under severe weather conditions
  - ✓ Temperature -25° C
  - ✓ Wind Velocity max. 49 m/s
  - ✓ Site flooding of 50cm
  - ✓ Special Cable connections
- Seismic
- Electrical preheating
- Jacket water heater (manual activation in case of Blackout)
- Battle mode (possibilities to overrule protections and software)
- N+1 redundancy and universal use on all entities
- Fuel autonomy of 12 hours + fuel available on site for at least 72h
- Wire and Terminal numbering (one to one)

Ultimate Electrical Means for Severe Accident and Multi Unit Event Management 28


Electrabel
GDF SUEZ
NON CONVENTIONAL EQUIPMENT
Storage Building
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
29


Electrabel
GDF SUEZ
NON CONVENTIONAL EQUIPMENT
Storage Building
Mobile GenSets
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
30


Electrabel
GDF SUEZ
CONTENT
• Introduction
• Design Nuclear Units Doel
• Non Conventional Equipment
• Conclusion
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
31


Electrabel
GDF SUEZ
CONCLUSION
• Electrical Power Supply is essential for a NPP
• It is recommended to have an Action Plan available and operable to manage beyond design basis circumstances
• Non Conventional Equipment Doel Nuclear Power Plant
✓ Extreme Beyond Design hazards
✓ Seismic qualified
✓ Extreme weather
✓ High Human Stress situations
✓ 'Plug and Play' system
✓ Some specific design requirements
✓ Specific severe accident/multi unit event procedures
THIRD LEVEL OF PROTECTION SYSTEM
Ultimate Electrical Means for Severe Accident and Multi Unit Event Management
32


You've
got the
energy
Electrabel
GDF SUEZ

SESSION SIX

"Margin assessments for modern power electronics"

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

Modification to Battery Chargers & Inverters Units
Florent Raison (AEG Power Solutions, Germany)

Recent Operating Experience involving Power Electronics Failure in Korea Nuclear Power Plants

Jaedo LEE
KINS, Korea

Abstract

Recently, modern power electronics devices for electrical component were steadily increased in electrical systems which used for main power control and protection. To upgrade the system reliability we recommended the redundancy for electrical equipment trip system. The past several years, Korean Nuclear power plants have changed the electrical control and protection systems (Auto Voltage Regulator, Power Protection Relay) for main generator and main power protection relay systems. In this paper we deal with operating experience involving modern solid state power electronics failure in Korean nuclear power plants. One of the failures we will discuss the degraded phenomenon of power electronics device for CEDMCS(Control Element Drive Mechanism Control System). As the result of the failure we concerned about the modification for trip source of main generator excitation systems and others. We present an interesting issue for modern solid state devices (IGBT, Thyristors).

1. Power Electronics Devices in NPPs

With the growth of power generation capacity, the capacity of each generator unit has amazingly increased. Also, progress in semiconductor technology has invited use of the thyristor for an excitation system. In generally, power electronics device mainly was used for power conversion for specific sources. Uninterruptible Power System (Charger, Inverter), Auto Voltage Regulator (generator), Control Element Drive Mechanism Control System (CEDMCS) were consisted.

Generator AVR has changed the rotary type into excitation type for development of digital technology. There have been three or four groups of rectifier system for excitation controller. Each group rectifier is composed of six-thyristor components.

During plant operations, each control rod group is moved by a Control Element Drive Mechanism. Four electromagnetic coils are used within each CEDM to move and hold a CEDM in place. The voltage applied to each coil is controlled by the Control Element Drive Mechanism Control System (CEDMCS). CEDMCS receives three phase voltage from a motor-generator set. To convert the three phase AC voltage provided by the motor-generator set to DC voltage needed to control each CEDM coil, the CEDMCS uses trio of silicon controlled rectifiers (SCRs) that are located within the power switch assembly of CEDMCS.

So power electronics have difficulty about judging a given life time of working condition. Though some manufactures recommend defining replacement period of electrical components such as electrolyte capacitors, resistors, relay and so forth, Plant's staff have checked electrical characteristics during overhaul. We have taken various actions to prevent transient plant condition and improve the reliability of operation.

This subject accounts for the fault trip and cause of CEDMCS, AVR which made of the electronics device lately. We also present corrective actions for long term or short term.

2. Recent Power Electronics Failure in Korea NPPs

Title 1: Shin-wolsung Unit 1 Reactor Trip by CEA position deviation due to CEDMCS failure
Event Description

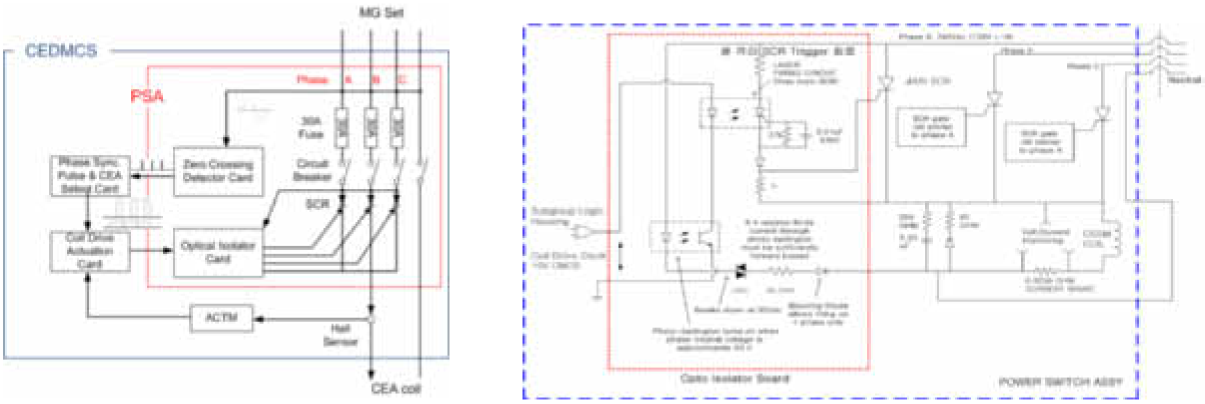


Fig1. SCR and Opto-Isolator Card Configuration

At 10:53 on August 19 in 2012 during normal operation, #24 Control Element Assembly (CEA) fell due to failure of A phase Silicon Controlled Rectifier(SCR) which is in actuating coil logic of the CEA belong to #6 subgroup of shutdown group. The reactor protection signal occurred due to the position deviation among CEAs, and the reactor was tripped. Upon investigation, the leading-in breaker was opened by excessive fault current due to short between A and B phases after the failure of A phase SCR in 3 phase logic powered by a MG set, and the fuse of A/B phase blew. As a result, there was power loss in #24 CEA actuating coil and the CEA fell.

Title 2: Shin-Kori Unit 1 Reactor Trip by CEA position deviation due to CEDMCS failure
Event Description

At 8:10 on October 2 in 2012 during normal operation, the reactor was tripped automatically due to reactor protection signal by Control Element Assembly (CEA) falling. Upon investigation, there was fusing in the Power Switch Assembly (PSA), and actuating power loss occurred due to failure of silicon controlled rectifier in #7 CEA upper gripper A phase circuit of #3 PSA in the Control Element Drive Mechanism Control System (CEDMCS). Position deviation among CEAs occurred by #7 CEA falling and the reactor was tripped due to reactor protection signal (DNBR-low) in the core protection calculator.

Title3: Yonggwang Unit 1 Reactor Trip resulted from Excitor and Generator Trip due to Grounding at Yonggwang Unit 4
Event Description

On June 3, 2009, a grounding occurred at the phase-'A' Gas Insulated Bus (GIB) of Yonggwang Unit 4 (YGN-4) which was resulted from a flashover between the GIB external enclosure and the internal conductor. The grounding resulted in opening of the power circuit breaker (PCB) and trip of the turbine/generator (TBN/GEN) and caused the reactor power cutback system (RPCS) to actuate for YGN-4 which could reduce the reactor power only and thus escaping from the reactor trip. However, the grounding caused YGN Unit 1 to experience a phase difference for the main excitor and to actuate the phase differential relay which resulted in the exciter and the main generator trip. Subsequently, the reactor was tripped by the turbine trip. All the safety systems functioned as designed, however, the non-safety

13.8kV bus was transferred from the Unit Auxiliary Transformer (UAT) to the Startup Unit Transformer (SUT), not in a 'fast transfer mode'(within 6 cycles) but in a 'slow transfer mode' (30 ~ 60 cycles) due to the difference of phase angle between the UAT bus and the SUT bus. Upon investigation, as a result of the YGN-4 grounding, three out of three phase differential relays were found to be actuated for YGN-1 causing the excitor and generator trip while one out of three those relays was actuated for YGN-2 not causing any transient. The grounding at YGN-4 was found to be due to a bad contact of the 'tulip contact' inside the GIB which appeared to be due to incomplete manufacturing or fault construction of the 'tulip contact'. There was an indication of flash-over inside the GIB which caused to experience such grounding. The phase angle difference was due to phase-'A' grounding. Also, it was found that one non-safety class Uninterrupted Power Supply (UPS) showed a momentary power loss during the electrical transient. A detailed investigation is to be followed. The Main Control Room (MCR) operators followed the appropriate Emergency Operating Procedures (EOPs) in response to the reactor trip and confirmed safe reactor shutdown. All the safety functions were not challenged and there was no adverse effect on the plant safety or radioactive material release to the environment as a result of this event.

3. Consideration of Trip Causes and Corrective Action

Title1 and title2 have similar phenomenon for reactor trip by CEA position deviation due to CEDMCS failure. The gap between the two events is the fault mechanism due to the continuous time of fusing current and breaker open operation characteristic. The main causes are over-temperature conditions for operating devices.

We may be several conditions that could result in an SCR failure due to an over-temperature condition :

(1) Exceeding maximum repetitive peak or off-state voltage due to notches on the 3 phase MG bus due to misadjusted phase firing. Overheating would result from slower than normal turn-on of the SCR

(2) Exceeding maximum critical rate of rise of the off-state voltage due to notches on the 3 phase MG bus due to misadjusted phase firing. Overheating would result from slower than normal turn-on of the SCR

(3) Excessive operating temperature within the CEDMCS cabinet. For example, overheating could occur if air flow in the cabinet was blocked.

(4) Insufficient gate voltage input to the SCR can cause an over temperature condition and create a short in a SCR junction, thus causing the SCR failure.

The following corrective actions were implemented the replacement of broken Power Switch Assembly (PSA), and operational test inspection of total PSAs, and CEA verification test. As for long term corrective action, the old CEDMCS will get to be replaced by the redundancy system of CEDMCS's power source. Recovery blocking voltage of SCRs devices was increased from 800V to 1,200V. That is to minimize the probability of thermal damage and enhance the reliability of equipment.

Title 3 is the event that YGN-1 reactor trip was due to the grounding occurred at YGN-4 and the grounding was found to be due to a bad contact of the 'tulip contact' inside the GIB which appeared to have resulted from incomplete manufacturing or fault construction of the tulip contact. YGN-1 also experienced non-safety UPS failure momentarily during the electrical transient which resulted in a loss of power for the plant computer. Hence, there were not enough data for the sequence of event (SOE).

For the electrical safety of domestic Nuclear Power Plant (NPP), the following corrective actions were implemented and planned.

(1) Replaced the failed GIB with a new one

(2) Plan to establish comprehensive and systematic study for the UPS integrity

(3) review the excitor system protection function in relation to one single fault events

- removing the synchronization transformer fault trip signal of excitor controller

- review thyristor capacity which can be operable possibility for two phase excitor controller on a phase fault

4. Results and discussion

Some laboratory researched the study that was defined a methodology that allows to establish the correlation between accelerated ageing tests and the real working conditions of a thyristor[1][2]. As part of the preventive maintenance, we need to replace these components periodically after a fixed number of years of operation. However, it has been observed that their electrical parameters are still within the specifications. Actually the residual lifetime of these devices is not known and perhaps the maintenance period could be widely lengthened. Their evaluation methods were presented by tests of the lifetime of a thyristor.

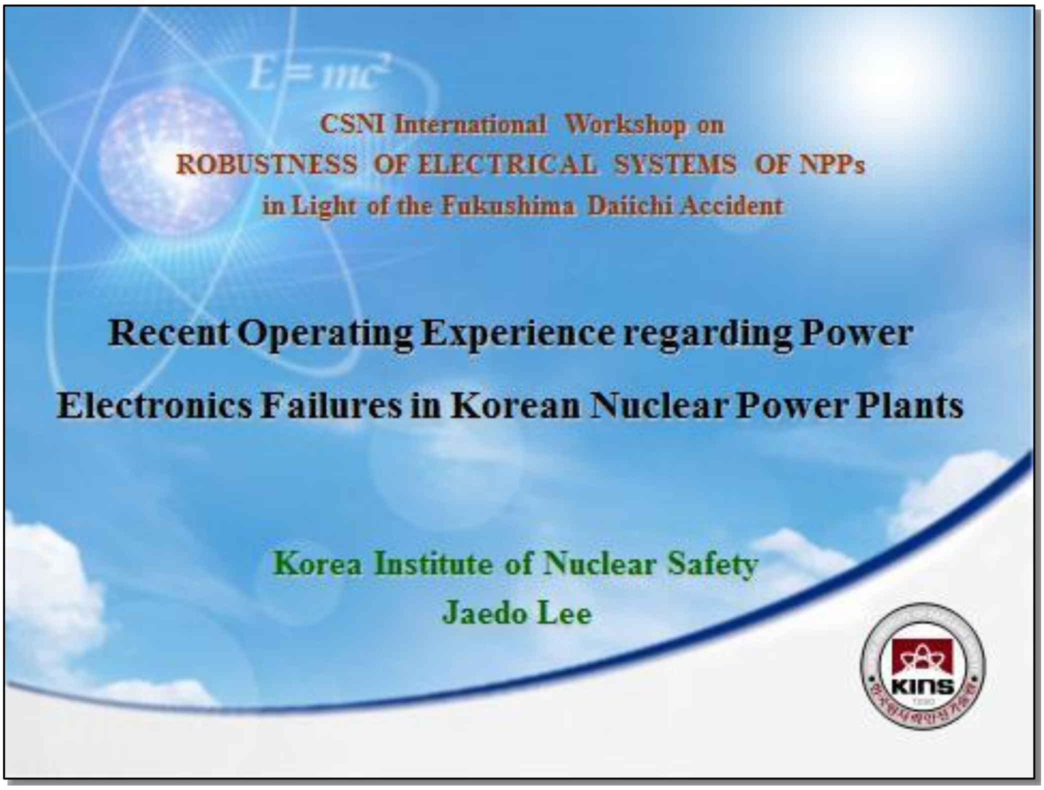
From these events, we can conclude that the improvement of the modern power electronics is as follow. In the case of type1 and type2, we should change CEDMCS into dual power controller and supply a close loop current method by the feedback control the power converter circuit.

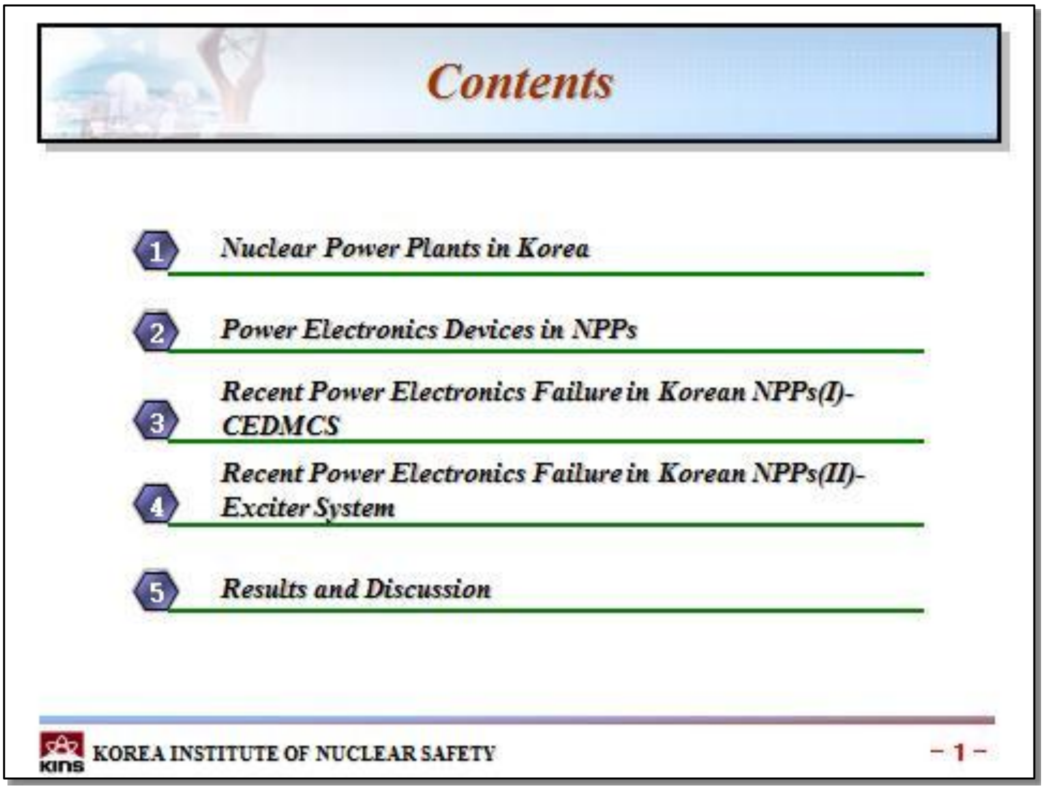
The type 3 case was reviewed in every a point of view of the synchronization transformer fault signal for DS-DEX exciter controller. Consequently, a phase unbalance detection function of synchronization transformer faults was removed due to the protection of controller itself. On operating two phase a phase fault, we verified that thyristor load current can be operable possibility for two phase excitor controller.

Through the improvement of CEDMCS and Excitor, we should have been informed the uncertainties in the real stress values and the equipment capability.

References

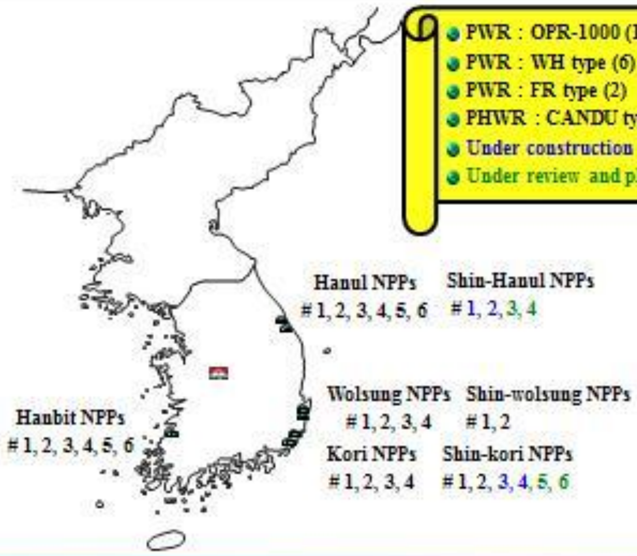
[1] Alexandrine Guedon-Gracia, Eric Woirgard, Christian Zardini. Guillaume Simon, “An assessment of the connection between the working operations of a thyristor system used in a power plant and accelerated ageing tests.”, 2004 IEEE International Symposium on Industrial Electronics, vol. 2, page 803-807.
[2] Milan Cepek, Chandra P.Krishnayya, “Thyristor Aging” 1998 POWERCON, vol. 1 page 649-653.
[3] Nagano S., Tari M., Inohara T., Koyanagi E., “Evaluation of Field Insulation of Turbine-Generators with Higher Thyristor Excitation” 1986 Power Engineering Review, vol. PER-6, page 47-48.
[4] Operational Performance Information System for Nuclear Power Plant (OPIS), http://opis.kins.re.kr


E = mc²
CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs
in Light of the Fukushima Daiichi Accident
Recent Operating Experience regarding Power
Electronics Failures in Korean Nuclear Power Plants
Korea Institute of Nuclear Safety
Jaedo Lee
KINS


Contents
1 Nuclear Power Plants in Korea
2 Power Electronics Devices in NPPs
3 Recent Power Electronics Failure in Korean NPPs(I)-CEDMCS
4 Recent Power Electronics Failure in Korean NPPs(II)-Exciter System
5 Results and Discussion
KOREA INSTITUTE OF NUCLEAR SAFETY
- 1 -

NPPs in South Korea

- PWR : OPR-1000 (12)
- PWR : WH type (6)
- PWR : FR type (2)
- PHWR : CANDU type (4)
- Under construction : APR-1400(4)
- Under review and plan : APR-1400(4)



KOREA INSTITUTE OF NUCLEAR SAFETY - 2 -

Power Electronics Devices in NPPs

- **Components**
  - Progress in semiconductor technology have driven use of power systems.
  - Power electronics devices mainly were used for power conversion, power controller, etc.
  - They consist of uninterruptible power system, exciter system and control element drive mechanism control system, etc.

UPS(Inverter)

CEDMCS(Power Switching Assembly)

KOREA INSTITUTE OF NUCLEAR SAFETY - 3 -

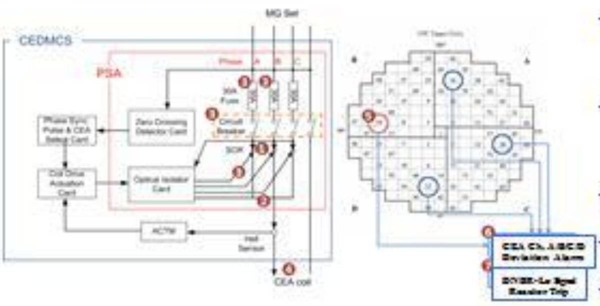
Recent Power Electronics Failures in Korean NPPs(I-1)

- Title 1 : **Shin-wolsung Unit 1 Reactor Trip by CEA position deviation due to CEDMCS failure**
  - ✓ On August 19, 2012 during normal operation, #24 Control Element Assembly fell due to failure of phase A Silicon Controlled Rectifier(SCR) which is in actuating coil logic of the CEA belong to subgroup #6 of shutdown group. The reactor protection signal occurred due to the position deviation among CEAs, and the reactor was tripped.
- Title 2 : **Shin-Kori Unit 1 Reactor Trip by CEA position deviation due to CEDMCS failure**
  - ✓ On October 2, 2012 during normal operation, the reactor was tripped automatically due to reactor protection signal by Control Element Assembly falling. Upon investigation, there was fusing in the Power Switch Assembly (PSA) due to failure of silicon controlled rectifier in #7 CEA upper gripper of phase A circuit of #3 PSA in the Control Element Drive Mechanism Control System (CEDMCS). Position deviation among CEAs occurred by #7 CEA falling and the reactor was tripped.

KOREA INSTITUTE OF NUCLEAR SAFETY - 4 -

Shin-wolsung Unit 1 Reactor Trip Causes

- Title 1 : **Shin-wolsung Unit 1 Reactor Trip by CEA position deviation due to CEDMCS failure**

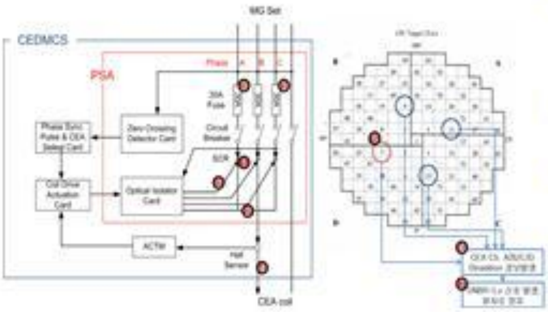


- ✓ Failure of phase A silicon controlled rectifier in #24 PSA
- ✓ Excessive fault current by phases A and B short, on the gate on phase B SCR
- ✓ Fuse of Phases A and B blew
- ✓ CEA #24 drop by power loss
- ✓ Reactor trip caused by DNBR-Lo

KOREA INSTITUTE OF NUCLEAR SAFETY - 5 -

Shin-Kori Unit 1 Reactor Trip Causes

➢ Title 2 : **Shin-Kori Unit 1 Reactor Trip by CEA position deviation due to CEDMCS failure**



- ✓ Failure of silicon controlled rectifier phase A of CEA upper gripper #7
- ✓ Excessive fault current by phases A and C short
- ✓ Fuse of Phases A and B blew
- ✓ CEA#7 drop by power loss
- ✓ Reactor trip caused by DNBR-Lo

KOREA INSTITUTE OF NUCLEAR SAFETY – 6 –

Recent Power Electronics Failures in Korean NPPs (I-2)

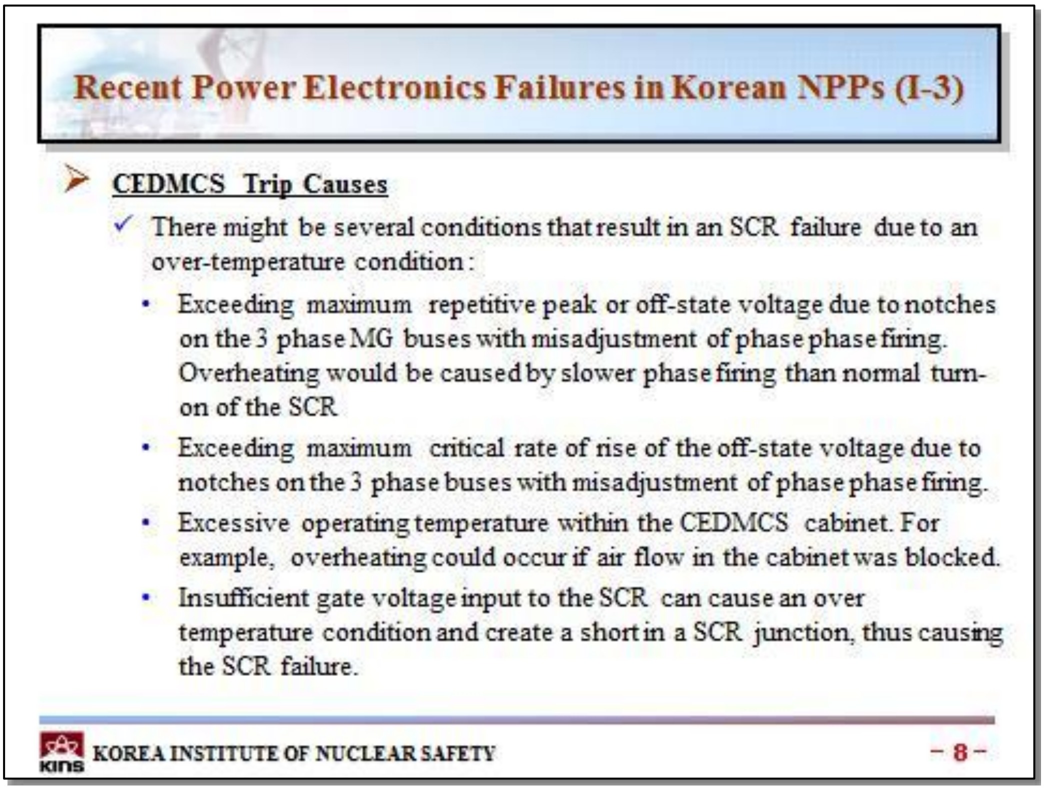
➢ **Comparison of Shin-wolsung Unit 1 and Shin-Kori Unit 1 Reactor Trip by CEA position deviation due to CEDMCS failures**

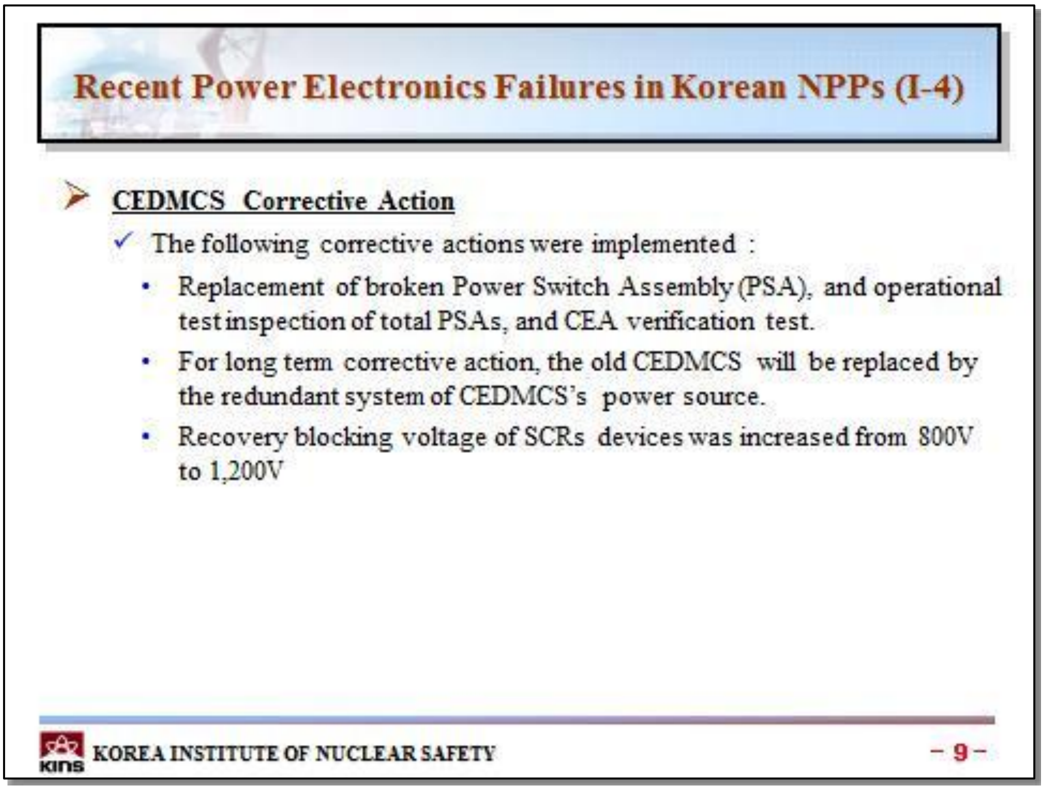
- ✓ The difference between the two events is the fault mechanism due to the continuous time of fusing current and breaker open operation characteristic

CONTENT	Criteria	Shin-Wolsung #1 (control element assembly #24 UG SCR)			Shin-Kori #1 (control element assembly #7 UG SCR)		
		Phase A	Phase B	Phase C	Phase A	Phase B	Phase C
Anode-Cathode	2MΩ above	1.64Ω	10.55MΩ	10.78MΩ	2.6Ω	8.6Ω	10.1MΩ
Gate-Cathode	20~50Ω Above	2.36Ω	26.70Ω	36.16Ω	1.7Ω	27.6Ω	29.3Ω
Check Results		Abnormal	Normal	Normal	Abnormal	Normal	Normal

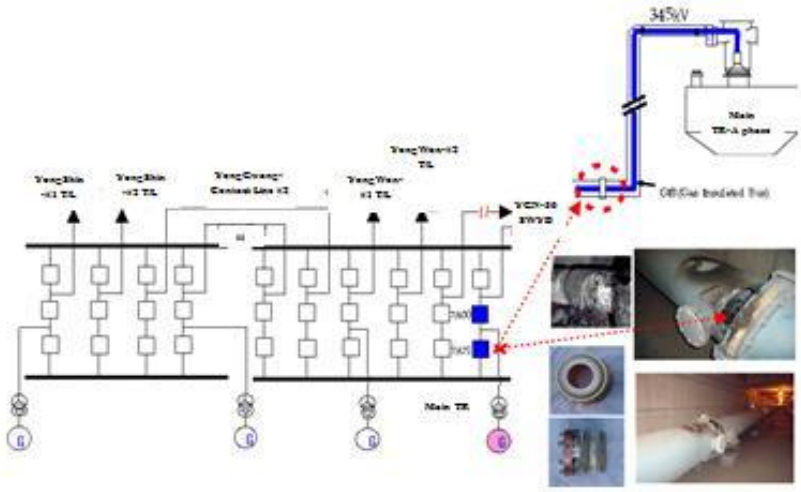
Shin-Wolsung #1	Shin-Kori #1
Abnormal and trouble signals occured at the same time	Trouble signal occured in 5 seconds after abnormal signal

KOREA INSTITUTE OF NUCLEAR SAFETY – 7 –


Recent Power Electronics Failures in Korean NPPs (I-3)
CEDMCS Trip Causes
There might be several conditions that result in an SCR failure due to an over-temperature condition :
Exceeding maximum repetitive peak or off-state voltage due to notches on the 3 phase MG buses with misadjustment of phase phase firing. Overheating would be caused by slower phase firing than normal turn-on of the SCR
Exceeding maximum critical rate of rise of the off-state voltage due to notches on the 3 phase buses with misadjustment of phase phase firing.
Excessive operating temperature within the CEDMCS cabinet. For example, overheating could occur if air flow in the cabinet was blocked.
Insufficient gate voltage input to the SCR can cause an over temperature condition and create a short in a SCR junction, thus causing the SCR failure.
KOREA INSTITUTE OF NUCLEAR SAFETY
- 8 -

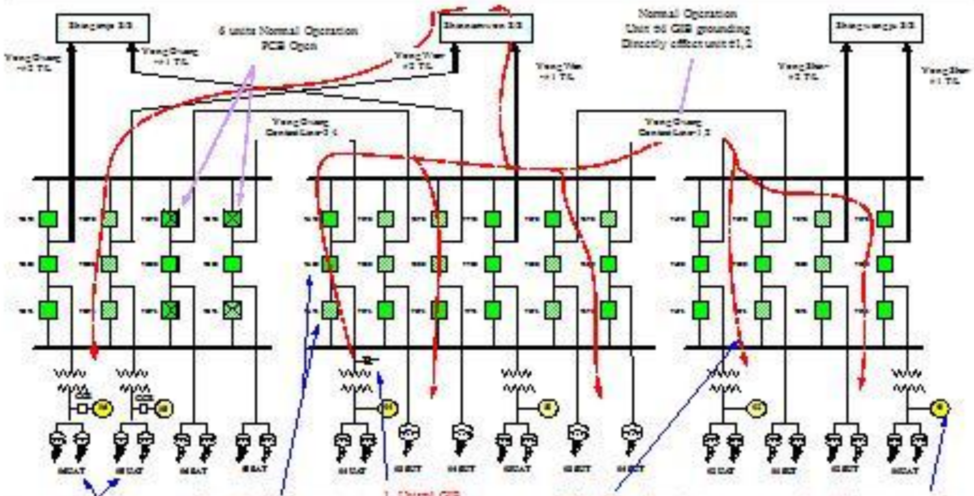

Recent Power Electronics Failures in Korean NPPs (I-4)
CEDMCS Corrective Action
The following corrective actions were implemented :
Replacement of broken Power Switch Assembly (PSA), and operational test inspection of total PSAs, and CEA verification test.
For long term corrective action, the old CEDMCS will be replaced by the redundant system of CEDMCS's power source.
Recovery blocking voltage of SCRs devices was increased from 800V to 1,200V
KOREA INSTITUTE OF NUCLEAR SAFETY
- 9 -

Recent Power Electronics Failures in Korean NPPs (II-1)



KOREA INSTITUTE OF NUCLEAR SAFETY — 10 —

Recent Power Electronics Failure in Korea NPPs (II-2)



KOREA INSTITUTE OF NUCLEAR SAFETY — 11 —

Recent Power Electronics Failures in Korean NPPs (II-3)

➢ **Reactor Trip Causes**

✓ Gas Insulation Bus(GIB) flashover occurred at the contact of inner conduct

✓ Grounding occurred at the phase-'A' Gas Insulated Bus (GIB) of Yonggwang Unit 4

✓ Switchyard voltage drop

✓ Three out of three phase differential relays were found to be actuated for YGN-1 causing the exciter and generator trip

✓ Reactor Trip

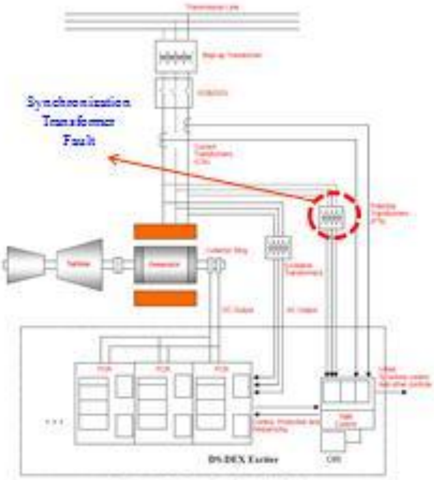


Figure 2.1 Typical Static Bus Fed Excitation

KOREA INSTITUTE OF NUCLEAR SAFETY

- 12 -

Recent Power Electronics Failures in Korean NPPs (II-4)

➢ **Corrective Action**

✓ The following corrective actions were implemented :

- Replacement of the failed GIB with a new one
- Plan to establish comprehensive and systematic study for the UPS integrity
- Review the exciter system protection functions in relation to one single fault event

- removing the synchronization transformer fault trip signal of exciter controller

- review thyristor capacity which is operable with only two phases exciter controller on a phase fault

KOREA INSTITUTE OF NUCLEAR SAFETY

- 13 -

Recent Power Electronics Failures in Korean NPPs (II-5)

- **Review removing the synchronization transformer fault trip signal of exciter controller**
  - ✓ The case was reviewed from every the point of view of the synchronization transformer fault signal for DS-DEX exciter controller.
  - ✓ The synchronization Tr fault trip consisted of zero cross signal fail, synchronization Tr fuse fail and synchronization Tr phase voltage unbalance.
  - ✓ The synchronization Tr fault trip can be substituted with Phase Unbalance Detection (PHUD) protection signal due to the same fault signal.
  - ✓ Consequently, phase voltage unbalance detector of synchronization transformer faults can be removed due to the protection of exciter system controller.

KOREA INSTITUTE OF NUCLEAR SAFETY – 14 –

Recent Power Electronics Failures in Korean NPPs (II-6)

- **Review the exciter system protection function in relation to one single fault event**
  - ✓ During normal operation, calculation of maximum load current of each thyristor
    - Rectifier quantity of exciter is N+1 which are supplied with the sufficient margin for normal condition.
    - maximum load current of each rectifier = 6,980/2 = 2,990[A]
    - maximum load current of each thyristor = 2,990/3 = 997[A]
  - ✓ On a phase fault, we verified that each thyristor was operable with only two phases exciter controller.
    - maximum load current of each thyristor = 2,990/2 = 1,495[A]
    - thyristor capacity current = 4,275[A] (5STP38Q4200)
    - as a result, thyristor capacity current margin is 2.9 times larger than the one of design

KOREA INSTITUTE OF NUCLEAR SAFETY – 15 –

Results and Discussion

- As a part of the preventive maintenance, we need to replace these components periodically after specified of years of operation.
- Actually the residual life of these devices is not known, however the life margin of power electronics devices could be determined sufficient time.
- Lately, the digital controller design to replace existing equipment should be considered with repect to the protective insulation coordination with other components.
- Through recent power electronics failures in Korean NPPs, we asked for the enhanced reliability for operating the power controller system.

KOREA INSTITUTE OF NUCLEAR SAFETY – 16 –

Thank you for your attention !

KOREA INSTITUTE OF NUCLEAR SAFETY – 17 –

How to Secure UPS Operation And Supply of Safety Critical Load During Abnormal Conditions in Upstream Supply

Gert Andersen
CTO, Switzerland

Silvan Kissling / Jörg Laaser
R&D Project Manager, Switzerland / Project Manager NPP, Switzerland

Abstract

UPS system design margins are usually given by manufacturer, but the events in Forsmark showed that these margins are not sufficient to protect UPS equipment and secure supply to critical loads. To withstand such events, it is not enough just to define margins for particular equipment. The overall plant design including environmental influences must be taken into consideration. For extreme environmental conditions, a UPS must include protection which design is matching to the upstream plant equipment. Immunity against abnormal conditions can not be finally guaranteed by higher margins. A limitation that excludes such influences must be implemented into the design. This presentation discusses possibilities to specify design margins, for rectifiers and inverters based on GUTOR thyristor and IGBT technology. It shows protection features to resist and solutions to limit overvoltages.

1. Introduction

In order to secure safe and reliable operation of Nuclear Power Plants (NPP), it is important to secure supply of all critical loads even if abnormal happened in upstream supply, therefore these loads are supplied by Uninterruptible Power Supply systems (UPS).

UPS system design margins are usually given by the UPS manufacturer, but the events in the Forsmark NPP showed that these margins are not always sufficient to protect UPS equipment and secure supply to critical loads. To withstand such abnormal events like lightning and transients, it is not enough just to define margins for particular equipments. The overall plant design including environmental influences must be taken into consideration.

This paper discusses possibilities to specify design margins, for rectifiers and inverters based on Schneider Electric UPS Gutor product line, using thyristor and IGBT technology. It also shows as well protection features to survive abnormal events by limiting internal possible overvoltage due to external events.

2. Critical loads

What are critical loads: Critical loads are equipments which if fail, will have an impact on safety; human as well as property.

In an NPP this will typically be equipments like monitoring and control equipments which are involved in safety related processes. In order to secure high reliability; redundant solution are installed. The level of redundancy may differ depending on criticality of the actual process. Triple redundant solutions are oft implemented in NPP's, such installations will also include three independent UPS systems including downstream distributions. Even if the MTBF for triple redundant installations are extremely high, based on possibility of internal failure and failure in supply within specified tolerances, it is still important to consider. What can happen if supply transients or other environmental issues, like e.g. lighting or beyond specified tolerances, would appear? Can such evidence have an impact on all systems, like a common cause failure?

3. Typical power supply concept

The following picture shows a typical rough electrical scheme for supply of critical loads as it is implemented in most nuclear power plants.

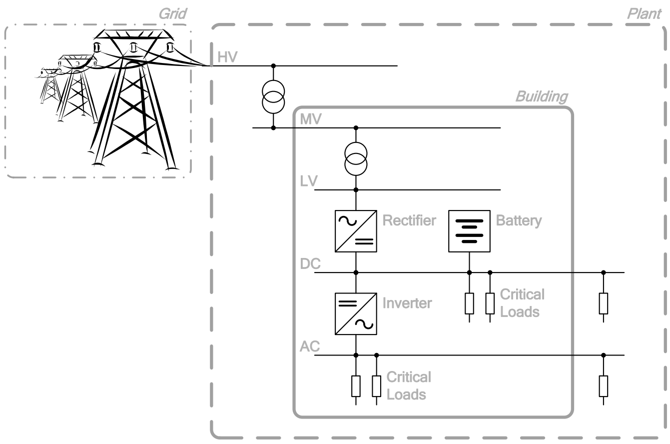


Figure 1: Typical power supply concept of a NPP[1]

The main components are:

- Grid: The plant is usually connected to the grid by means of overhead lines.
- HV: High voltage wiring and switchgear located inside the plant area.
- MV: Medium voltage wiring and switchgear located partially inside of a building.
- LV: Low voltage wiring and switchgear located inside of a building.
- Rectifier: The rectifier / battery charger is supplied from the LV line. It supplies critical DC-loads and charges the battery, which are both connected to the DC-bus.
- Battery: Energy source for autonomy supply of DC-bus and inverters
- DC: Battery buffered DC-bus supplying critical DC-loads.
- Inverter: The inverter is supplied from the battery buffered DC-bus. It supplies critical AC-loads which are connected to the AC-bus.
- AC: Low voltage AC wiring and switchgear supplying critical AC-loads.
- Critical loads: AC or DC powered critical loads which can partially be located outside the building.

4. Abnormal conditions in the upstream supply

Several abnormal conditions in the upstream supply, which can influence the critical DC- and AC-loads, are imaginable. The ones addressed by this paper are described and illustrated here after.

4.1 Lightning

Lightning has to be considered as one of the most extreme environmental influences to the plant's supply system. It is caused by atmospheric phenomena which are not controllable by humans. Therefore the only way to address the risk of a lightning and to reduce its impact on the supply system is to protect the plant and the critical equipment. There is no way to prevent the event from happening.

[1]. Source: GUTOR Electronic LLC

The possible voltage and current magnitude of a lightning stroke depends on lot of environmental and geographical factors and can hardly be defined. However, IEC 62305 defines theoretical lightning stroke levels and waveforms that need to be considered when designing a protection scheme.

The worst case pulse is defined with these parameters:

- Rise time T1 = 10 µs
- Time to half value T2 = 350 µs
- Peak current I = 200 kA

(According IEC 62305-1:2010, Table 3)

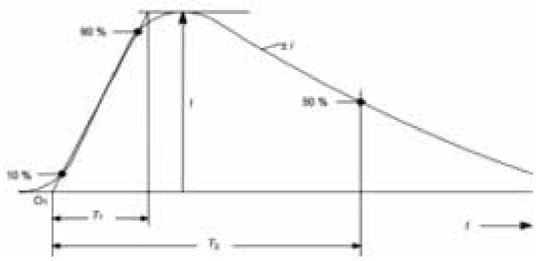


Figure 2: Lightning pulse according to IEC 62305-1[2]

In the NPP context, a lightning stroke most probably occurs in the HV and MV equipment located outside the plant buildings. But also all other electrical equipment located outside the buildings (incl. critical loads) can potentially be affected. Figure 3 shows some potential lightning strokes.

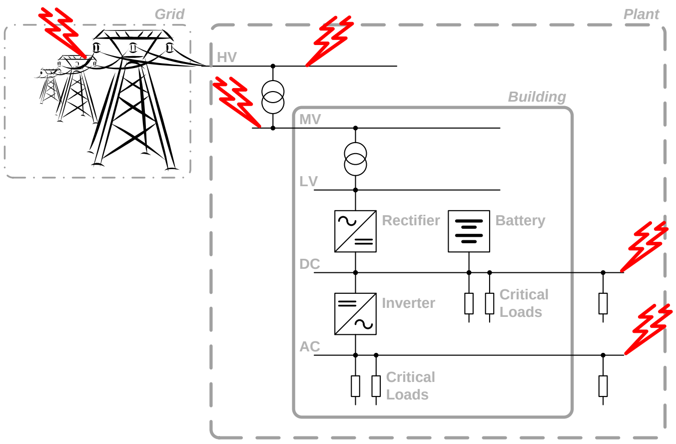


Figure 3: Potential lightning strokes affecting an NPP[3]

The effect of the stroke to the NPP will be different for all the stroke locations indicated on above picture and can hardly be described. Generally it can be stated that if no suitable protection is foreseen in the design of the plant, the effects of a lightning stroke can range from degradation of electrical equipment (no immediate effect but reduction of lifetime) up to catastrophic failure of critical control equipment.

It is therefore essential to consider lightning protection in the electrical design of a NPP. A selection of possible protection measures are:

- Overhead lines with grounded top lines
- Coverage of electrical equipment with building structures
- Surge arrestor devices located on HV, MV and LV supply lines and distributions
- Surge arrestor devices located directly inside sensitive electrical equipment
- System robustness to withstand higher surge pulses

None of these protection mechanisms can provide a complete protection by itself. Only a well designed combination of the above can effectively help to protect the critical electrical equipment. IEC 62305 provides guidance for such a protection design.

[2]. Source: IEC 62305-1: 2010, Figure A.1

[3]. Source: GUTOR Electronic LLC

Voltage transient

This topic occurred in Forsmark NPP in 2006. As mentioned in the IRS report 7788, a low frequency transient caused a disconnection of the offsite power to the safety related bus bars. There are various reasons that can cause a transient, e.g. static discharge, switching, lightning or power trip out. The UPS can be affected by a transient on the AC-input on the rectifier.

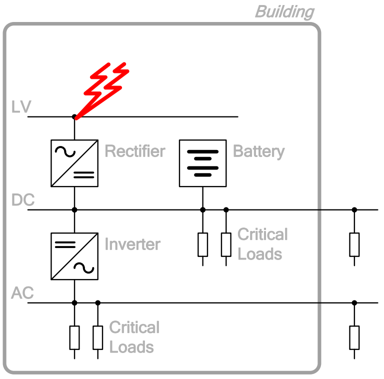


Figure 4: Potential transient affecting a UPS[4]

4.2.1 Definition of transient

"Define the transient!" This statement is the key in this topic. The definition of a transient is technical difficult and the possibility to do so differ from NPP to NPP. Important are the following data:

How fast increases the voltage?

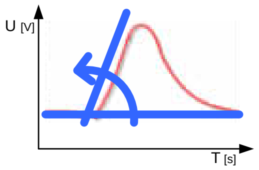


Figure 5: Transient increase speed[5]

How high is the voltage increase?

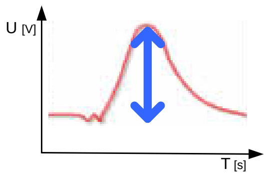


Figure 6: Transient voltage increase[6]

Duration of overvoltage?

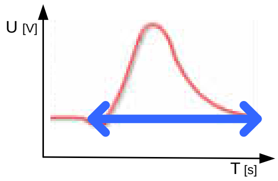


Figure 7: Transient duration[7]

Voltage increase only?

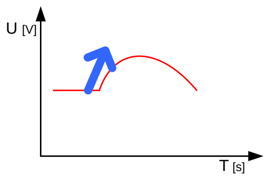


Figure 8: Positive transient[8]

[4]. Source: GUTOR Electronic LLC

[5]. Source: GUTOR Electronic LLC

[6]. Source: GUTOR Electronic LLC

[7]. Source: GUTOR Electronic LLC

[8]. Source: GUTOR Electronic LLC

Voltage decrease before voltage increase?

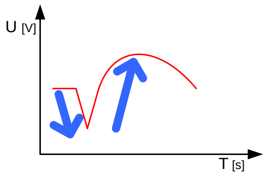


Figure 9: Dual transient[9]

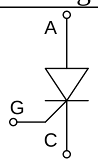
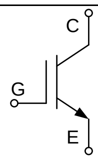
5. Critical UPS components

An important duty of the UPS supplying the critical DC and AC loads is to protect them from the effects of the possible upstream anomalies described in the former chapters (lightning and transient overvoltage). Therefore, the UPS has to be designed in a way that it can withstand such anomalies without affecting the load.

5.1 Technology

One of the key components in this context is the power semiconductors used in the rectifier section. Two main device type technologies are used in modern designs: Thyristors or IGBT's.

An analysis of the two technologies in the context of the two upstream anomalies described in the former chapters reveals their advantages and disadvantages:

	Thyristor	**IGBT**
Description	Thyristors are bipolar semiconductor devices for switching applications. They are mainly intended for AC 50/60 Hz applications. The device has three terminals: Anode, Cathode and Gate.	IGBT (insulated-gate bipolar transistor) are bipolar semiconductor devices for switching applications. They can be used for DC, AC 50/60 Hz as well as higher frequency switching applications. The device has three terminals: Collector Emitter and Gate.
Control	Thyristors can be activated through a trigger current introduced to the Gate. It then remains conducting as long as a positive current flows from Anode to Cathode. Switching OFF is only possible by commutation (current needs to pass zero-crossing) and not through the Gate signal.	IGBTs can be controlled through a voltage applied to the Gate terminal. It can be activated (Switch ON) by applying the control signal and can be deactivated (Switch OFF) by removing the control signal.
Symbol	 **Figure 10: Thyristor Symbol[10]**	 **Figure 11: IGBT symbol[11]**

[9]. Source: GUTOR Electronic LLC

[10]. Source: GUTOR Electronic LLC

Key features	50/60 Hz application Long operation experience Robust	High efficiency Fast switching Simple gate-drive Low-saturation-voltage
Advantage in case of lightning anomaly	Less sensitive to surge voltage transients	
Advantage in case of transient overvoltage		Can be switched OFF to limit the energy flow into the UPS system

Both devices have opposite advantages and disadvantages regarding the two analyzed phenomena. These anomalies can therefore not be addressed by simply switching to the other device type. Additional measures are required.

5.2 Design

According to IEC62040 a UPS must withstand several voltage variations like burst, surge, static discharge and voltage dips. With standard IEC61000-4-34 voltage dips are described more in detail. However, a transient as happened during the power trip out in NPP Forsmark (IRS report 7788) is not captured by this standard.

A UPS shall operate within the nominal voltage variations allowed by the upstream network, the rectifier shall supply power to DC-bus and keep the battery charged. Input voltage tolerances must be defined in consideration with upstream networks.

Since, in most cases it is not possible for NPP's to define a transient, it is necessary that a UPS manufacturer knows the functional limits of their UPS:

- What is the highest input voltage for permanent operation?
- At what permanent AC-input voltage the regulation of DC-output voltage will fail?
- What is the speed of AC-input voltage detection, in value: V/msec?
- What is the speed of DC-output voltage detection, in value: V/msec?
- What is the speed of DC-output voltage regulation, in value: V/msec?

With these data it is possible to define the transient, which the UPS can withstand without impacting the performance to secure the output of a UPS.

Practical tests of these figures are difficult for UPS manufacturer. The testing of various voltage variations in V/msec on full-scale models are often close to destructive levels. Those tests are very difficult to realize, are expensive and can often not be used as type tests.

By experience, NPP requirements for UPS systems are following two different philosophies:

[11] Source: GUTOR Electronic LLC

5.2.1.1 Wide-Range Input

The rectifier must supply the DC-bus and secure charging of the battery even under extreme input voltage variations.
Voltage decrease is non-critical as finally a back-up is given by the battery.
Voltage increase is critical, as protective function often fails on rectifier technology. The regulation speed of the rectifier must be fast enough to react to the voltage variation. E.g. the thyristor type technology has the main disadvantage that it is complex to switch off the thyristor before next zero-crossing. It requires additional components which may have an impact on overall reliability.
During the ON-time of the thyristor any AC-input voltage variation has a direct impact to the DC-output. This fact sets the reaction time of a protection function, it must be faster than 10ms.

AC-input voltage

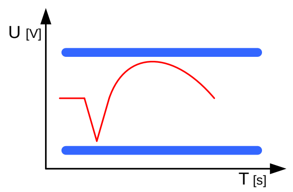


Figure 12: Wide-Range input[12]

DC-output voltage with fast-regulating Rectifier

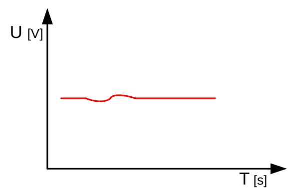


Figure 13: DC-output regulated[13]

DC-output voltage with slow-regulating Rectifier

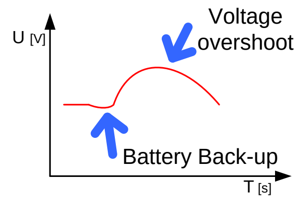


Figure 14: DC-output unregulated[14]

5.2.1.2 Narrow-Range Input

By definition, the rectifier will safely switch off during short AC-input voltage variations and the battery is supplying the DC-bus and inverter. The rectifier restarts when the AC-input voltage is back in tolerance.
The narrow-range input decreases the operational requirement. E.g., during the voltage transient of Forsmark NPP 2006, AC-input voltage was dropping first to 20% of nominal voltage before it increased to 120% of nominal voltage. If the voltage decrease is captured by the rectifier regulation, a narrow-range input has the advantage of a rectifier safe-shutdown. Subsequently, the DC-bus and inverter are supplied by battery until AC-input voltage is back in tolerance.

AC-input voltage

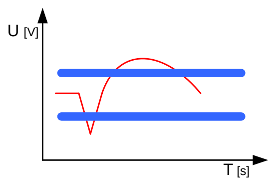


Figure 15: Narrow-Range input[15]

DC-output voltage rectifier

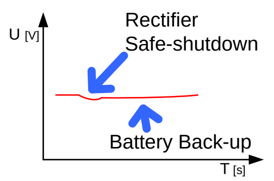


Figure 16: DC-output back-up[16]

[12]. Source: GUTOR Electronic LLC

[13]. Source: GUTOR Electronic LLC

[14]. Source: GUTOR Electronic LLC

[15]. Source: GUTOR Electronic LLC

[16]. Source: GUTOR Electronic LLC

5.2.1.3 DC Voltage protection

Apart of the AC-input voltage specifications, the DC-output voltage can be kept within tolerance by protective elements. This can be done by a Voltage Limiter. It is necessary to design the limitation function of the Voltage Limiter according to the required DC-voltage tolerance.

AC-input voltage

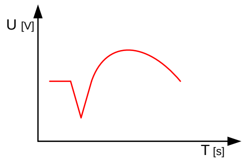


Figure 17: Dual transient[17]

DC-output voltage with Voltage Limiter

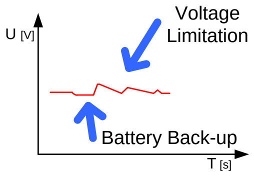


Figure 18: DC-output with VLU (Voltage Limitation Unit)[18]

6. Solution

6.1 Lightning

In order to properly protect the critical load, and the UPS itself, from the effects of lightning a thorough lightning protection concept based on IEC 62305 is required.

Such a concept includes an initial analysis of the plant:

- Analysis of the NPP as a whole
- Detection of potential stroke points
- Definition of protection zones
- Identification of all conductors crossing the zone borders

Based on the initial analysis, the required protection equipment can be defined on plant level. This includes:

- Overhead lines with grounded top lines
- Surge arrestor devices located on HV and MV supply
- Class 1 surge arrestor devices located in LV supply incoming
- Class 2 surge arrestor devices located in LV distribution
- Class 3 surge arrestor devices located in critical equipment
- Surge arrestor devices located on each conductor crossing a zone boarder.

Special care must be taken to reach a proper selectivity between the different surge arrestor devices installed throughout the plant. Otherwise the protection function in case of a lightning stroke is not guaranteed.

Based on the lightning protection concept and the selected surge arrestor devices, the specific requirements for the UPS can be defined.

[17]. Source: GUTOR Electronic LLC

[18]. Source: GUTOR Electronic LLC

6.1.1 Recommendation to NPP operators

Surge arrestor devices which are integrated into UPS systems by the UPS manufacturer can only be effective if they are selective to the other protection equipment of the plant. As this protection equipment is usually not in the design and delivery scope of the UPS manufacturer, he must rely on specifications provided by the customer.

Schneider Electric therefore recommends to the customers to

- Work out a thorough lightning protection concept covering the whole plant
- Select matching surge arrestor devices for the whole plant
- Define detailed requirements for the protection of the UPS systems
- Exactly define the type of surge arrestor to be installed in the UPS systems
- Provide detailed information about the protection equipment installed at the upstream side

6.2 Voltage transient

There will be always a voltage transient with:

- Higher voltage than designed
- Voltage increase faster than rectifier regulation

The power supply on the DC-bus must be secured. Even if the rectifier does fail fatally, due to an AC-input voltage far beyond specified tolerances including transients, the inverter must still continue to supply the critical load as long as energy is available from battery and or external DC-bus.

To cover the lack of simulation tests a protection function must be implemented into the Rectifier. The protection must secure that the DC-voltage never exceeds the defined level.

One solution can be to increase the speed of the rectifier regulation. But with thyristors type technology, this speed increase is limited.

Another solution is to implement protective elements into the rectifier. This protection must secure that the DC-voltage never exceeds a defined level. This protection can be realized with a voltage limiter, which is also known as Voltage Limitation Unit (VLU).

6.2.1 GUTOR Voltage Limitation Unit

A fast transient on the AC-input cannot be protected by the rectifier, since the thyristors can not be switched off until the next zero-crossing. During this time, the transient can directly affect the DC-voltage and could lead to a shutdown of the inverter.

The VLU guarantees that the DC-output voltage stays in an allowable range. Furthermore, in case of a permanently high DC-voltage, the VLU includes an additional protection function. The rectifier thyristors will be permanently blocked and the rectifier will be switched off.

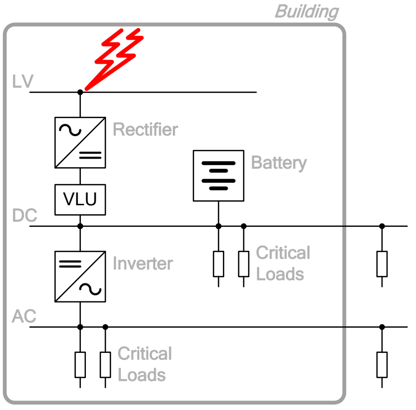


Figure 19: VLU[19]

[19]. Source: GUTOR Electronic LLC

7. Conclusion

Overall reliability cannot be secured, just by focusing on individual systems in a complex power supply and control systems as used in NPP’s. It is important to take the big picture and in this way to secure that each sub-system is coordinated with each other. Only in this way; the highest level of overall reliability can be secured. In this way even abnormal events beyond standardized levels, which are specified by applicable standards, will not necessary lead to a loss of the critical load.

The level of redundancy will depend on the architecture of critical loads. Therefore, the best solution will be to have total independency between the redundant systems from the HV line down to, and also including, the critical loads.

How to Secure UPS Operation And Supply of Safety Critical Load During Abnormal Conditions in Upstream Supply

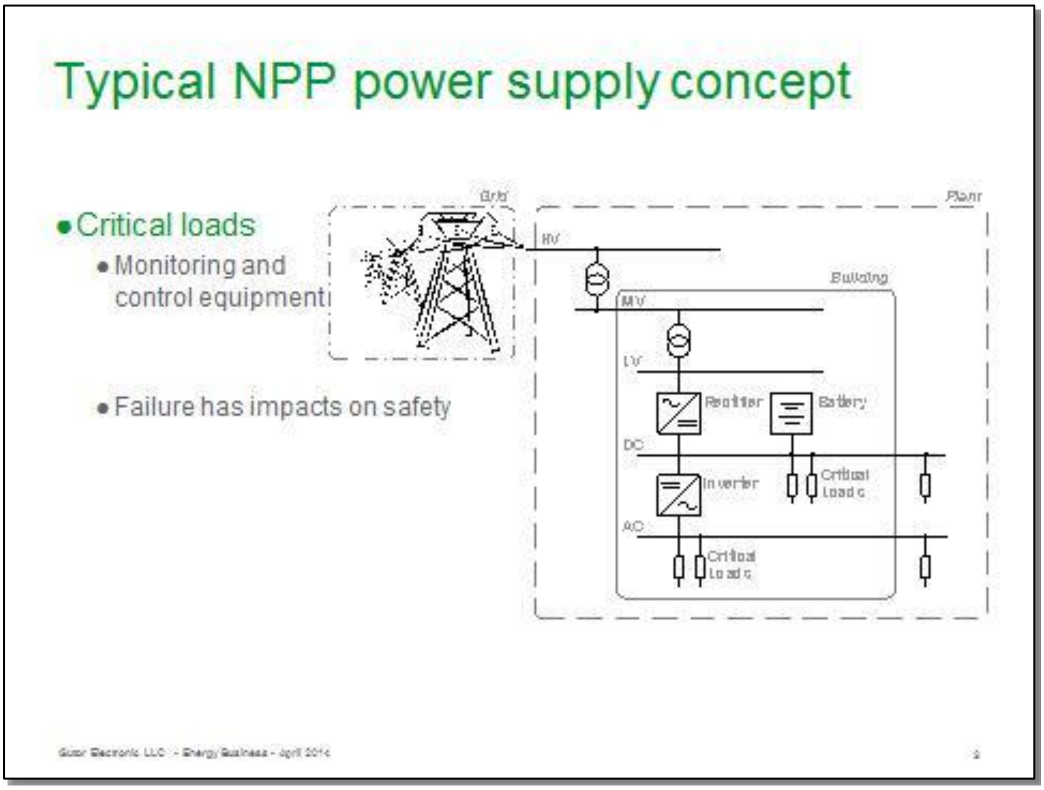
Gutor technology

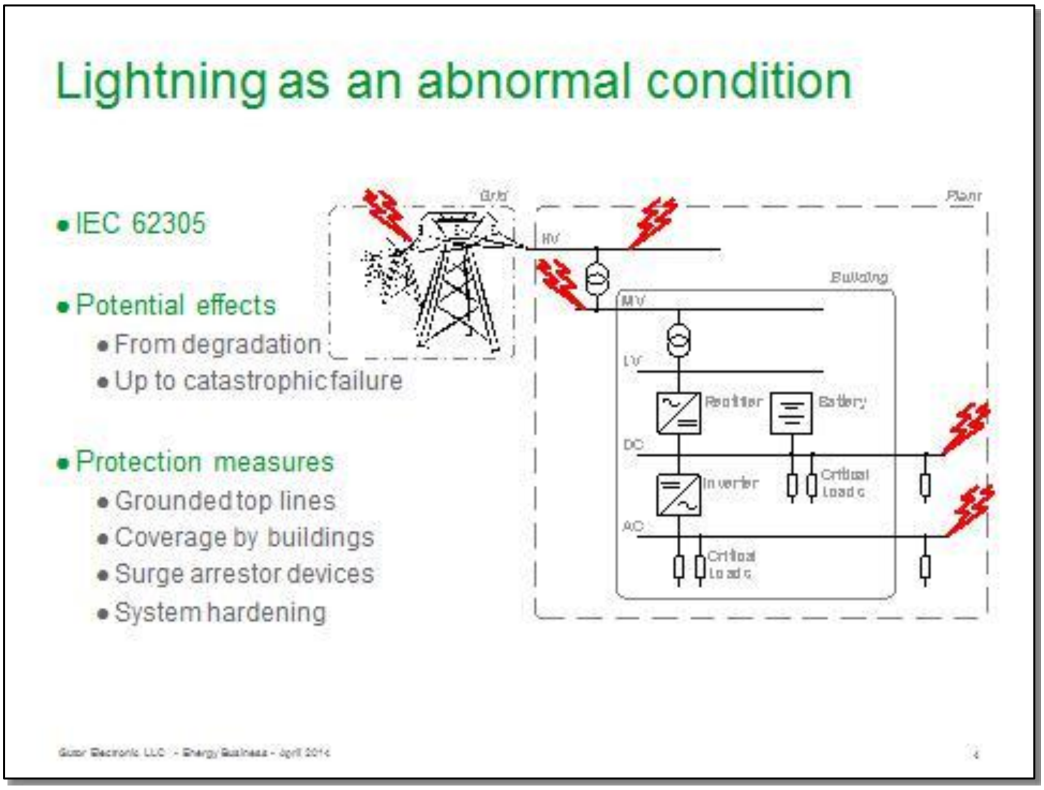
Schneider Electric

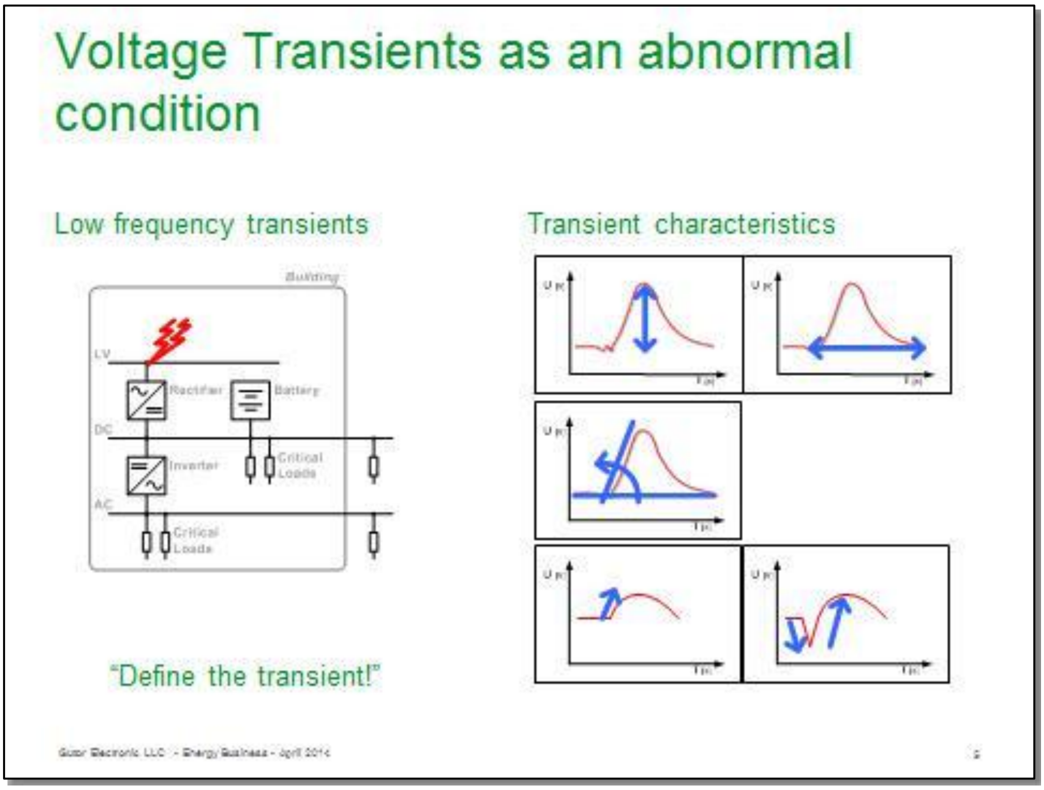
Introduction

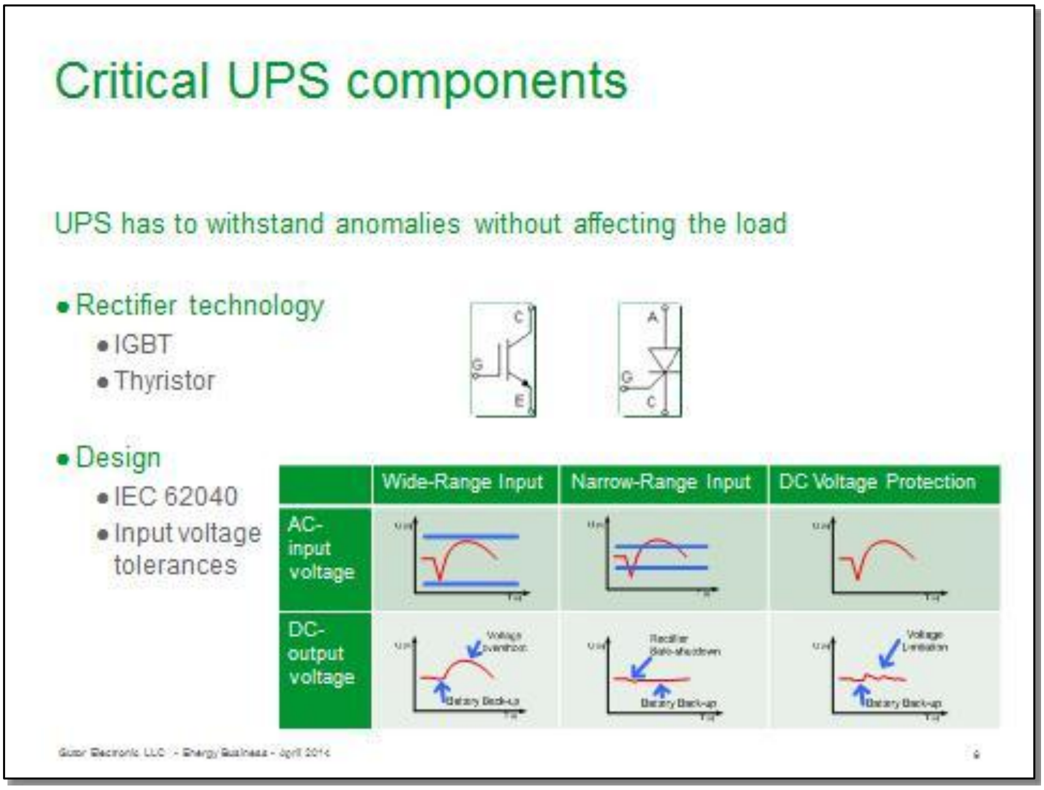
- Secure supply of critical loads is essential for safe and reliable operation of Nuclear Power Plants (NPP)
- Uninterruptible Power Supply Systems (UPS) are used
- UPS system design margins given by manufacturer
- This paper discusses
  - Design margins for rectifiers and inverters using thyristor and IGBT technology
  - Protection features to survey abnormal evens by limiting internal overvoltage due to external events

Gutor Electronic LLC - Energy Business - April 2014


Typical NPP power supply concept
• Critical loads
• Monitoring and control equipment
• Failure has impacts on safety
Grid
Plant
HV
Building
MV
LV
Rectifier
Battery
DC
Inverter
Critical loads
AC
Critical loads


Lightning as an abnormal condition
• IEC 62305
• Potential effects
• From degradation
• Up to catastrophic failure
• Protection measures
• Grounded top lines
• Coverage by buildings
• Surge arrestor devices
• System hardening
Grid
Plant
HV
Building
MV
LV
Rectifier
Battery
DC
Inverter
Critical loads
AC
Critical loads


Voltage Transients as an abnormal condition
Low frequency transients
Building
LV
Rectifier
Battery
DC
Inverter
Critical Loads
AC
Critical Loads
"Define the transient!"
Transient characteristics
Gutor Electronic LLC - Energy Business - April 2014

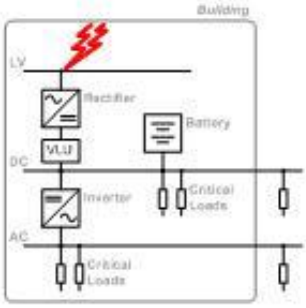

Critical UPS components
UPS has to withstand anomalies without affecting the load
• Rectifier technology
• IGBT
• Thyristor
C
G
E
A
G
C
• Design
• IEC 62040
• Input voltage tolerances
Wide-Range Input
Narrow-Range Input
DC Voltage Protection
AC-input voltage
DC-output voltage
Voltage overshoot
Battery Back-up
Rectifier Safe-shutdown
Battery Back-up
Voltage Limitation
Battery Back-up
Gutor Electronic LLC - Energy Business - April 2014

Solution for lightning event

- General recommendation
  - Create lightning protection concept (IEC 62305)
  - Define selective protection equipment on plant level
- Protection devices integrated in UPS
  - To guarantee selectivity, customer has to…
    - Define detailed requirements
    - Define exact type of surge arrestor
    - Provide detailed information about the installed protection equipment

Solution for voltage transient event

- DC-bus must be secured
- Protection function required in rectifier
  - Increase regulation speed (limited with thyristor technology)
  - Implement protective elements
- Gutor Voltage Limitation Unit (VLU)
  - Limits DC-output voltage
  - Protects rectifier
  - Analog solution, no firmware



Conclusion

- Abnormal events beyond standardized levels shall not lead to a loss of critical load
- Secure highest level of overall reliability
  - Not just by focusing on individual systems
  - Important to take the big picture
  - Coordination between sub-systems
  - Total independency between redundant systems (from the HV line down to the critical loads)

Source of all pictures in presentation: GUTOR Electronic LLC

Modifications to Battery chargers & inverters Units

Florent Raison
AEG Power Solutions, Germany

Seismic constraints: a new era

Over-exceeding the seismic specifications of the nuclear industry has always been the top priority of AEG Power Solutions. Since the Forsmark event, and especially since the Fukushima Daïchi accident, utilities have reviewed their specifications.

As a consequence, safety related battery chargers and inverters have to withstand higher acceleration levels.

Simulation, design and test procedures are key drivers of the battery charger and inverter industry.

1. Simulation

Forces analysis through simulation is the first step of the product design process. The CAD drawings of our equipment, including the mechanical frame of the cabinet and the internal components, are used for the simulation of vibration.

In the frame of 10 Hz, most new specifications show higher values, with higher constraints on our equipment. Our nuclear product range has been adapted to these new requirements.

2. Design & Test

PCBs (Printed Circuit Boards), as key components in charge of the regulation and monitoring of the load, are first separately tested during the design phase, as a specific component. They are subjected to the following tests:

- Critical load analysis
- Thermal imaging
- Climatic test
- Vibration & shock test

Then the complete equipment will follow a complete test program, including:

- Type test
- EMC test
- Seismic test
- Aging test

Technology: a true driver for robustness and reliability

Technology is key in achieving goals in terms of robustness and reliability of battery chargers and inverters. AEG Power Solutions renewed its entire range of products in 2011-2013 and made relevant choices.

1. Software free – 100% analogue technology

By updating its complete range of nuclear products, AEG Power Solutions is now offering a new range of solutions to the nuclear industry which minimize the risk of component obsolescence, in case of product replacement on existing nuclear power plants, or of new construction.

BEFORE

NOW

In order to increase the product reliability and to facilitate the qualification programs of the products, the decision was made to offer 100% analogue technology (Software free)

1. Split of regulation & monitoring functions

The different regulation & monitoring functions are separately split per PCB. This provides a few technical advantages related to robustness and reliability:

- Lower sensitivity to vibration
- Low EMC disturbance
- Low MTTR (Mean Time To Repair)

On the top of this technical choice, AEG is offering:

1. a 1+1 redundancy for two key functions:

- Power supply of the PCB
- DC overvoltage protection (Forsmark)

2. An intelligent power supply:
   Thanks to an automatic switch off of the non-operating functions, in case of a transfer from the grid to the batteries, AEG Power Solutions equipment will limit the internal power consumption of the PCBs, for the benefit of the overall battery autonomy.

3. An independent auxiliary supply between regulation and control

4. One single regulation & monitoring solutions for all types of products (rating, voltage), involving a simplified spare parts management, and facilitating qualification operations.

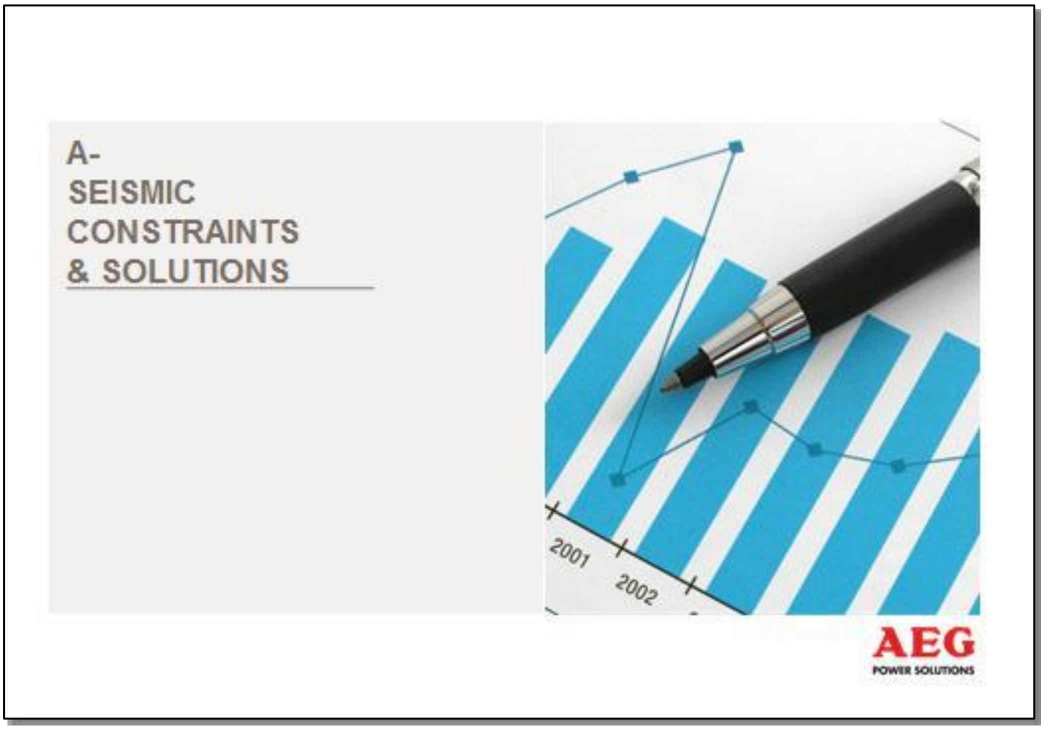
Diagnostic tools: A real mean to improve equipment reliability

The general concept of the diagnostic tools is to perform regular maintenance in an easier and more efficient way, preventing any modification of the already qualified equipment on site.

AEG Power Solutions diagnostic tools and equipment (battery chargers or inverters) are connected through two single connectors only.

Safe and efficient, the AEG Power Solutions diagnostic tools are calibrated internally (AEG qualified for calibration), so that AEG is performing a permanent control of the whole product chain.


MODIFICATIONS TO BATTERY CHARGER & INVERTER UNITS
CSNI – INTERNATIONAL WORKSHOP
Florent RAISON – Business Development Director
AEG
POWER SOLUTIONS


A-
SEISMIC
CONSTRAINTS
& SOLUTIONS
2001
2002
AEG
POWER SOLUTIONS

WHAT WE NEED TO AVOID IN CASE OF AN EARTHQUAKE ?

Insufficient connections ?

Halfen rail too weak ?

→ Stability calculation is key !

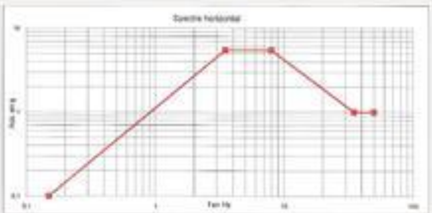
Please note that these are not AEG cabinets !!!

AEG POWER SOLUTIONS

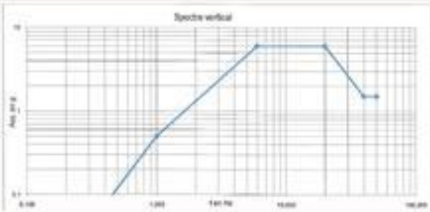
SEISMIC SPECTRUM

ONE EXAMPLE OF RECENT NEW SEISMIC REQUIREMENTS:

5,5 G - 10 HZ



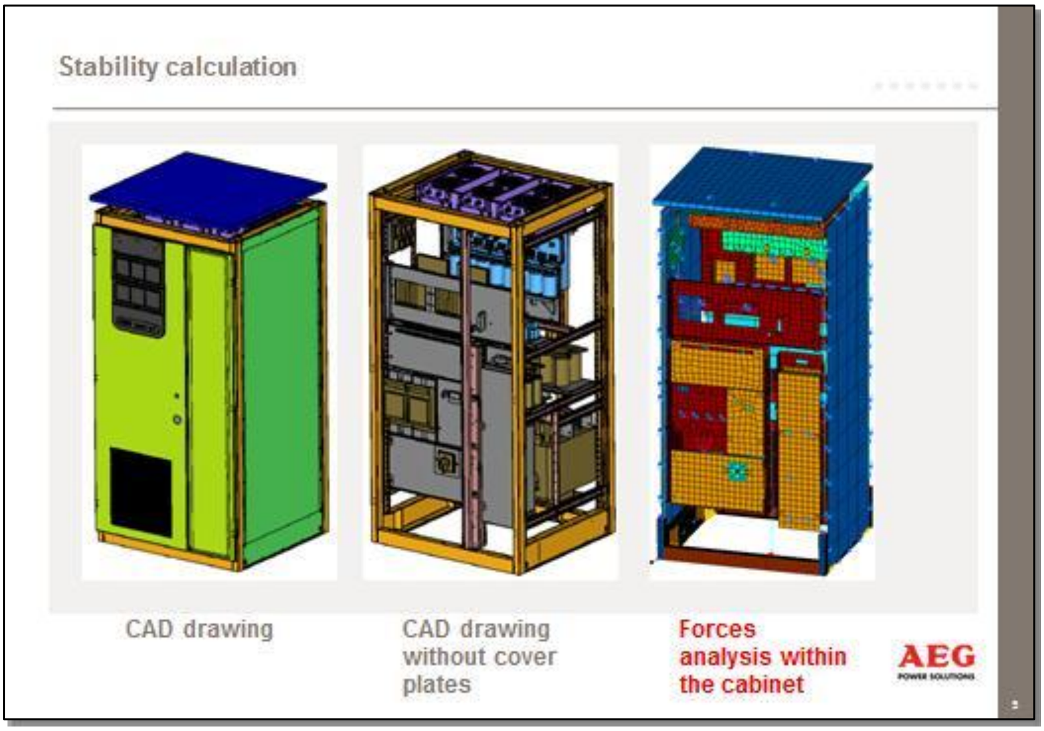
6 G - 10 HZ

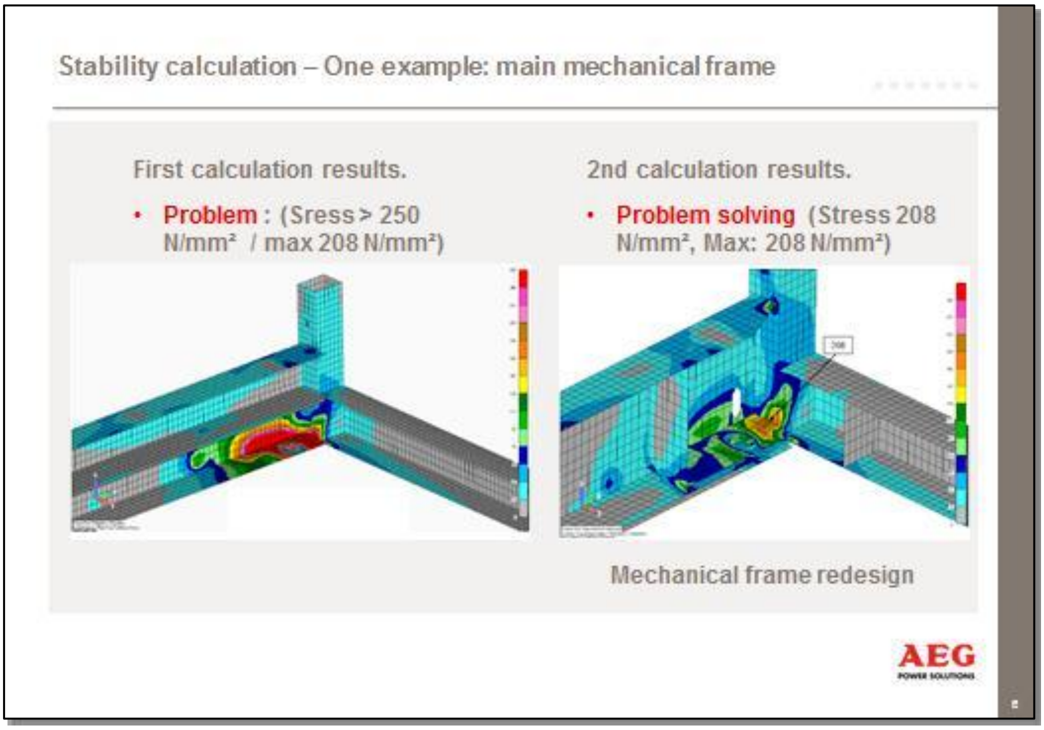


FORSMARK & FUKUSHIMA: 2 EVENTS – 2 TRENDS

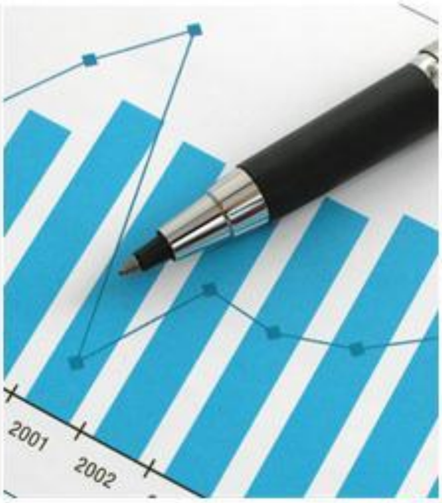
- Less qualification per calculation or analogy, more qualification per test (shaker table)
- Increase of seismic level specification (up to 6G)

AEG POWER SOLUTIONS


Stability calculation
CAD drawing
CAD drawing without cover plates
Forces analysis within the cabinet
AEG
POWER SOLUTIONS


Stability calculation – One example: main mechanical frame
First calculation results.
• Problem : (Sress > 250 N/mm² / max 208 N/mm²)
2nd calculation results.
• Problem solving (Stress 208 N/mm², Max: 208 N/mm²)
Mechanical frame redesign
AEG
POWER SOLUTIONS

B- EMERGENCY GENSET CONNECTION



AEG
POWER SOLUTIONS

NEW TREND: ``ULTIMATE ``SOCKET

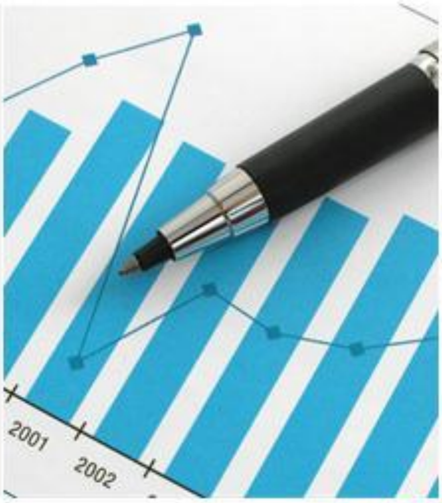
More utility specifications refer to the implementation of an ultimate socket :

- Connection to an external diesel generator
- Used in extreme situation

→ possibility to manually connect an `` ultimate `` source of energy

AEG
POWER SOLUTIONS

C- DESIGN & TEST / STRESSED AMBIANT CONDITIONS



AEG POWER SOLUTIONS

PCB QUALIFICATION

- **PCB design analysis**
  - Thermal Imaging
  - Critical Load Analysis
- **Climatic Test**
  - Cold Test
  - Heat Test
  - Cyclic Heat Test (in operation)
    - Profil 25C° ± 3K / 60C° ± 3K (1000h.)
    - Input mains: Umin: 323Vac / Umax.. 418Vac

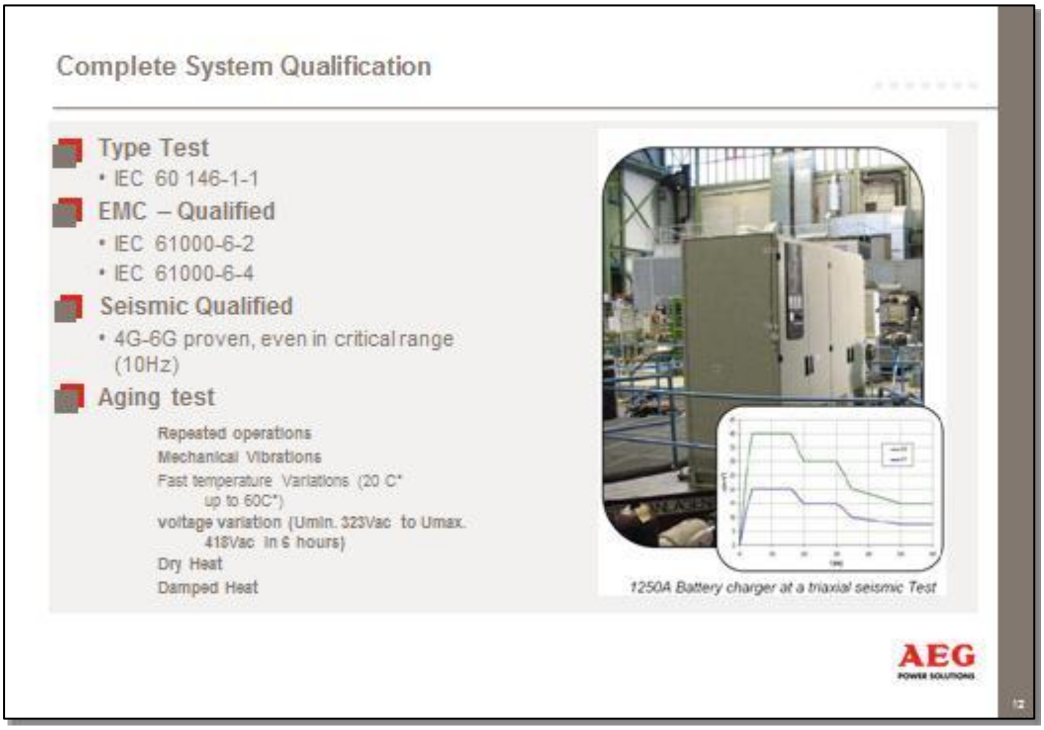
Critical Load Analysis

Test chamber of a cyclic temperature Test for PCB´s

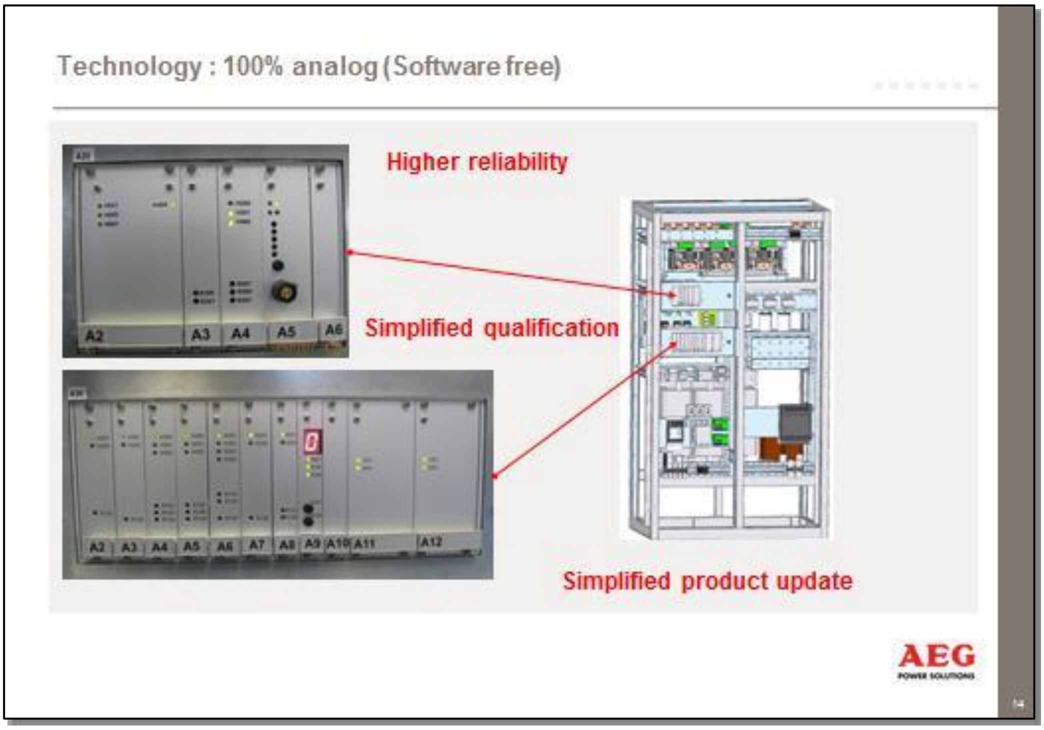
AEG POWER SOLUTIONS

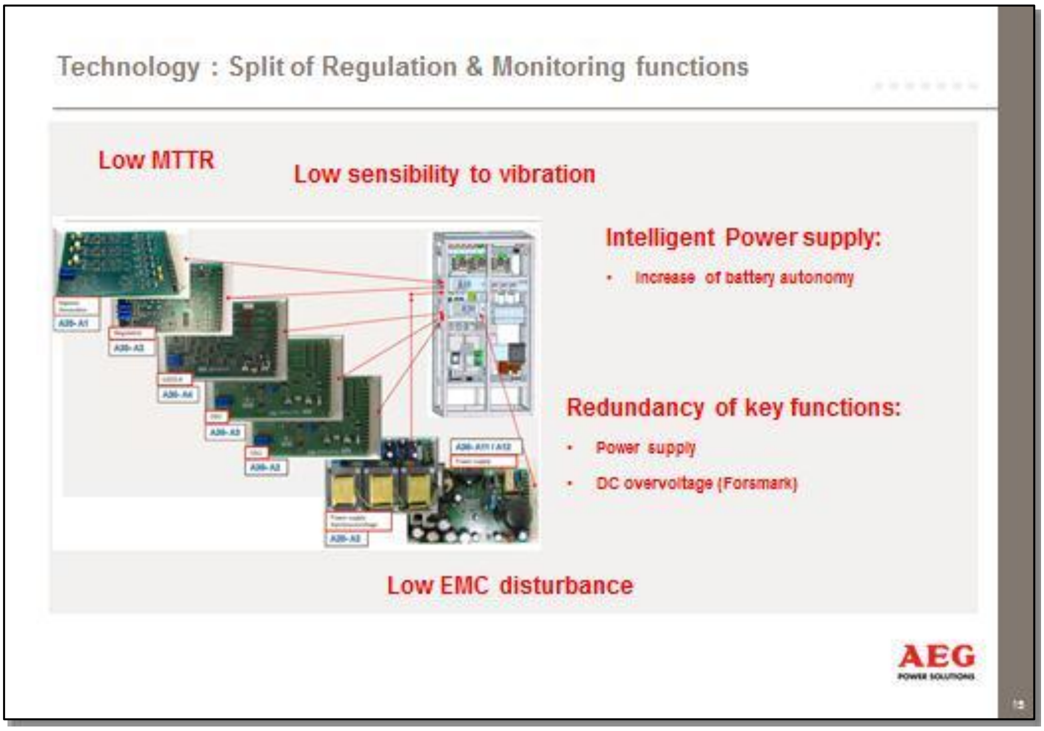
10


PCB QUALIFICATION
Vibration Test
(Laboratory Phönix TESTLAB)
→ Up to 60ms/s² Test in Operation
Shock test
(Laboratory Phönix TESTLAB)
→ Up to 300m/s²
PCB´s in shock Test
AEG
POWER SOLUTIONS


Complete System Qualification
Type Test
• IEC 60 146-1-1
EMC – Qualified
• IEC 61000-6-2
• IEC 61000-6-4
Seismic Qualified
• 4G-6G proven, even in critical range (10Hz)
Aging test
Repeated operations
Mechanical Vibrations
Fast temperature Variations (20 C° up to 60C°)
voltage variation (Umin. 323Vac to Umax. 418Vac in 6 hours)
Dry Heat
Damped Heat
1250A Battery charger at a triaxial seismic Test
AEG
POWER SOLUTIONS

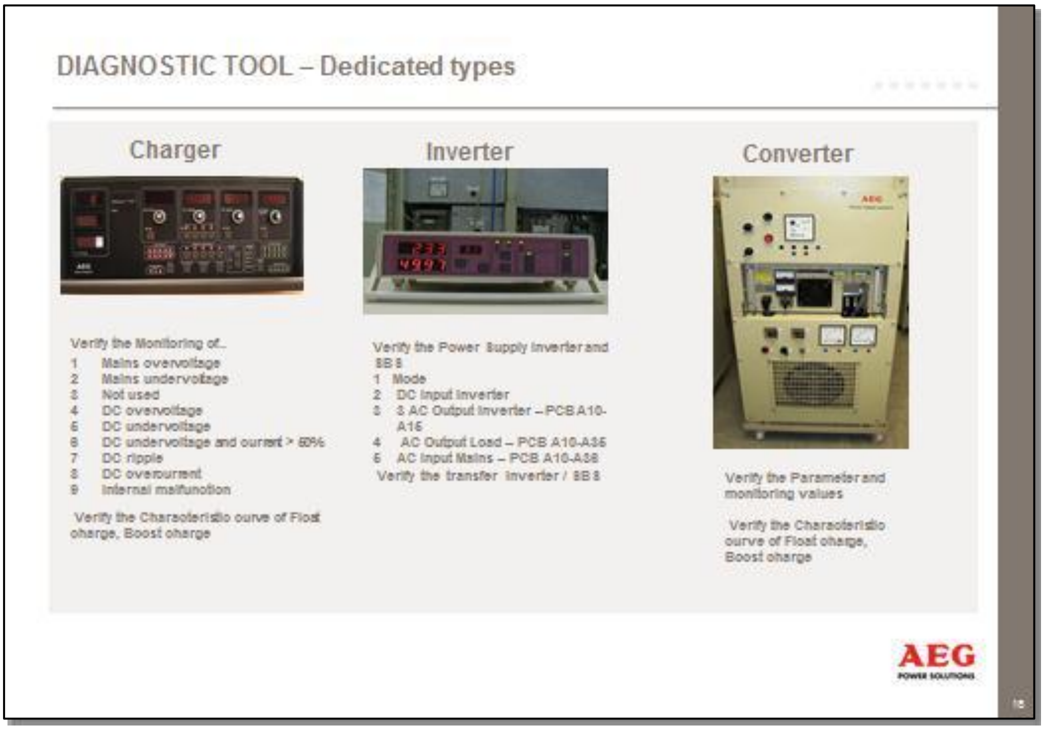

D-
SOFTWARE FREE
SOLUTIONS
2001
2002
AEG
POWER SOLUTIONS

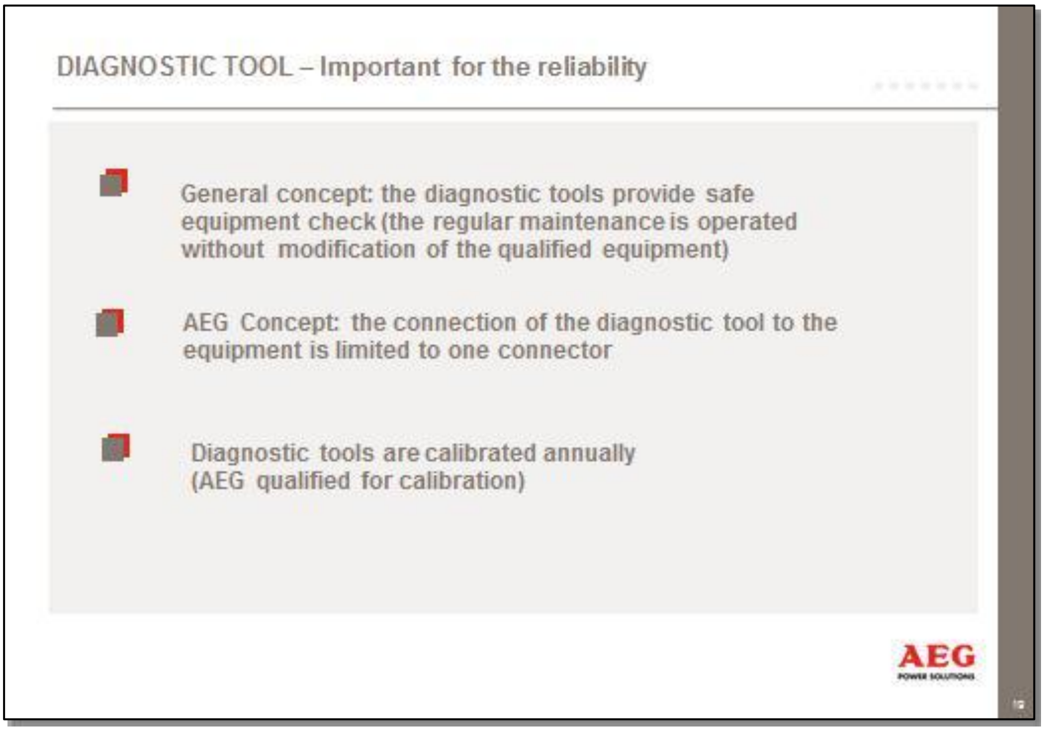

Technology : 100% analog (Software free)
Higher reliability
Simplified qualification
Simplified product update
A2
A3
A4
A5
A6
A7
A8
A9
A10
A11
A12
AEG
POWER SOLUTIONS


Technology : Split of Regulation & Monitoring functions
Low MTTR
Low sensibility to vibration
Intelligent Power supply:
• Increase of battery autonomy
Redundancy of key functions:
• Power supply
• DC overvoltage (Forsmark)
Low EMC disturbance
AEG


Components update
BEFORE
NOW
Reduced mass of components
(reduction of seismic stress)
AEG


E-
EFFICIENT
MAINTENANCE
TOOL
2001
2002
AEG
POWER SOLUTIONS


DIAGNOSTIC TOOL – Dedicated types
Charger
Inverter
Converter
Verify the Monitoring of..
1 Mains overvoltage
2 Mains undervoltage
3 Not used
4 DC overvoltage
5 DC undervoltage
6 DC undervoltage and current > 60%
7 DC ripple
8 DC overcurrent
9 Internal malfunction
Verify the Characteristic curve of Float charge, Boost charge
Verify the Power Supply Inverter and SBS
1 Mode
2 DC Input Inverter
3 3 AC Output Inverter – PCB A10-A15
4 AC Output Load – PCB A10-A35
5 AC Input Mains – PCB A10-A38
Verify the transfer Inverter / SBS
Verify the Parameter and monitoring values
Verify the Characteristic curve of Float charge, Boost charge
AEG
POWER SOLUTIONS


DIAGNOSTIC TOOL – Important for the reliability
General concept: the diagnostic tools provide safe equipment check (the regular maintenance is operated without modification of the qualified equipment)
AEG Concept: the connection of the diagnostic tool to the equipment is limited to one connector
Diagnostic tools are calibrated annually (AEG qualified for calibration)
AEG


Thank you for your attention
AEG
Power Solutions
AEG

SESSION SEVEN

"Digital components in power systems"

Digital Components in Swedish NPP Power Systems

Mattias Karlsson
Swedish Radiation Safety Authority, Sweden

Tage Eriksson
Swedish Radiation Safety Authority, Sweden

Abstract

Swedish nuclear power plants have over the last 20 years of operation modernised or exchanged several systems and components of the electrical power system. Within these works, new components based on digital technology have been employed in order to realize functionality that was previously achieved by using electro-mechanical or analogue technology. Components and systems such as relay protection, rectifiers, inverters, variable speed drives and diesel-generator sets are today equipped with digital components. Several of the systems and components fulfil functions with a safety-role in the NPP. Recently, however, a number of incidents have occurred which highlight deficiencies in the design or HMI of the equipment, which warrants questions whether there are generic problems with some applications of digital components that needs to be addressed.

The use of digital components has presented cost effective solutions, or even the only available solution on the market enabling a modernisation. The vast majority of systems using digital components have been operating without problems and often contribute to improved safety but the challenge of non-detectable, or non-identifiable, failure modes remain.

In this paper, the extent to which digital components are used in Swedish NPP power systems will be presented including a description of typical applications. Based on data from maintenance records and fault reports, as well as interviews with designers and maintenance personnel, the main areas where problems have been encountered and where possible risks have been identified will be described. The paper intends to investigate any "tell-tales" that could give signals of unwanted behaviour. Furthermore, particular benefits experienced by using digital components will be highlighted. The paper will also discuss the safety relevance of these findings and suggest measures to improve safety in the application of digital components in power systems.

1. Introduction and summary

The current Swedish commercial nuclear fleet consists of ten nuclear power reactors at three sites, and two reactors at one site has been closed following a political decision. These were built in the period 1972 to 1985 and in their original design contained electrical and I&C components of limited complexity with analogue components for earlier designs and solid state components in later designs. Recent events in NPPs have raised concerns regarding the adequacy of the design of the electrical systems. In light of technological evolution, there is a concern that the introduction of digital components may be a contributing factor to the increasing fault frequency. The Swedish Radiation Safety Authority has in discussions with the safety departments of the Licensees established an overview of the relative penetration of digital I&C to ascertain where deficiencies or strengths have been identified. In order to define the context, the focus has been on the introduction of autonomous programmable electronic devices (PECs)[1] in safety classified electrical systems.

The conclusion is that the introduction of the PECs themselves has not been identified as a major reason for recent events and that components have responded to events as designed. However, the basis for design and the functional behaviour of systems, structures and components (SSCs) has been inadequately defined and understood and there have been shortcomings in the validation of functional behaviour.

An increased focus should be on establishing a well defined design basis in order to ascertain the behavior of the electrical system so that robustness and protection requirements can be defined to minimise any uncertainty in component behavior. In order to minimise the design basis required, a simplicity of system design is desirable, and introduction of PECs therefore requires a more detailed assessment of the design basis.

2. Background and current situation

There has been a gradual introduction of PECs in the Swedish plants. This is most prevalent in the older plants that have undergone modernisation programs to adapt to new safety requirements, in particular to cope with the increased requirements on separation and diversity of systems as compared to original design.

Oskarshamn 1 and 2 were originally designed with two emergency diesel generator (EDG) backed electrical divisions. Oskarshamn 1 has been modernised to a four train system and Oskarshamn 2 is currently undergoing a similar modernisation. Ringhals 1 was a four train electrical system in original design but had a limited physical separation, in particular regarding cable routing. This was resolved under a modernisation program initiated in the late 1990s and two additional electrical divisions[2] were introduced, giving the plant effectively a four plus two train system electrically.

Forsmark 1 and 2 have an original four train electrical system with a two plus two separation / segregation concept and measures have been taken to enhance the separation by increasing the physical separation, by providing separate fire compartments, rather than relying on distance separation. Some equipment replacement have been carried out due to ageing or equipment failures, however no large scale replacements have been carried out.

Oskarshamn 3 and Forsmark 3 are the newest plants, built in the mid 80s, with four train electrical systems having a strong physical separation in the original design and no major modernisations have been necessary in the safety systems. Oskarshamn 3 have implemented a power uprate, which is currently being planned for Forsmark 3 as well.

Ringhals 2-4 are Westinghouse built PWR units, contrary to the other plants being Asea built BWRs, and have an original four train electrical configuration. Ringhals 2 have modernised the Reactor Protection System.

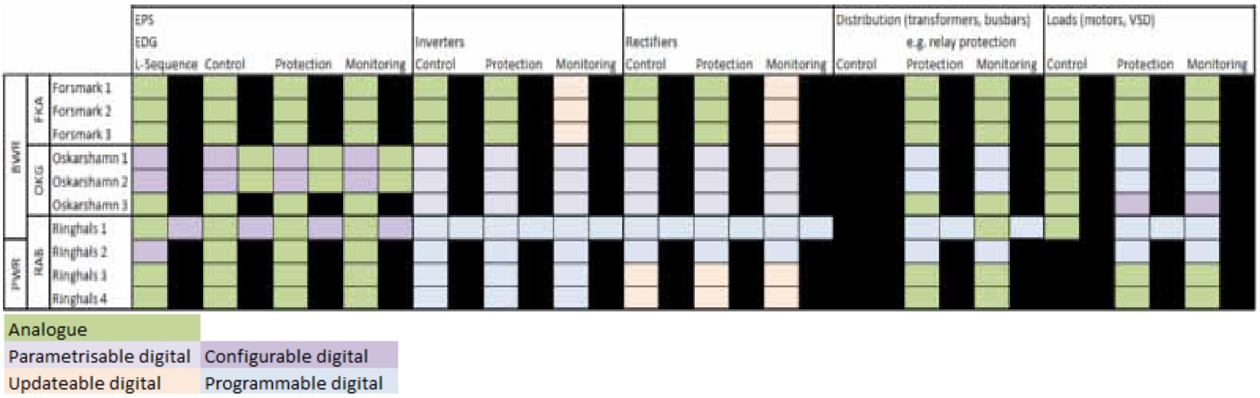
During modernisations, digital based components have been used subjected to appropriate qualification governed by technical guidelines, and to a lesser extent during component replacements when

[1]. In this paper, digital components generally mean programmable electronic components, or embedded devices, more specifically microprocessor based devices with an instruction set an application code. Fixed logic components, for example based to transistors or even relays, although being digital and sometimes complex, are excluded.

[2]. Referred to as a diversified plant section (DPS). This is not to be confused with the concept of diversified protection system, which in fact is also implemented, but out of scope for this paper.

no suitable component type of original design (generally analogue) has been found. Figure 1 provides a rough estimate of the relative penetration of digital I&C components in safety classified electrical systems. It is apparent, and expected, that plants that have undergone modernisations have to a larger extent introduced digital I&C. Modernisation projects, having larger resources available, have an enhanced capability to undergo the extensive qualifications required introducing new components and it is recognised that the increased unavailability of original components over time leads to difficulties of the long term management of the plant. Plants that have not yet undergone major modifications are anticipating a similar development, but have meanwhile established agreements with vendors to sustain the existing design for the near time future.

Being at the midst of a technological changeover, is there then a need for a strengthened guidance in the approach to modernisations based on digital I&C in particular? This question will be further elaborated in subsequent chapters.



Analogue. Non-microprocessor based technology.
Parametrisable. Fixed program code with possibility to change specific parameters; changing the threshold values or constants in a calculation algorithm.
Configurable. Fixed program code with possibility to change the functionality of the device to change the functional behaviour of the device; possibility to change the application code executed.
Updateable. Re-programmable, generally by vendor updates.
Programmable. Re-programmable by end user.
Where two columns are used, it indicates a degree of diversification is implemented.

Figure 1. Apparent[3] penetration of PECs in electrical systems.

2.1 Diversification[4]

Diversification has not been addressed specifically for PECs[5] in either of the Swedish plants, i.e. no general strategy has been adopted to use diverse equipment between trains, nor between levels of defence

---

[3]. This high-level overview represents a summary done by the Swedish Radiation Authority based on information by the Licensees. It should not be interpreted as a definite statement but serves to illustrate the general view of the penetration of digital I&C rather than a systematic and definite review.

[4]. This paper only refers to electrical diversification and does not consider functional diversification.

[5]. The paper does not address the I&C platforms used for other than the electrical system, such as the reactor protection system.

in depth. Diversification has however been implemented as a viable design solution, notably in Ringhals 1 with two independent diversified electrical trains in addition to the original four electrical trains and in Oskarshamn 1 and 2 the emergency diesel generators are diversified on a two plus two basis.

3. Experiences and relation to digital I&C

A general view of digital I&C is to avoid it, or limit the functionality in order to decrease complexity, in order to avoid the arduous qualification requirements associated with this equipment. While this is a reasonable position, at the same time it indicates that the current awareness and standards governing the processes are well defined. Particular drawbacks regarding digital I&C generally mentioned are sensitivity, complexity and non-transparency, but no particular events solely attributable to the components programmability have been identified, hence a review of the recent safety-significant events and their relation to digital I&C was made.

A number of recent particular electrical events of safety significance in the Swedish NPPs are listed in Table 1.

Table 1. Recent events at Swedish NPPs.

Event	Ref.	Issue	Root cause(s)
Ringhals 2, 2001	IRS-7459	Incorrect software function	Validation of SW modification
Forsmark 1, 2006	IRS-7788	Multiple DiD failures	Protection coordination, functional specification, functional validation
Forsmark 2, 2008	IRS-8062	Incorrect functional implementation	Phase unbalance (lightning)
Forsmark 3, 2012	IRS-8294	Component dimensioning inadequate	Overvoltage
Forsmark 3, 2013	IRS-8315	Isolation device concept breakdown	Phase unbalance (breaker failure)

3.1. Ringhals 2, 2001, software misconfiguration

In 2001, an over-current relay tripped due to overload during a routine load switchover manoeuvre. The relay tripped far below the set value, at around 60% of nominal current although settings were correct. The relay type had been recently introduced during switchgear modernisations 1998-2001 and thus was found in several functions, including safety-related ones. The root cause was a software modification carried out to enable testing using the plants existing test equipment. The modification was fairly trivial, increasing the sampling frequency of the module, and expanding memory capacity to allow for the increased number of samples. However, the change of sampling frequency also affected the overload calculation in the upper part of the calculation range. Due to the modification being deemed minor, a full change management process was not considered necessary so this effect was not realised in the change management process nor at the factory acceptance test. At site, testing was done by the “highway method”, i.e. testing was limited to nominal current and a current over the trip threshold, and not by ramping which would have revealed the fault.

The deficiency in this case was actually in the software development process, where the equipment no longer conformed with the software design specification and was not detected in the development process.

There were opportunities to identify the fault prior to the relay entering operational service, in particular by:

1. The design modification should have been recognised as major, and
2. Complete functional testing should have been carried out

3.1. Forsmark 1, 2006, ”the Forsmark event”

A voltage transient was generated off-site and propagated through the station electrical system, causing two out of four UPS units to trip non-selectively, and consequently the corresponding EDG units failed to start. There were software based components in the rectifier unit, which had no errors contributing to the event progression, however indications are that there was a functionality that contributed to the event progression. When the transient arrived at the UPS, the rectifier initially shut down, due to the overvoltage on the DC side. In such a situation, the rectifier automatically attempts to reconnect after a time delay and it was at the first reconnection attempt that the trip occurred non-selectively. Regardless, the transient situation as such had not been foreseen, hence the equipment was not validated for such a situation.

1. The transient design basis for the equipment should be well understood and defined, and
2. The functional behaviour of the equipment (reconnection) should have been understood in the design

An independent aggravating error was that the grid switchover functionality was incorrectly implemented so that switch over to the standby grid was not done automatically as it should. The under frequency relay that should initiate the switchover had been replaced a few years earlier and had a phase order dependency that had not been recognised in the design and no primary testing of the function had been carried out.

1. The component functional requirements should have been identified during design, and
2. Primary testing should have been carried out after the installation

Another independent error was that the gas turbine did not start as it should in such a situation according to the safety analysis report. This was due to faults in the gas turbine start control equipment, which is software based. Investigations found that the processor was non-functional and that part of the software was missing. A contributing cause is likely that the gas turbine is not safety classified and hence does not receive the same attention as safety classified systems.

1. The safety significance of of systems, structures and components with safety-significance should be clarified, and
2. Adequate testing and validation should be carried out regularly

3.2. Forsmark 2, 2008, phase unbalance

A lightning strike at Forsmark 2 in 2008 caused a phase unbalance that tripped the UPS powering the reactor circulation pumps (RCP). The plant remained connected to the external grid during and after the disturbance, but the power level dropped to 40% due to the tripped RCPs and the reactor was soon after tripped manually. When the RCPs lose power supply, a flywheel storage should provide energy to let the RCPs run down according to a pre-defined ramp to reduce thermal stress on the fuel rods. The logic to initiate this ramp was not activated in this scenario, as normal bus power was available and the reactor had not tripped from the event. Therefore the coolant flow was reduced faster than designed for in the technical specifications.

There were no failures in the digital equipment due to the event, but the behaviour had not been adequately addressed in the design stage and the component protection took priority over the safety feature.

1. The component functional requirements should have been identified during design

3.3. Forsmark 3, 2012, overvoltage

A lightning strike at Forsmark 3 in 2012 caused an overvoltage transient that propagated through the distribution system and destroyed one of four safety related UPS by exceeding the withstandability of the electrical by-pass switch. The surge arrestors installed at the stand-by grid step-down transformer were insufficiently dimensioned to limit the transient peak sufficiently to avoid the damage. Furthermore, as no transient recorders are available at this voltage level, the exact amplitude of the peak can only be estimated.

1. The component withstandability should be matched to the ambient electrical conditions at the point of connection

3.4. Forsmark 3, 2013, phase unbalance

During outage, the station was fed through only one breaker to the external grid. Testing of the main generator AVR inadvertently tripped the breaker to the grid, but one phase remained connected. This caused a voltage unbalance on the internal power system, but insufficient to start the emergency diesel generators and isolate the emergency power systems and instead safety related objects tripped due to phase unbalance. The isolation device concept was inadequate to handle a phase unbalance situation.

1. The design basis for the equipment should be well understood and defined, and
2. The isolation device concept should be adapted to the design basis

4. Findings and recommendations

The main reasons for recent failures have been an incomplete design basis, with an over-reliance on existing principles during modernisations. Therefore, an emphasis should be placed on establishment of an appropriate design basis, with a re-assessment of the design basis for changes in system topology or component type. This should take into account electrical system modelling of possible failures as well as an understanding of component behaviour and sensitivities. With more complex components with increasing sensitivities and enhanced functionalities, an increasingly accurate understanding needs to be established. With obsolescence of components, this is an inevitable evolution, but mitigating steps can be taken by establishing vendor liaison to maintain the required spare parts.

Faults in the electrical systems have been challenging to analyse, often due to a lack of detailed information about the electrical situation, and in this area, increased measurement and monitoring would contribute to a better understanding of the electrical ambience in the plant. Here, digital I&C could be utilised to a larger extent without affecting the functionality of equipment. In some complex situations, digital I&C may as well present the best option for protection, such as phase unbalance being difficult to measure accurately with analogue devices.

Using particular design solutions is generally undesirable, as it leads to a limited knowledge base, and well known and validated designs should be preferred. As digital I&C is becoming increasingly commonplace and analogue counterparts are becoming rare, it may be a preferred solution to use the better known component with a larger knowledge- and experience base. Validation methods are well established, but puts more configuration management requirements on operators and vendors. In order to utilise the collective knowledge base, there needs to be an effective means of communicating operating experiences between users and vendor.

5. Conclusion

Even though the notable penetration of programmable electronic components in the electrical power systems of the Swedish NPPs, the review has not identified any causal relation between digital I&C components and an increasing failure rate. The main limitation seen is an incomplete design basis, incompletely understood functionality and an incomplete design verification. Any feature-rich SSC will exhibit similar challenges, but with digital I&C having increased sensitivity as well as enhanced functionality they will require a more thorough assessment than did simpler, analogue designs with fewer features and lower sensitivity.

The well-known principles of prevention, protection and mitigation remain valid and focus need to shift from digital components in particular to a general concept of design basis for electrical systems accompanied with thorough functional specifications, fit for purpose with well-defined behaviours. A re-assessment of the design basis should always to be made during component replacements as extant design basis for the plant is not generally applicable for modern equipment.

A modernisation needs to encompass a modernisation of design requirements as well as of the devices themselves.

References

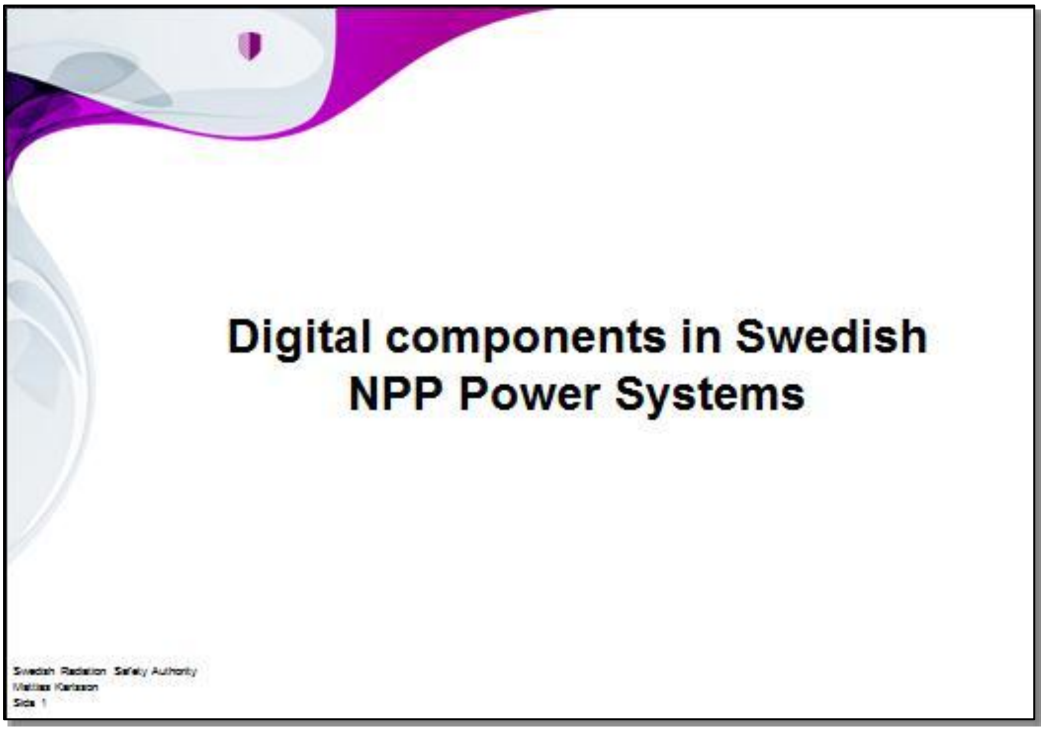
IRS-7459, INCORRECT ALGORITHM IN MEMORY MODULE OF OVERLOAD PROTECTION DEVICES

IRS-7788, LOSS OF 400 KV AND SUBSEQUENT FAILURE TO START EMERGENCY DIESEL GENERATORS IN SUB A AND SUB B

IRS-8062, DISCREPANCY WITH THE ASSUMPTIONS IN SAR SAFETY ANALYSES
NRC-IN-2010-17, COMMON CAUSE FAILURE OF BOILING-WATER REACTOR RECIRCULATION PUMPS WITH VARIABLE SPEED DRIVES

IRS-8294, LOW VOLTAGE SAFETY GRADE POWER ELECTRONICS FAILED DUE TO AN HV OVERHEAD LINE LIGHTNING OVERVOLTAGE

IRS-8315, EDG FAILED TO START AFTER UNDETECTED LOSS OF TWO PHASES ON 400 KV INCOMING OFFSITE SUPPLY


Digital components in Swedish NPP Power Systems
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 1

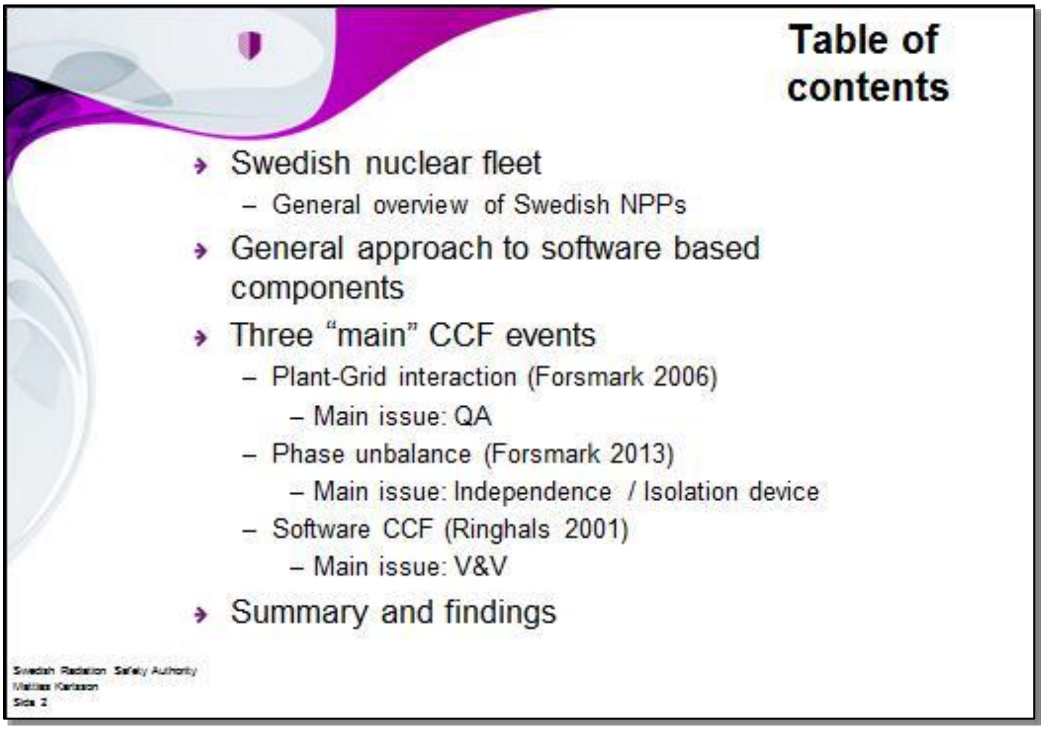
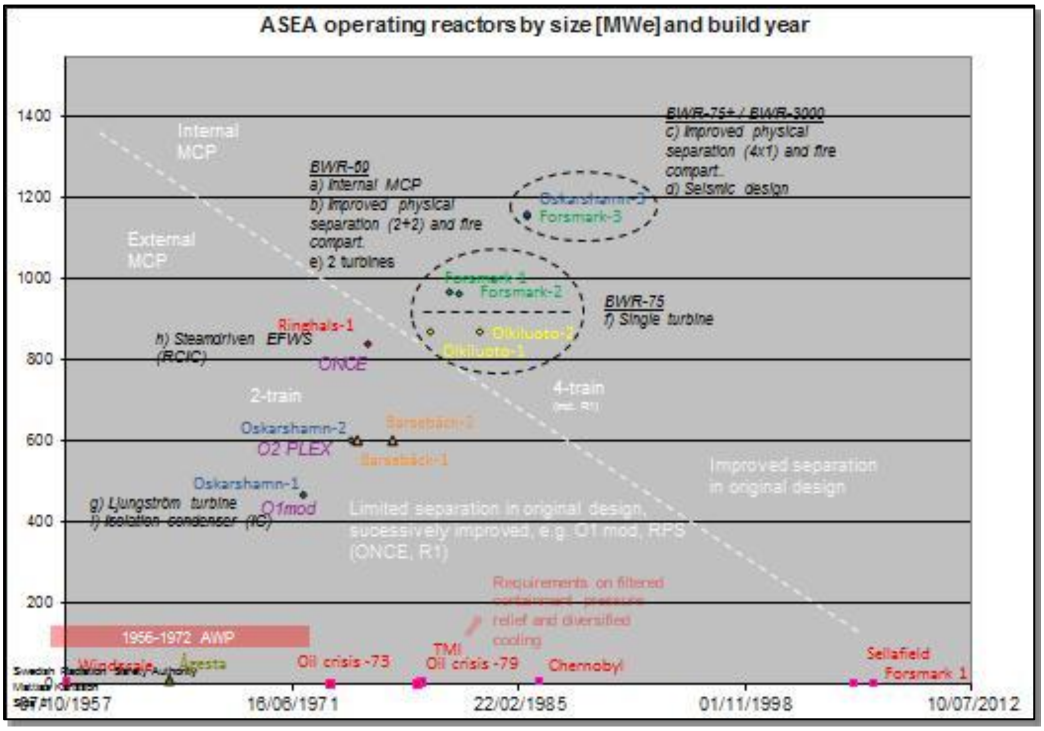
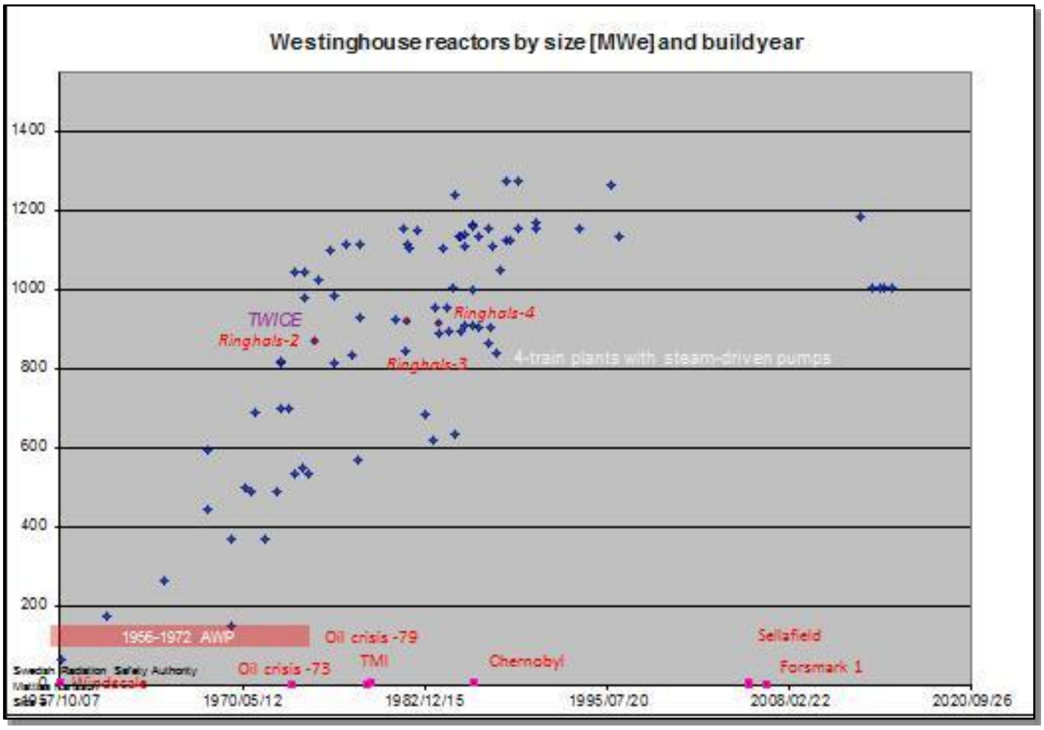
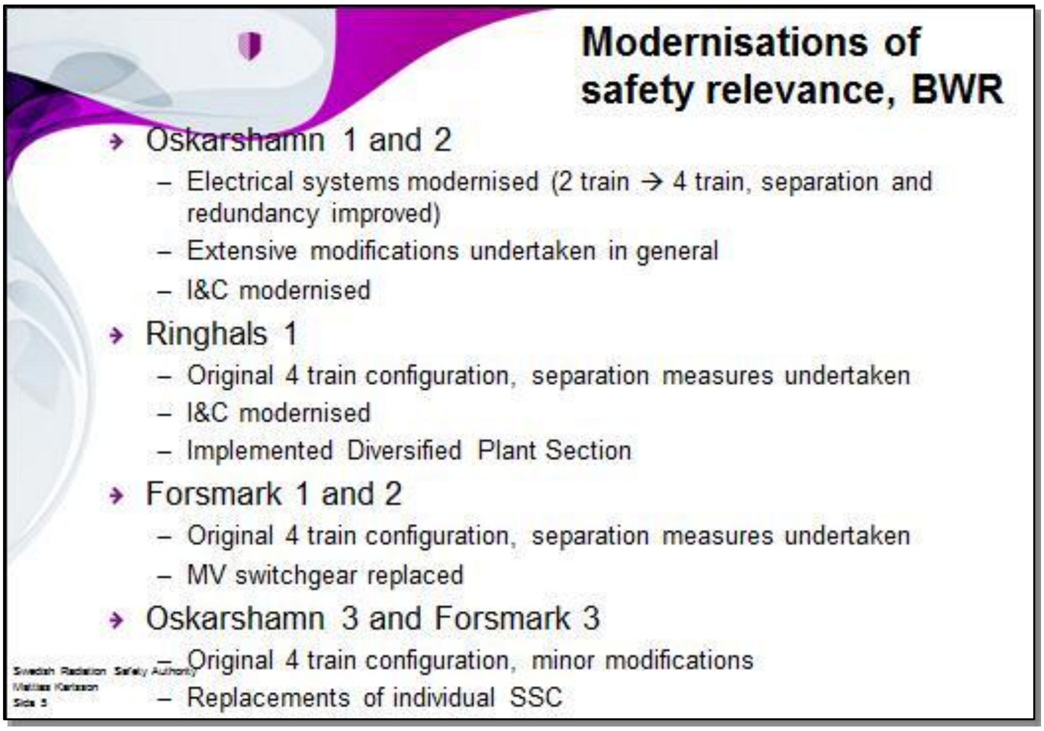
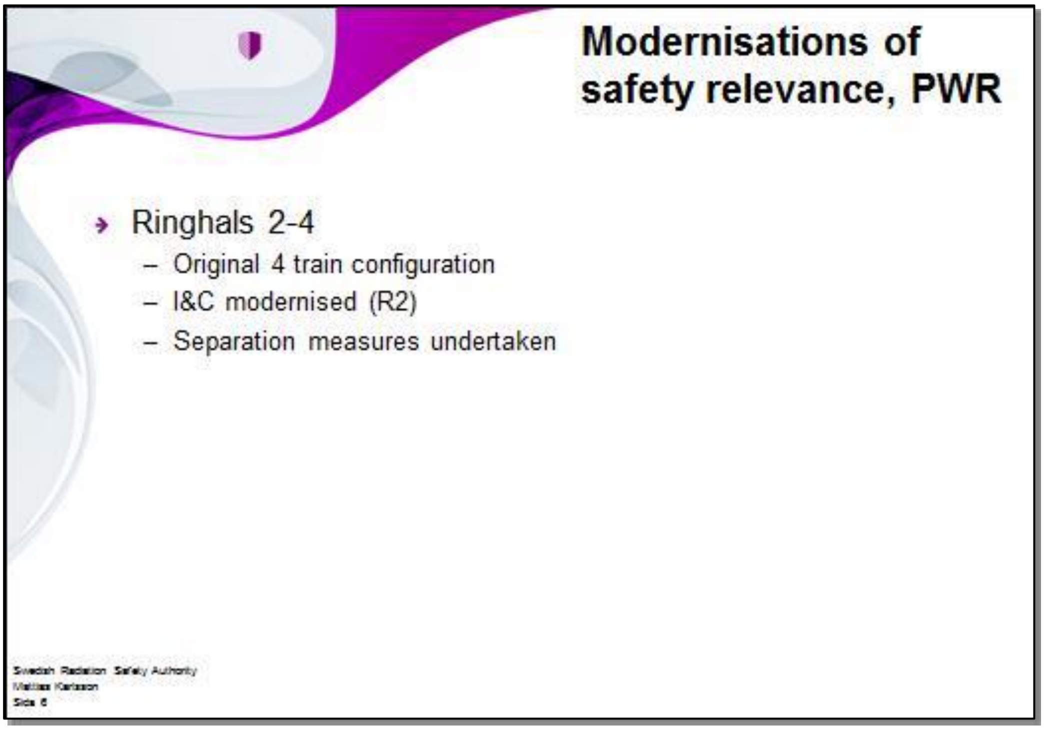


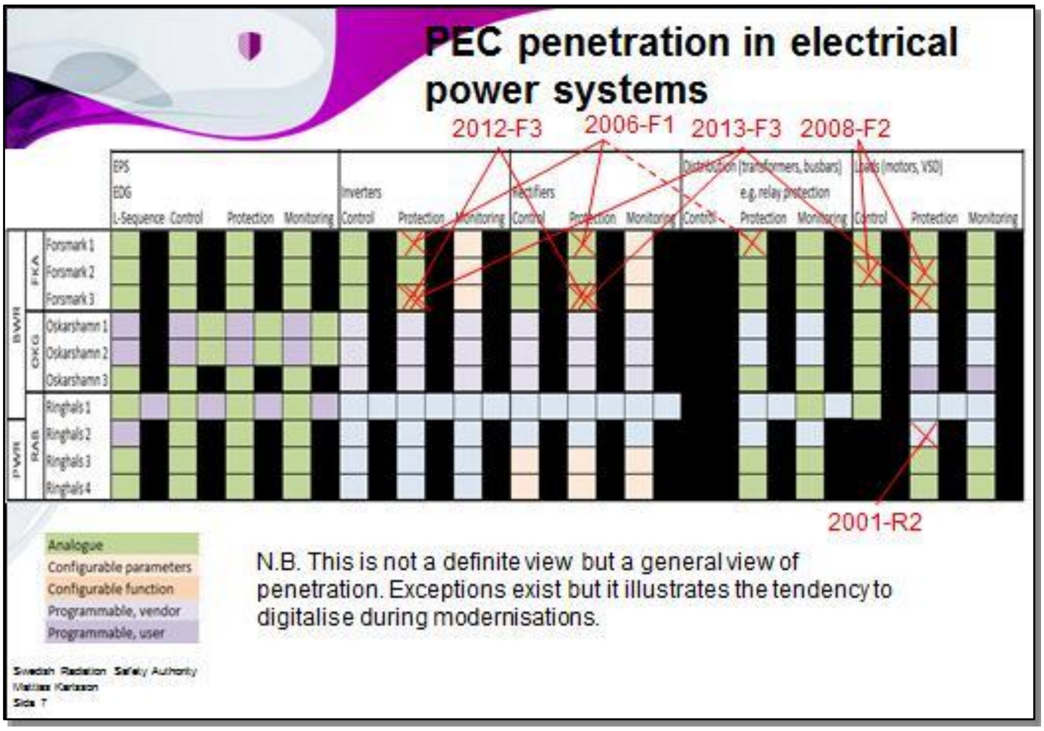
Table of contents
Swedish nuclear fleet
– General overview of Swedish NPPs
General approach to software based components
Three "main" CCF events
– Plant-Grid interaction (Forsmark 2006)
– Main issue: QA
– Phase unbalance (Forsmark 2013)
– Main issue: Independence / Isolation device
– Software CCF (Ringhals 2001)
– Main issue: V&V
Summary and findings
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 2

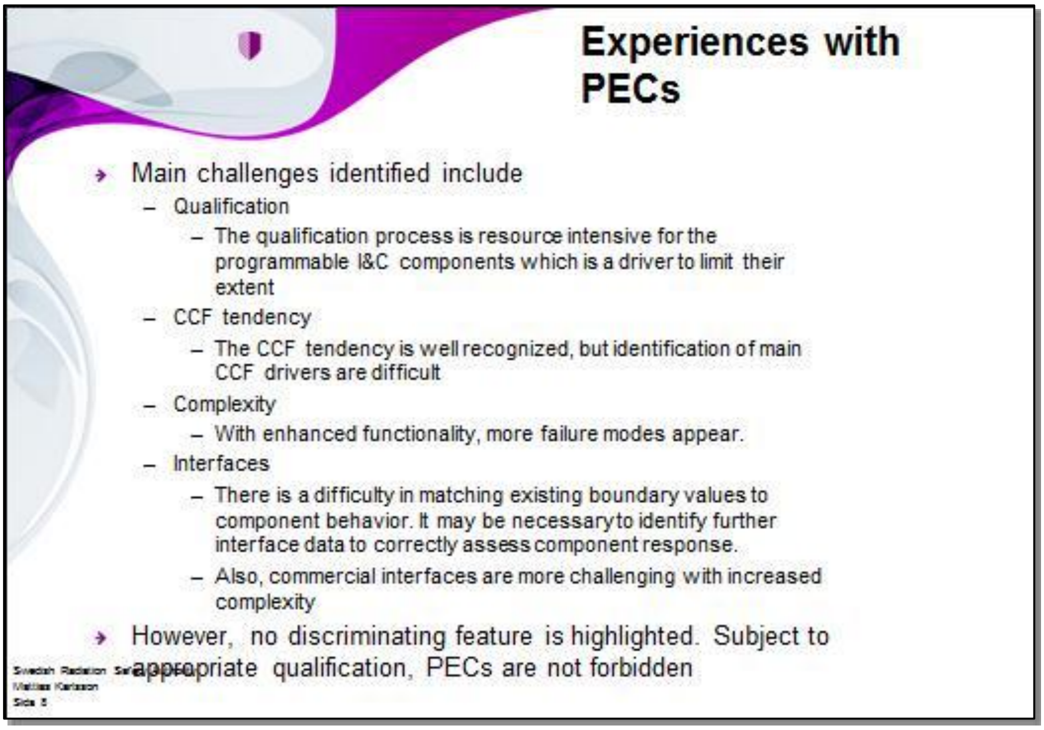

ASEA operating reactors by size [MWe] and build year
1400
1200
1000
800
600
400
200
Internal MCP
External MCP
BWR-69
a) Internal MCP
b) Improved physical separation (2+2) and fire compart.
e) 2 turbines
BWR-75+ / BWR-3000
c) Improved physical separation (4x1) and fire compart.
d) Seismic design
Forsmark-3
Forsmark-2
BWR-75
f) Single turbine
Ringhals-1
h) Steamdriven EFWS (RCIC)
ONCE
2-train
4-train
Oskarshamn-2
O2 PLEX
Barsebäck-1
Oskarshamn-1
g) Ljungström turbine
i) Isolation condenser (IC)
O1mod
Limited separation in original design, sucessively improved, e.g. O1 mod, RPS (ONCE, R1)
Improved separation in original design
Requirements on filtered
relief and diversified cooling
1956-1972 AWP
Oil crisis -73
TMI
Oil crisis -79
Chernobyl
Sellafield
Forsmark 1
16/06/1971
22/02/1985
01/11/1998
10/07/2012

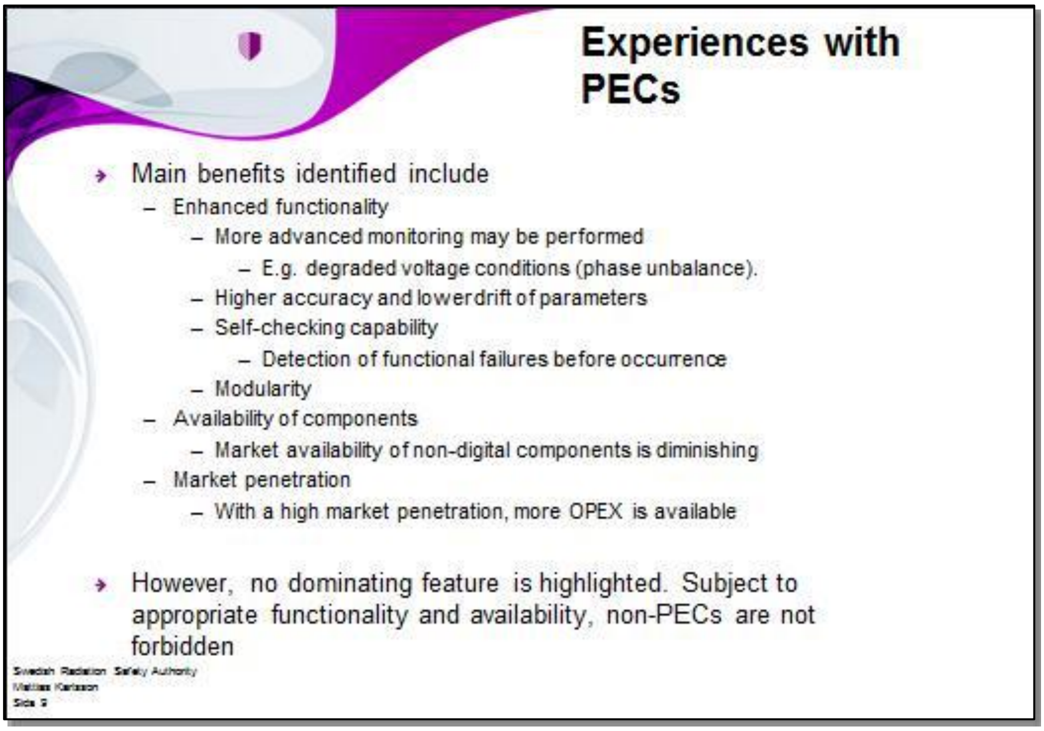

Westinghouse reactors by size [MWe] and buildyear
1400
1200
1000
800
600
400
200
TWICE
Ringhals-2
Ringhals-4
Ringhals-3
4-train plants with steam-driven pumps
1956-1972 AWP
Oil crisis -79
Oil crisis -73
TMI
Chernobyl
Sellafield
Forsmark 1
Swedish Radiation Safety Authority
Windscale
1970/05/12
1982/12/15
1995/07/20
2008/02/22
2020/09/26

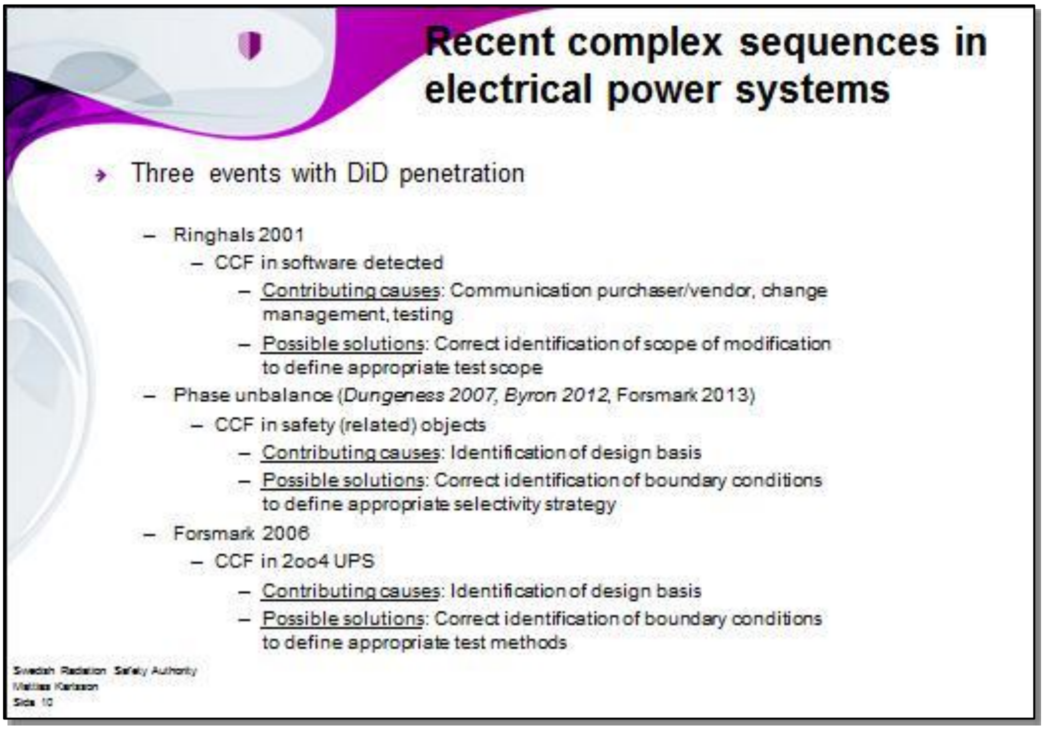

Modernisations of safety relevance, BWR
Oskarshamn 1 and 2
– Electrical systems modernised (2 train → 4 train, separation and redundancy improved)
– Extensive modifications undertaken in general
– I&C modernised
Ringhals 1
– Original 4 train configuration, separation measures undertaken
– I&C modernised
– Implemented Diversified Plant Section
Forsmark 1 and 2
– Original 4 train configuration, separation measures undertaken
– MV switchgear replaced
Oskarshamn 3 and Forsmark 3
– Original 4 train configuration, minor modifications
– Replacements of individual SSC
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 5


Modernisations of safety relevance, PWR
Ringhals 2-4
– Original 4 train configuration
– I&C modernised (R2)
– Separation measures undertaken
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 6


PEC penetration in electrical power systems
2012-F3
2006-F1
2013-F3
2008-F2
EPS
EDG
L-Sequence Control
Protection
Monitoring
Inverters
Control
Protection
Monitoring
Rectifiers
Control
Protection
Monitoring
Distribution (transformers, busbars)
e.g. relay protection
Control
Protection
Monitoring
Loads (motors, VSD)
Control
Protection
Monitoring
BWR
FKA
Forsmark 1
Forsmark 2
Forsmark 3
OKG
Oskarshamn 1
Oskarshamn 2
Oskarshamn 3
PWR
RAB
Ringhals 1
Ringhals 2
Ringhals 3
Ringhals 4
2001-R2
Analogue
Configurable parameters
Configurable function
Programmable, vendor
Programmable, user
N.B. This is not a definite view but a general view of penetration. Exceptions exist but it illustrates the tendency to digitalise during modernisations.
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 7


Experiences with PECs
Main challenges identified include
– Qualification
– The qualification process is resource intensive for the programmable I&C components which is a driver to limit their extent
– CCF tendency
– The CCF tendency is well recognized, but identification of main CCF drivers are difficult
– Complexity
– With enhanced functionality, more failure modes appear.
– Interfaces
– There is a difficulty in matching existing boundary values to component behavior. It may be necessary to identify further interface data to correctly assess component response.
– Also, commercial interfaces are more challenging with increased complexity
However, no discriminating feature is highlighted. Subject to appropriate qualification, PECs are not forbidden
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 8


Experiences with PECs
Main benefits identified include
– Enhanced functionality
– More advanced monitoring may be performed
– E.g. degraded voltage conditions (phase unbalance).
– Higher accuracy and lower drift of parameters
– Self-checking capability
– Detection of functional failures before occurrence
– Modularity
– Availability of components
– Market availability of non-digital components is diminishing
– Market penetration
– With a high market penetration, more OPEX is available
However, no dominating feature is highlighted. Subject to appropriate functionality and availability, non-PECs are not forbidden
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 9


Recent complex sequences in electrical power systems
Three events with DiD penetration
– Ringhals 2001
– CCF in software detected
– Contributing causes: Communication purchaser/vendor, change management, testing
– Possible solutions: Correct identification of scope of modification to define appropriate test scope
– Phase unbalance (Dungeness 2007, Byron 2012, Forsmark 2013)
– CCF in safety (related) objects
– Contributing causes: Identification of design basis
– Possible solutions: Correct identification of boundary conditions to define appropriate selectivity strategy
– Forsmark 2006
– CCF in 2oo4 UPS
– Contributing causes: Identification of design basis
– Possible solutions: Correct identification of boundary conditions to define appropriate test methods
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 10

Observations with PECs

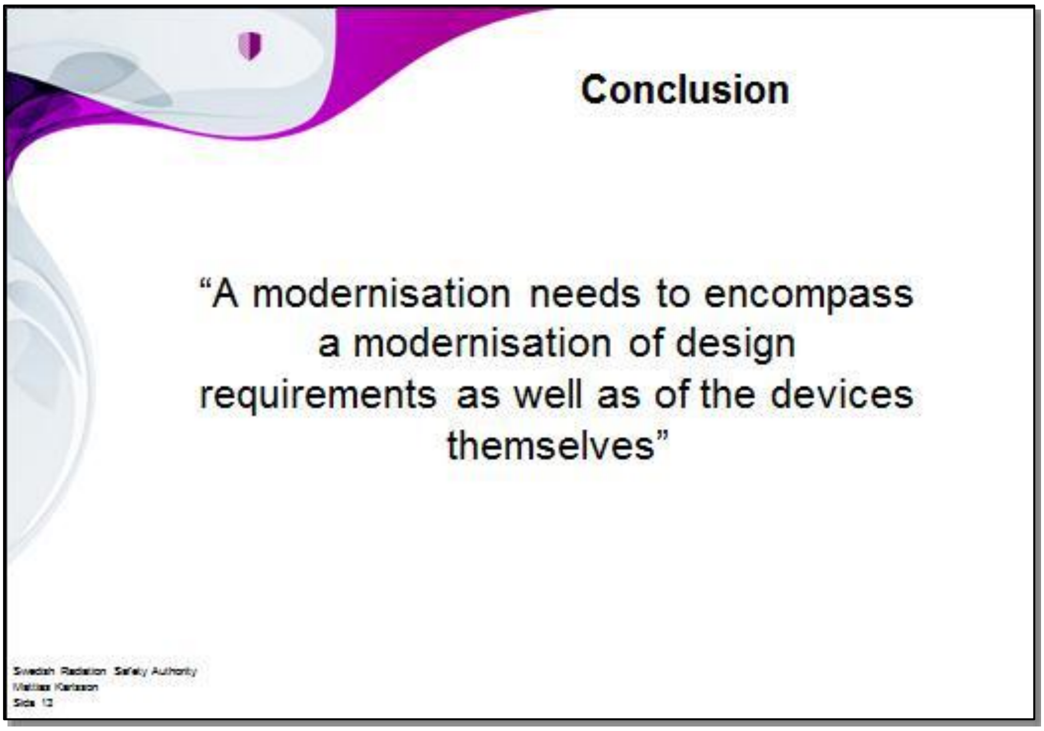
- Design philosophy does not generally cover autonomous distributed PECs
- It is generally at the discretion of the system designer to consider the feasibility of PECs
  - Established requirements for PECs are used for V&V
- There are no regulatory limitations on PECs as long as safety requirements are met
- How to identify that safety requirements are met when complexity increases?

Swedish Radiation Safety Authority
Mattias Karlsson
Side 11

Findings

- No unique errors attributable solely to thePEC have been identified
  - The programmable element is usually well considered and has not been a major contributor to recent issues
- The analysed high-impact events reviewed could have been detected by identification of proper design basis and validation / test methods
  - Phase unbalance has not been identified in the design basis. Components with a robustness to phase unbalance are rare (i.e. motors are unbalance sensitive).
  - Fast transients have not been identified in the design basis. Some robustness to transients can be achieved by inertia devices (e.g. motors)
  - Change management is critical for any change
- Complexity is the major challenge
  - Microprocessor based devices contribute to an increase in complexity
- More effort is required to establish an appropriate <u>design basis</u> and appropriate <u>functional validation</u>

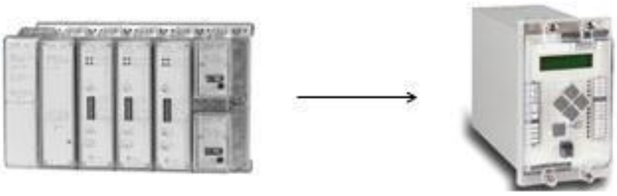
Swedish Radiation Safety Authority
Mattias Karlsson
Side 12


Conclusion
“A modernisation needs to encompass a modernisation of design requirements as well as of the devices themselves”
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 13


Ringhals 2001 event brief
IRS-7459
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 14

Introduction

- Overload protection relay replacement
  - Type replacement in several systems



- During FAT, incompatibility between test equipment and component is identified
- Vendor agrees to rectify issue

Swedish Radiation Safety Authority
Mattias Karlsson
Sida 15

Problem solution

- Vendor identifies that an increase in sampling frequency solves the issue
- Solution is achieved by software modification
  - A HW configuration change is also required to increase memory
- As a minor adaptation, full validation is not required according to vendor instructions
  - Purchaser does not identify the need for enhanced validation

Swedish Radiation Safety Authority
Mattias Karlsson
Sida 16

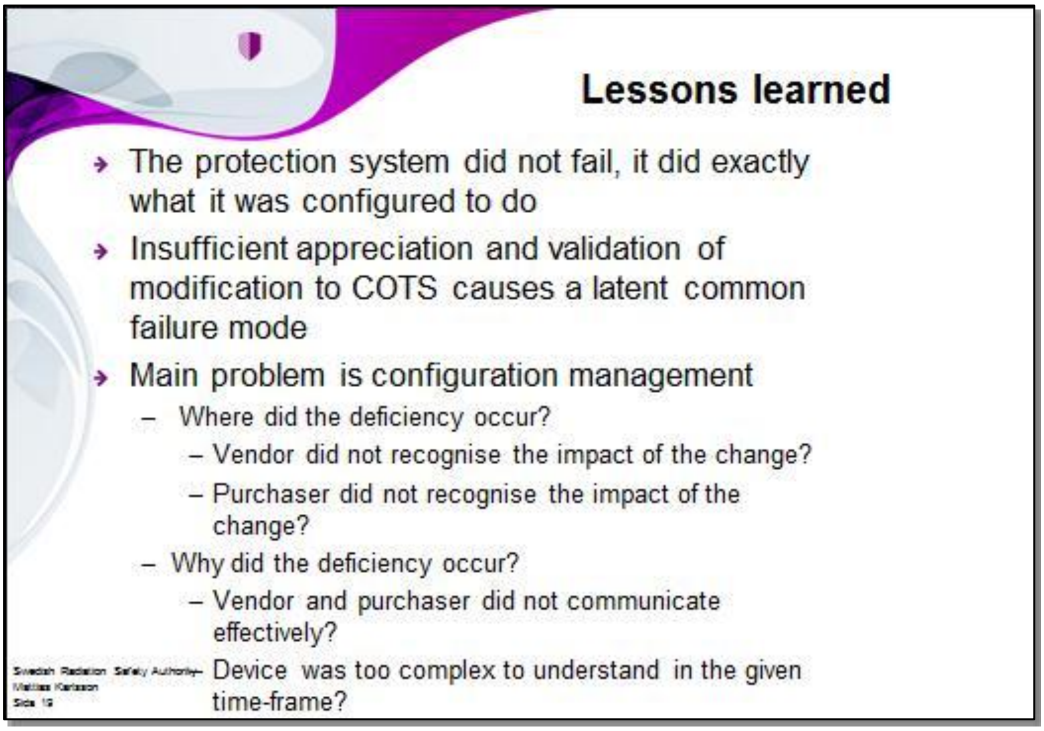
Problem creation

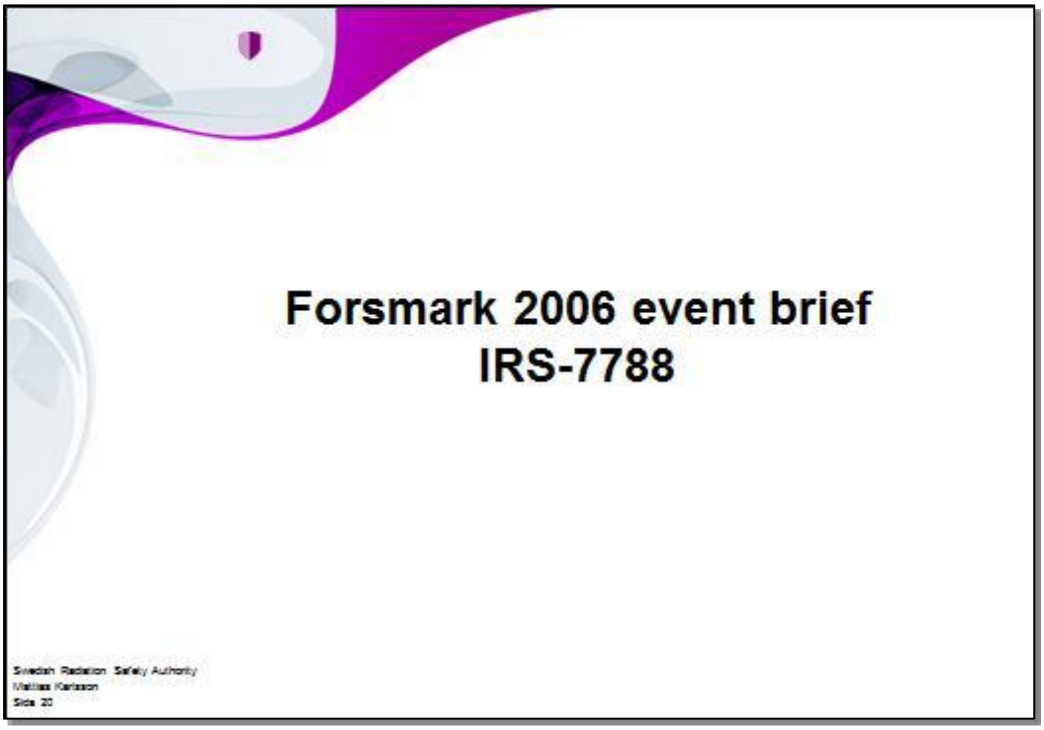
- However, the sampling frequency change causes an error in the overload calculation
  - Overload is detected earlier than desired!
- SAT testing is done by ”highway method” – problem is not detected
  - A ramp test would have detected the discrepancy!

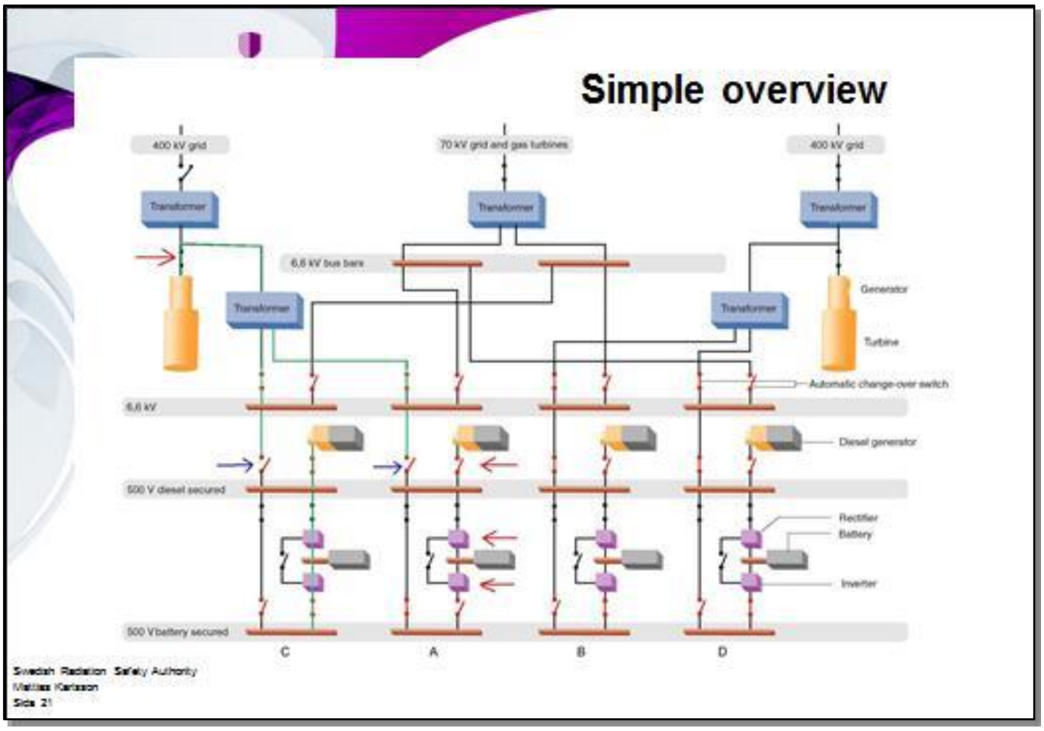
Problem detection

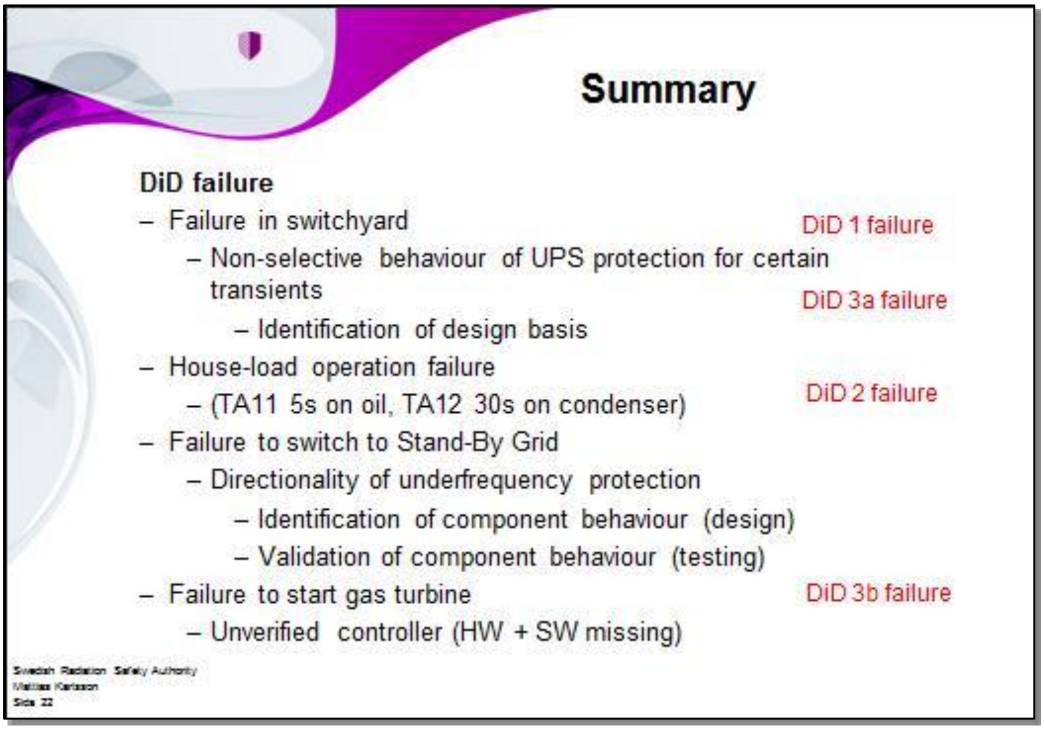
- During operation, the fault is initially undetected due to overdimensioning of cables (low currents)
- During a routine operation of load switchover, a relay trips far below (60%) the overload threshold
- Fault finding commences and identifies the error as a CCF and eventually concludes the described sequence

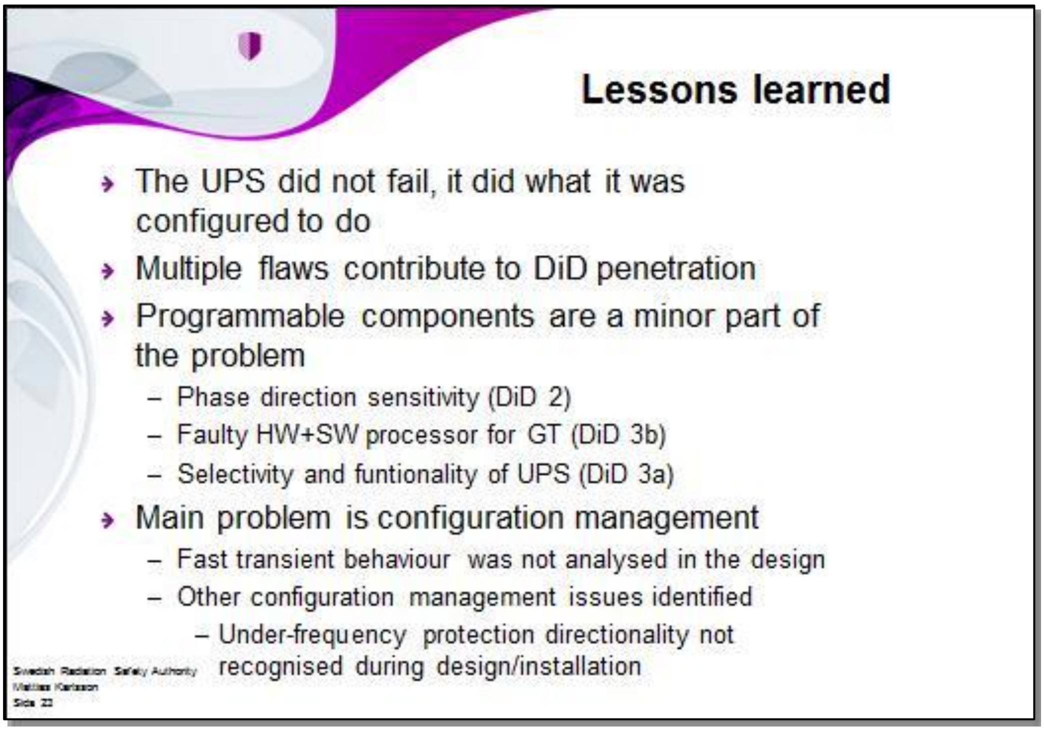
- Problem is resolved by correcting the flaw and improvement of routines initiated

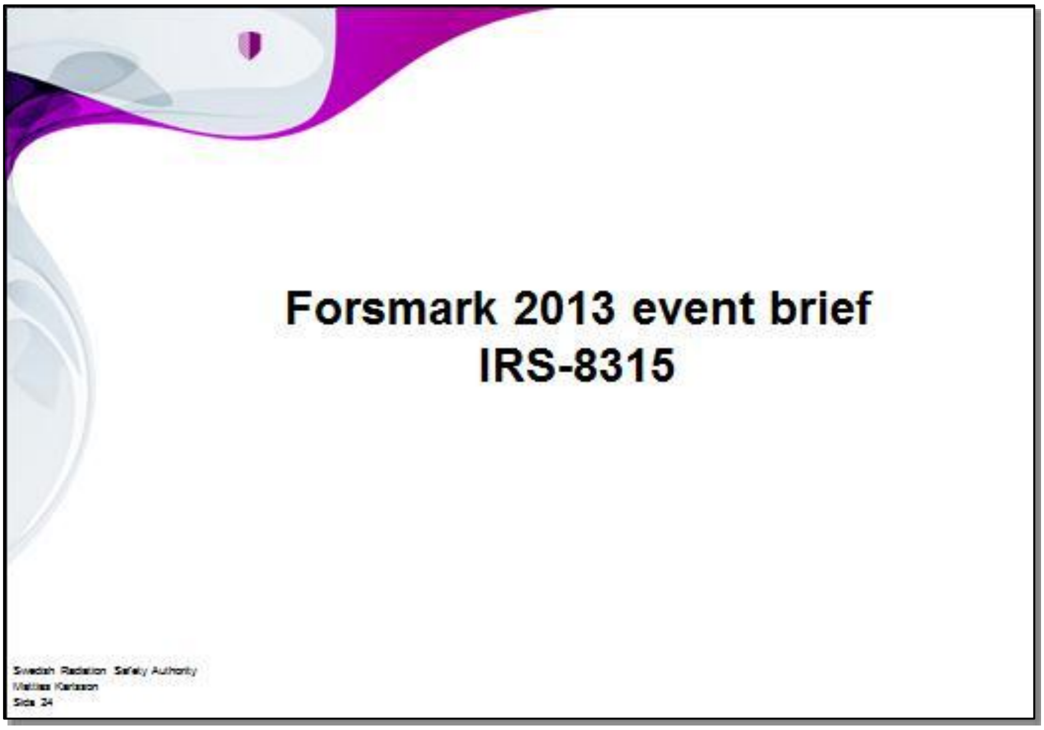

Lessons learned
The protection system did not fail, it did exactly what it was configured to do
Insufficient appreciation and validation of modification to COTS causes a latent common failure mode
Main problem is configuration management
– Where did the deficiency occur?
– Vendor did not recognise the impact of the change?
– Purchaser did not recognise the impact of the change?
– Why did the deficiency occur?
– Vendor and purchaser did not communicate effectively?
– Device was too complex to understand in the given time-frame?
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 19

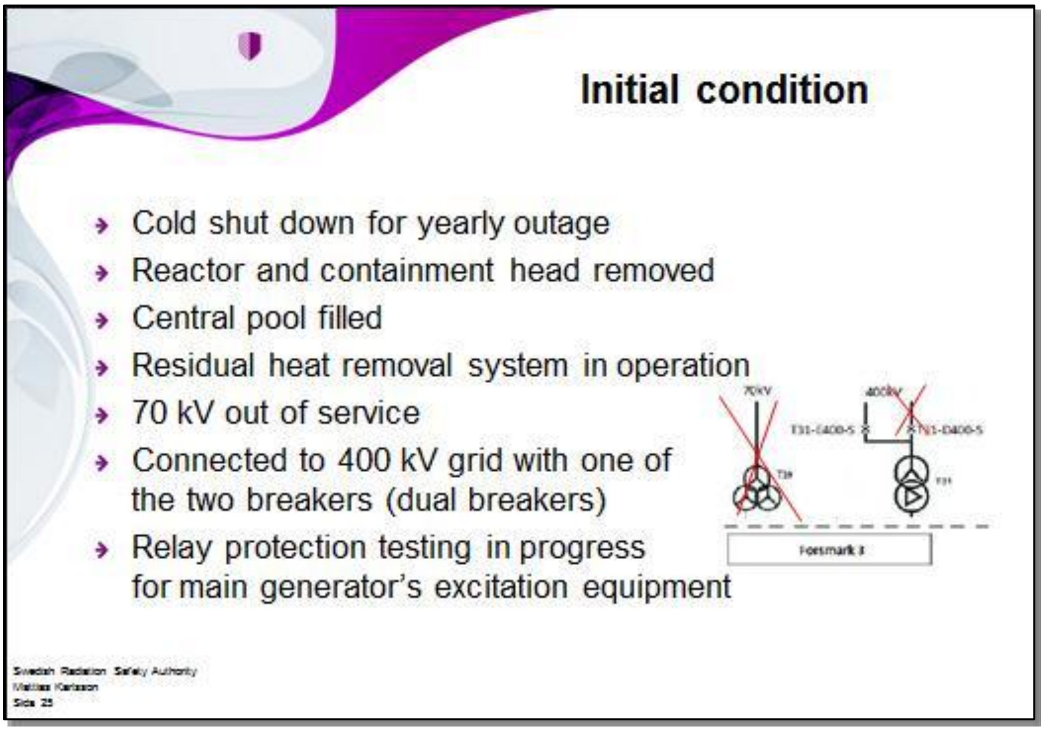

Forsmark 2006 event brief
IRS-7788
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 20

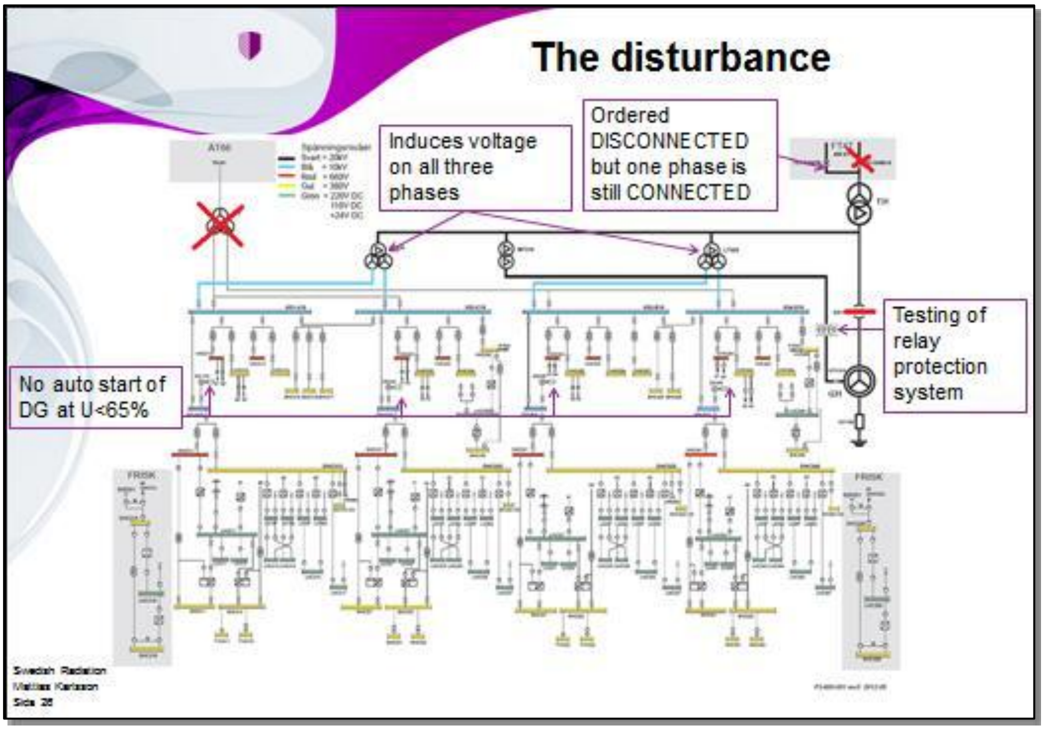

Simple overview
400 kV grid
70 kV grid and gas turbines
400 kV grid
Transformer
Transformer
Transformer
6,6 kV bus bars
Transformer
Transformer
Generator
Turbine
Automatic change-over switch
6,6 kV
Diesel generator
500 V diesel secured
Rectifier
Battery
Inverter
500 V battery secured
C
A
B
D
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 21

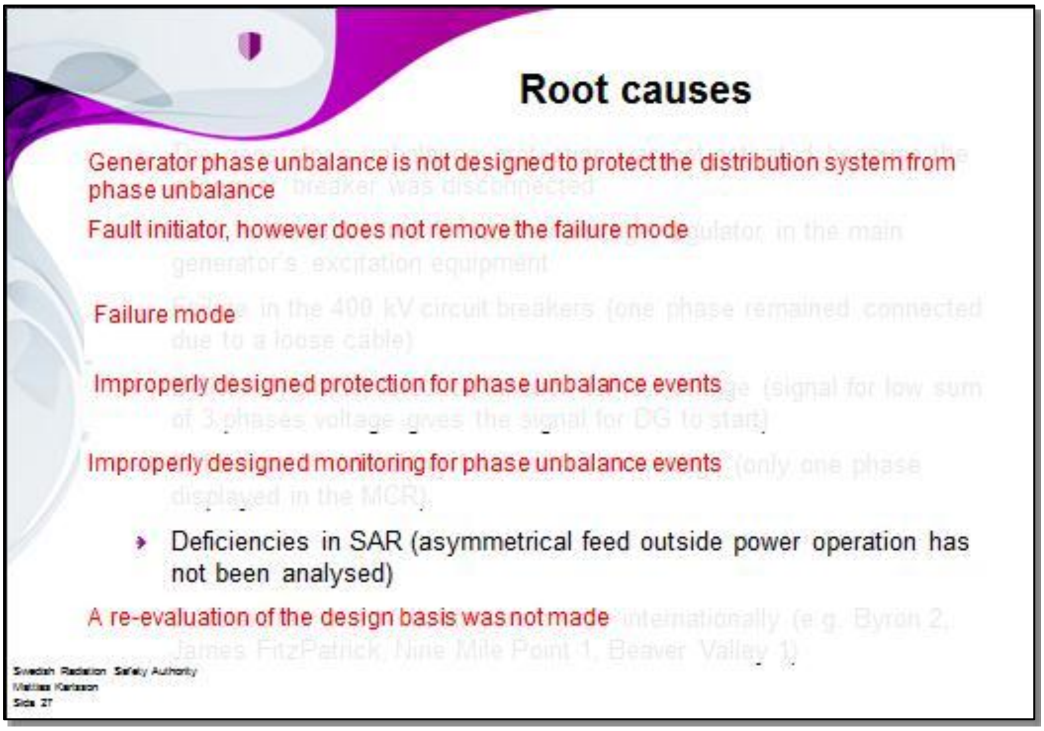

Summary
DiD failure
– Failure in switchyard
DiD 1 failure
– Non-selective behaviour of UPS protection for certain transients
DiD 3a failure
– Identification of design basis
– House-load operation failure
– (TA11 5s on oil, TA12 30s on condenser)
DiD 2 failure
– Failure to switch to Stand-By Grid
– Directionality of underfrequency protection
– Identification of component behaviour (design)
– Validation of component behaviour (testing)
– Failure to start gas turbine
DiD 3b failure
– Unverified controller (HW + SW missing)
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 22

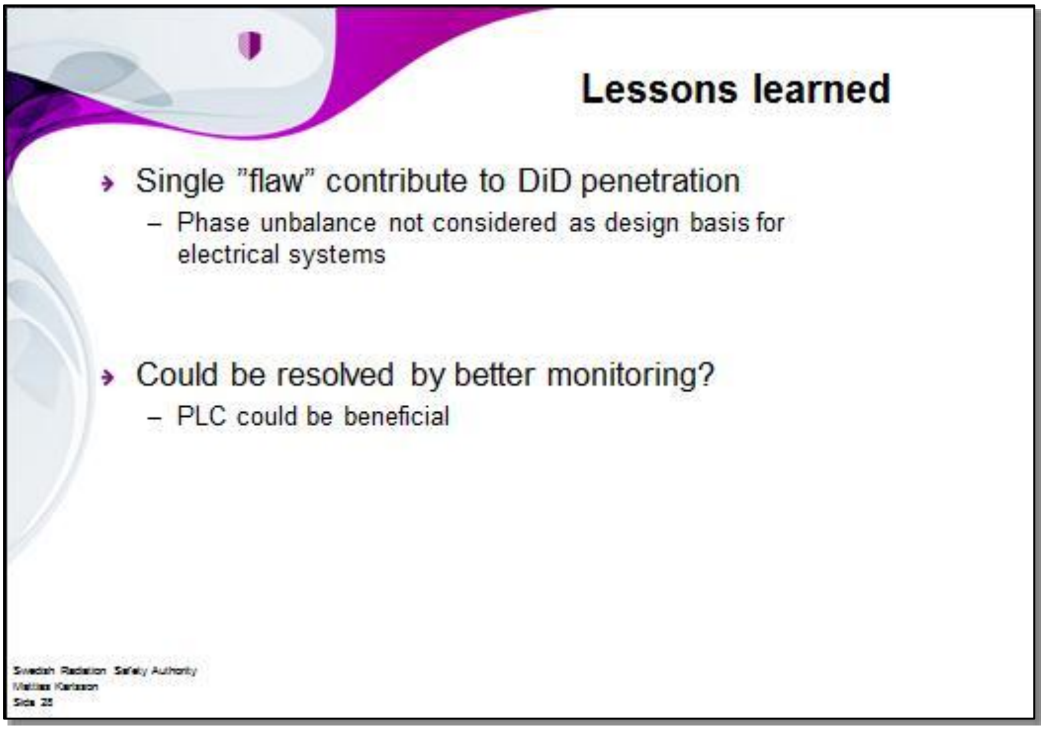

Lessons learned
The UPS did not fail, it did what it was configured to do
Multiple flaws contribute to DiD penetration
Programmable components are a minor part of the problem
– Phase direction sensitivity (DiD 2)
– Faulty HW+SW processor for GT (DiD 3b)
– Selectivity and funtionality of UPS (DiD 3a)
Main problem is configuration management
– Fast transient behaviour was not analysed in the design
– Other configuration management issues identified
– Under-frequency protection directionality not recognised during design/installation
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 23


Forsmark 2013 event brief
IRS-8315
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 24


Initial condition
Cold shut down for yearly outage
Reactor and containment head removed
Central pool filled
Residual heat removal system in operation
70 kV out of service
Connected to 400 kV grid with one of the two breakers (dual breakers)
Relay protection testing in progress for main generator's excitation equipment
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 25


The disturbance
Induces voltage on all three phases
Ordered DISCONNECTED but one phase is still CONNECTED
Testing of relay protection system
No auto start of DG at U<65%
Swedish Radiation
Mattias Karlsson
Sida 26


Root causes
Generator phase unbalance is not designed to protect the distribution system from phase unbalance
Fault initiator, however does not remove the failure mode
Failure mode
Improperly designed protection for phase unbalance events
Improperly designed monitoring for phase unbalance events
Deficiencies in SAR (asymmetrical feed outside power operation has not been analysed)
A re-evaluation of the design basis was not made
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 27


Lessons learned
Single "flaw" contribute to DiD penetration
– Phase unbalance not considered as design basis for electrical systems
Could be resolved by better monitoring?
– PLC could be beneficial
Swedish Radiation Safety Authority
Mattias Karlsson
Sida 28

Operating Experience of Digital, Software-based Components Used in I&C and Electrical Systems in German NPPs

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

André Lochthofen, Claudia Quester, Robert Arians
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Germany

Abstract

In recent years, many components in instrumentation and control (I&C) and electrical systems of nuclear power plants (NPPs) were replaced by digital, software-based components. Due to the more complex structure, software-based I&C and electrical components show the potential for new failure mechanisms and an increasing number of failure possibilities, including the potential for common cause failures. An evaluation of the operating experience of digital, software-based components may help to determine new failure modes of these components. In this paper, we give an overview over the results of the evaluation of the operating experience of digital, software-based components used in I&C and electrical systems in NPPs in Germany.

1. Introduction

The components of I&C and electrical systems in German NPPs are generally in use since the commissioning of the plants in the 1970s/1980s. Thus, an increasing amount of components of I&C and electrical systems has to be replaced reaching its end of lifetime. In recent years, many of them were replaced by digital, software-based components. Therefore, digital, software-based components both in safety and in non-safety systems show an increased use in NPPs. A further increase is expected as the supply of spare parts for hardwired systems is deteriorating.

The specific characteristics of digital, software-based components differ from the characteristics of non-digital components: They have e. g. a more complex structure, additional properties, changed failure behavior, and a changed man-machine-interface. Furthermore, digital, software-based components show the potential for new failure modes and an increasing number of failure possibilities due to the use of software or programmable logic.

As failure modes of digital, software-based components and man-machine-interface differ fundamentally from non-digital components, an evaluation of the operating experience of digital, software-based components used in I&C and electrical systems in NPPs in Germany was carried out by GRS. For this evaluation, data from different German NPPs, boiling water reactors (BWR) (type 69 and type 72) as well as pressurized water reactors (PWR) (Generation 2 up to Konvoi), were collected. To improve statistics and to include failures in non-safety systems, events not fulfilling the incident reporting criteria of German authorities are also included in this evaluation. The data provided by licensees of German NPPs were recorded between 2000 and 2012. Digital, software-based components used in the NPPs have been identified and their operating experience has been analyzed in order to identify relevant failure modes and to establish a knowledge base for future failure rating. Therefore, particular attention is paid to purely software-related failures as well as to the sensitivity of digital, software-based components to potential failures, e. g. stemming from ambient conditions like radiation.

2. Data collection

The data collected for the evaluation stem from different German NPPs. GRS collects data from German boiling water reactors and German pressurized water reactors, both of different types. GRS collected 1008 events stemming from the years 2000-2012 in 6 different German NPPs.

The 1008 events include components from I&C and electrical systems as well as from measuring transducers. 38.5 % of the data stem from I&C systems, 4.7 % of the data stem from electrical systems, and 56.8 % of the data stem from measuring transmitters. 6617 components installed (plant data) were recorded.

3. Evaluation of operational data

In a first step, the evaluation of the collected events focused on the following aspects:

- Affected process based systems
- Failure detection methods
- Relevance of software
- Relevance of environmental effects

The following figures show the process based systems, in which the evaluated events took place, figure 1 for boiling water reactors and figure 2 for pressurized water reactors. Only systems with a percentage higher than 5 % are shown, the remaining systems are summarized into “other”.

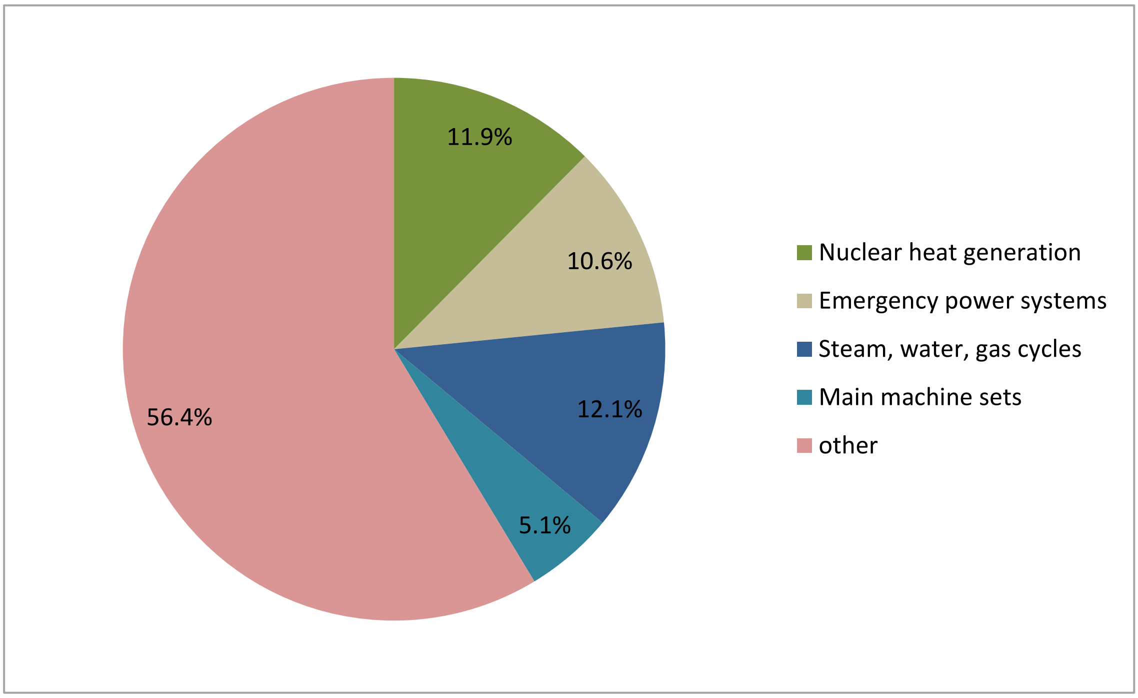


Figure 1: Systems in which the evaluated events took place (for boiling water reactors)

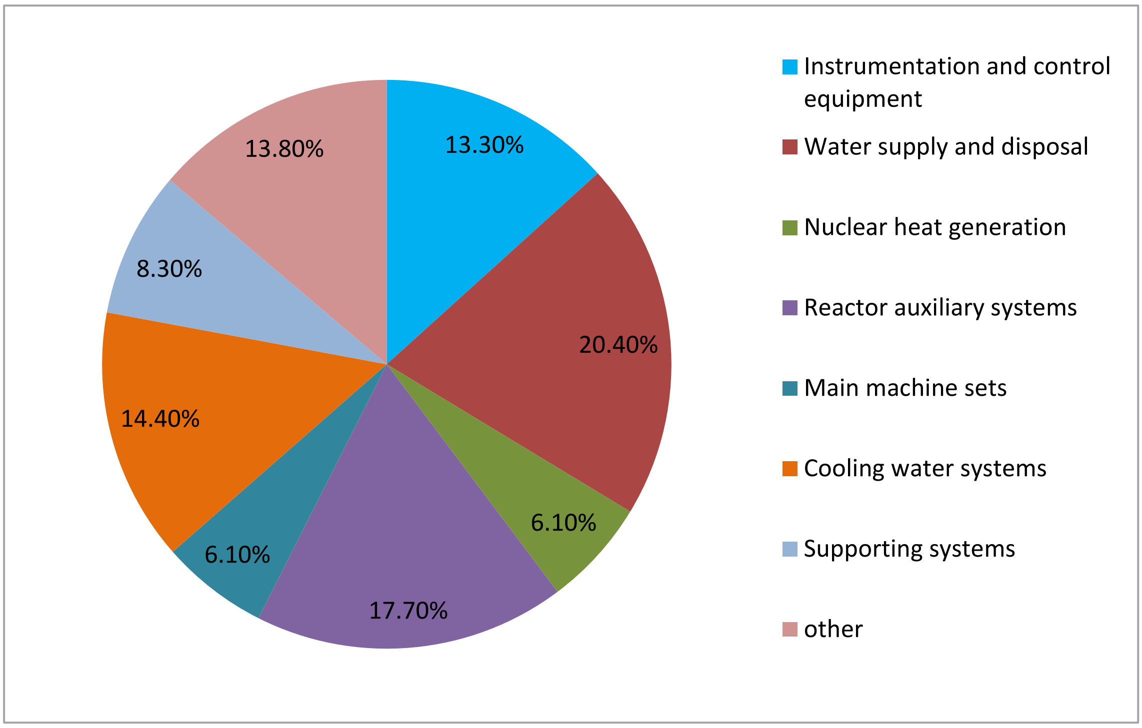


Figure 2: Systems in which the evaluated events took place (for pressurized water reactors)

Most of the evaluated events in boiling water reactors took place in the Steam, water and gas cycles (12.1 %), the nuclear heat generation (11.9 %) and the emergency power systems (10.6 %). For pressurized water reactors, most of the evaluated events took place in systems for water supply and disposal (20.4 %), the reactor auxiliary systems (17.7 %), and the cooling water systems (14.4 %).

The GRS analysis concerning failure detection showed that mostly, failures were detected during technical testing or by system warning. Only a small number of events caused a failure on demand. It was further evaluated how non-self-reporting failures were detected. Figure 3 shows the distribution of the different forms of failure detection for the non-self-reporting failures. It can be seen that most of the failures (77.4 %) were detected due to technical inspections, which means during a planned check of the component. Only a small amount of failures (4.4 %) were not detected until the component was requested (failure on demand). Also only small amounts of events were detected during operation (failure occurred while the component was operating) and at inspection tours of personnel (failure was detected on planned tours of the personnel). As most of the failures have been detected due to technical inspections and only a small amount of failures lead to a failure on demand, it can be stated that the current failure detection methods applied in the NPPs regarded in the analysis are suitable. But the events initiated by a failure on demand, if occurring in a safety system, can have a major impact on plant safety. Thus, an in-depth analysis of these events has to be performed.

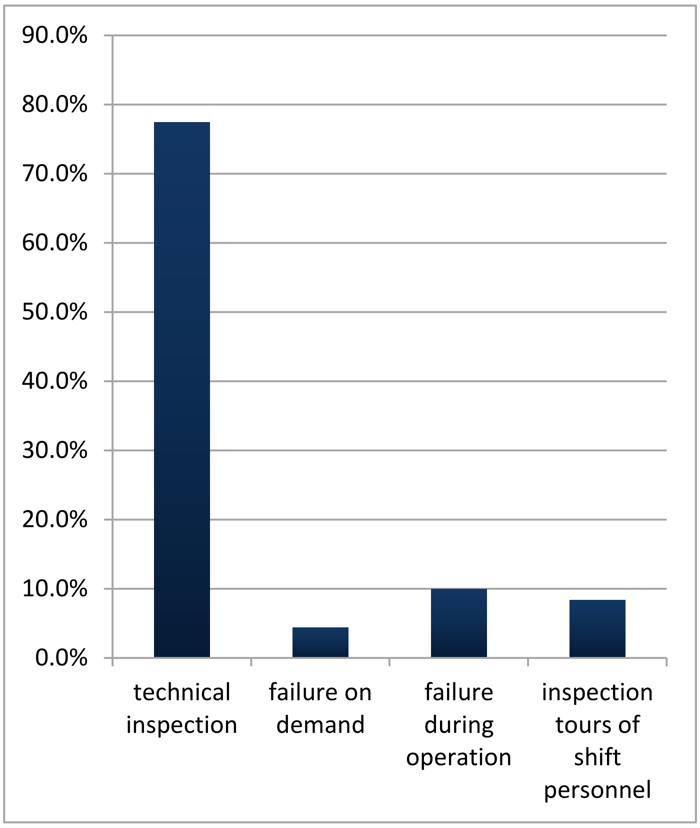


Figure 3: Failure detection of non-self-reporting events

In the GRS analysis, the data were divided into hardware and software failures as cause of the event. In order to identify possible new failure mechanisms in software-related events, these events were classified into three groups:

- RS: events in which the software has caused the event, like e. g. programming errors
- HS: events in which a hardware error is the cause for a software failure, like e. g. buffer batteries
- KS: events caused by a failure of the part which is related to software but which will not necessarily lead to failure of the whole component, like e. g. displays

Other events which are purely hardware-related are not considered in this evaluation. Figure 4 shows the results of this classification in groups. On the left side of figure 4, the software-related events (RS, HS, and KS) are shown in comparison to purely hardware-related events. It can be seen that even in digital, software-based components, which are considered in this analysis only, most of the events show purely hardware-related failures (85.9 %). The right side of figure 4 shows the distribution of the software-related events only. In most cases the software itself has caused the event (RS: 45.8 %).

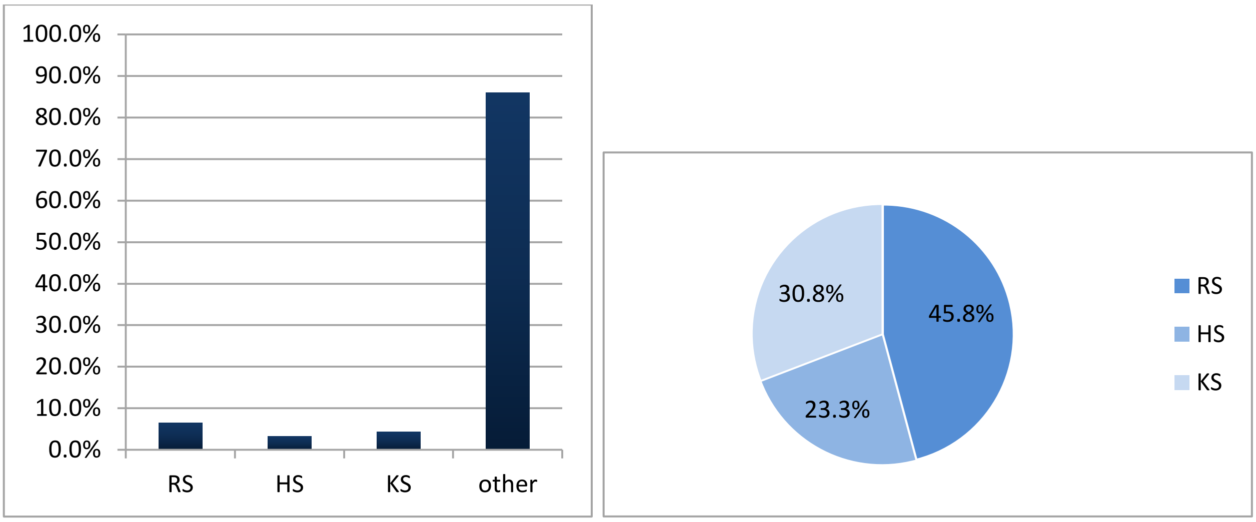


Figure 4: Events related to software compared to all events (left side) and compared to sum of RS, HS, and KS (right side)

Another focus of the GRS analysis was on environmental effects of digital, software-based components. This evaluation has shown no significant number of events. Within the observation period 13 events of measuring transmitters are recorded which were caused due to radiation. The affected measuring transmitters were in 4 cases for differential pressure measurement, in 4 cases for overpressure measurement, and in 5 cases for rotational speed and speed measurement. Two events are reported with lightning as cause. In one case, an analogue input module showed a failure of analog channels after a lightning strike. In another case, an ultrasonic flow transmitter showed a flow increase after a lightning strike. Only a few events were found with humidity (3) or heat (7) as cause of the event.

Thus, for the collected data it can be stated that environmental effects only have a minor impact on the functionality of digital, software-based components as installed in the regarded German NPPs.

4. New failure mechanisms

In a further step of the evaluation of the operating experience of digital, software-based components we have identified some new failure modes for these components. In the following, two of these failure modes are presented exemplarily.

Buffer battery: 1.6 % of all evaluated events were caused by buffer batteries in I&C components. We have identified some events in which failures with buffer batteries are the cause, for example:

- Loss of safety control system of the refuelling machine: Due to exhausted buffer batteries in the safety control system of the refuelling machine the program modules in the volatile memory of the central processing unit (CPU) of the safety control system got lost.
- Complete CPU program loss in the safety control system of the refuelling machine due to faulty buffer batteries
- CPU program loss due to loss of power supply for CPU buffering

Communication and system time: We have identified events in which communication between components failed or the component itself failed due to wrong time input, for example:

- Wrong data input when changing to daylight saving time
- Restart and/or new synchronisation to remove error

5. Software events fulfilling the incident reporting criteria of German authorities

In addition to the analysis of data collected in selected German NPPs, we have evaluated German events which fulfil the incident reporting criteria of German authorities. Here, we also found some events with software-related failures. In the following, two of these events are described shortly.

In one case, a digital, software-based neutron flux monitoring system caused an event. The behaviour of the medium-range channel was not in line with the specification. From 2001 to 2007, a repeated control rod insertion in the area of low, increasing reactor power (below 5 %) was observed. Due to the low reactor power the incident reporting criteria were not fulfilled. During test series in 2007, the relative neutron flux change rate showed an overshooting behaviour at low input signals. This behaviour is not allowed and therefore the incident reporting criteria were fulfilled. The cause for the overshooting behaviour was a programming error within the algorithm to calculate the relative neutron flux change rate.

In the other case, a digital, software-based module in the limitation system showed a temporary malfunction. A communication block in the affected module began emitting constant signals when the malfunction occurred and therefore the entire communication of the backplane bus in the cabinet was blocked. The assumed reason for the malfunction was an error in the adaption of the firmware when changing the fabrication method of the module from application-specific integrated circuit (ASIC) to field-programmable gate array (FPGA) technology.

Both described events show that an error in the software can lead to events that can have a negative impact on safety systems of NPPs.

6. Conclusion

Operational data from 6 different German NPPs, boiling water reactors (type 69 and type 72) as well as pressurized water reactors (Generation 2 up to Konvoi), were collected and evaluated.

It was shown that the current methods are suitable to detect failures in software-based components. Mostly, failures are detected during technical testing. Only a small number of failures led to a failure on demand. But if such failures on demand occur in a safety system they can have a major impact on plant safety. Thus, further evaluation of these events has to be performed to identify possibilities for improvement.

Further, the failure causes have been analyzed. It was found out that failures of software-based components were mainly caused by parts which are not related to the software.

In the analysis of the collected data it was shown that environmental effects (heat, humidity, radiation and lightning) only have a minor impact. It can be stated that the software-based components are able to run reliably under the environmental conditions which can be found in NPPs under normal operation.

In the analysis new failure mechanisms were identified. 1.6 % of all events were caused by buffer batteries, which led e.g. to losing the safety control system of the refuelling machine. In addition, failures in communication led to various problems with the communication between systems.

The examples of two software related events fulfilling the incident reporting criteria of German authorities show that programming errors can have a major impact on the system.

GRS

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

04.04.2014

Committee on the Safety of Nuclear Installations (CSNI) International Workshop on "ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs in the Light of Fukushima Daiichi Accident"

GRS

Outline

- Introduction
- Data collection
- Evaluation of operational data
  - System
  - Event detection
  - Events related to software
  - Environmental impacts
  - Selected software events in German NPPs fulfilling the incident reporting criteria of German authorities
  - New failure mechanisms
- Summary

2

Introduction (1/2)

- The components of I&C systems are often in use since their commissioning in the 1970ies / 1980ies
  - Components reach their end of lifetime
  - Procurement of spare parts is getting more and more difficult
  - → Further replacement of equipment is expected
- A replacement with identical components is not always possible or even not wanted
  - → Modern software-based components are applied
- Software-based components show specific characteristics differing from characteristics of analogue equipment
  - More complex structure
  - Additional properties
  - Changed failure mechanisms and failure behaviour
  - Changed man-machine interface

3

Introduction (2/2)

- Potential for new failure mechanisms and an increasing number of failure possibilities in modern I&C equipment due to use of software or programmable logic (e.g. FPGA)
- Concerning single failures
  - Higher reliability than analogue equipment due to additional self-testing and failure detection routines
- Concerning common cause failures (CCF)
  - Software-CCF may occur if latently existing programming errors are triggered by a certain, randomly arising system status or combination of parameters
  - Possibility of manipulation of software-based equipment by malware has a remarkably contribution to the potential of CCF

→ Reliability of software-based and programmable equipment has to be investigated and assessed

4

GRS

Data collection (1/2)

- Selected German nuclear power plants
  - Boiling water reactor (BWR)
    - Type 69
    - Type 72
  - Pressurized water reactor (PWR)
    - Generation 2
    - Vor-Konvoi
    - Konvoi
- To improve statistics and to include failures in non-safety systems, events not fulfilling the incident reporting criteria of German authorities are also included in this evaluation
- Data recorded between 2000 and 2012

5

GRS

Data collection (2/2)

- Operational data of digital, software-based components used in I&C and electrical systems in NPPs in Germany
  - 1008 events
  - 6617 plant data (installed components)
  - Event data consist of
    - I&C systems: 38.5%
    - Electrical systems: 4.7%
    - Measuring transmitter: 56.8%

6

GRS

Evaluation of operational data (1/9)

- Evaluation of data

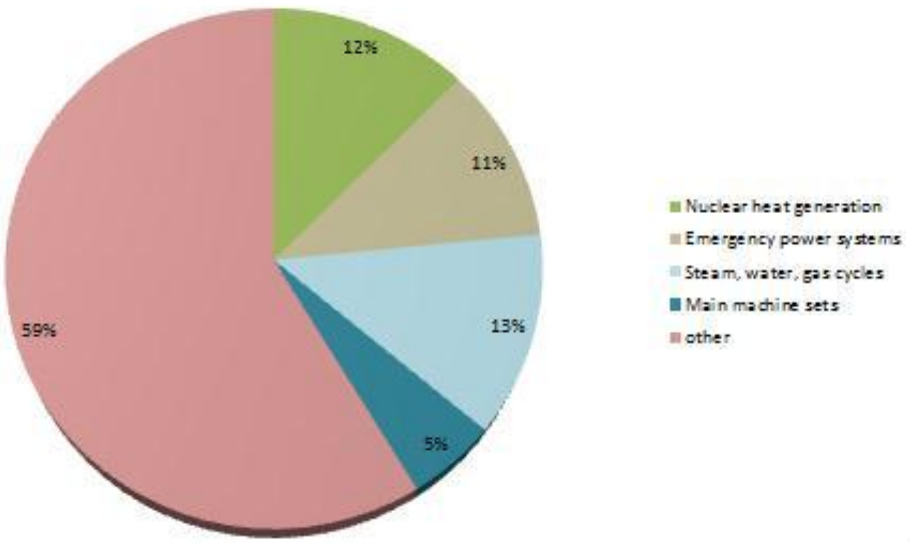
Focus:
- Affected process based system
- Failure detection method
- Relevance of software
- Relevance of environmental effects

7

GRS

Evaluation of operational data – System (2/9)

- BWR - affected process based systems

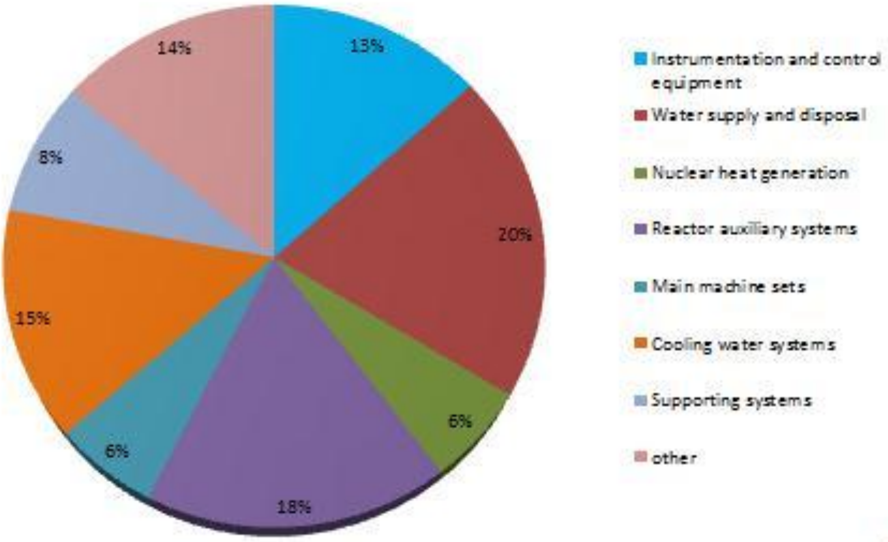


8

GRS

Evaluation of operational data – System (3/9)

- PWR - affected process based systems



9

GRS

Evaluation of operational data – Failure detection (4/9)

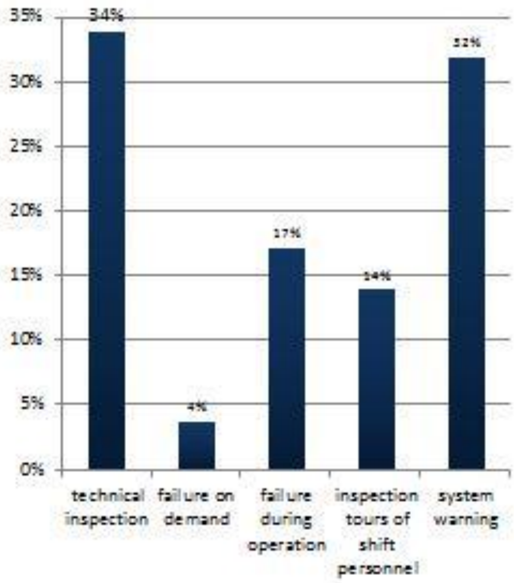
- Failure detection methods:
  - Technical inspection
    - Planned check of component
  - Failure on demand
    - Failure was not detected until component was requested
  - Failure during operation
    - Failure occurred while component was operating
  - Inspection tours of personnel
    - Failure was detected on planned tour of the personnel
  - System warning

10

GRS

Evaluation of operational data – Failure detection (5/9)

- Failure detection
  - Most failures found during technical inspection and by system warning
  - Small amount of failure on demand



11

GRS

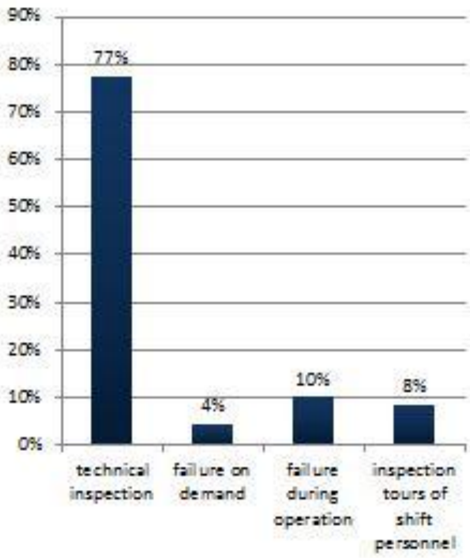
Evaluation of operational data – Failure detection (6/9)

- Failure detection of non-self-reporting events
  - Most failures found during technical inspection

  → Current detection methods suitable for event detection
  - Only few events with failure on demand

  However:
  - May have high relevance for plant safety

  → Further investigation necessary



12

Evaluation of operational data – Events related to software (7/9)

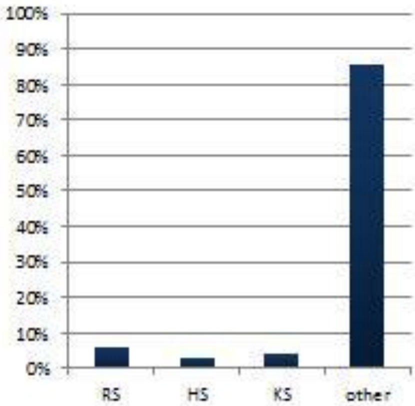
- Evaluation of the relevance of software for the events
  - Data were divided into hardware and software failures as cause of the event.
  - In order to identify possible new failure mechanisms in software-related events, these events were classified into three groups:
    - RS: Software causing event (e.g. programming errors)
    - HS: Hardware error causing software failure (e.g. buffer battery)
    - KS: Component related to software (e.g. display)

13

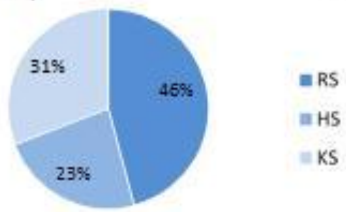
Evaluation of operational data – Events related to software (8/9)

- compared to all events
  - RS: 6 %
  - HS: 3 %
  - KS: 4 %

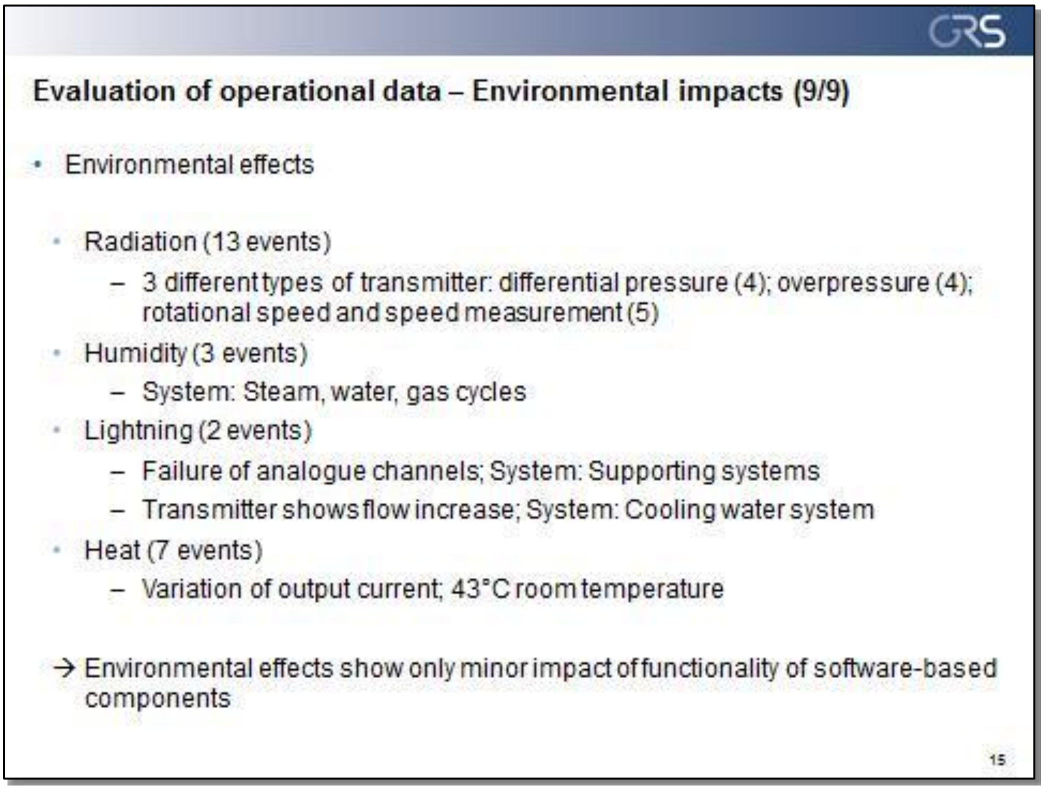
  → Most events are caused by hardware related failures

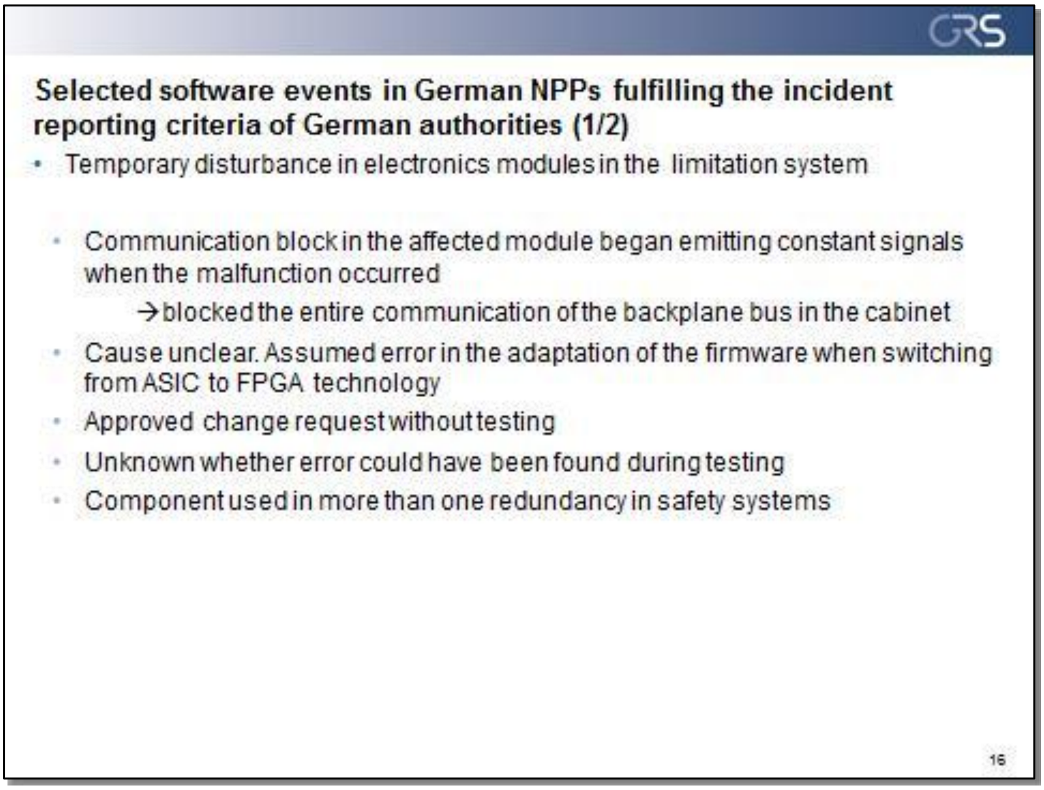


- compared to sum (RS,HS,KS)
  - RS: 46 %
  - HS: 23 %
  - KS: 31 %



14


GRS
Evaluation of operational data – Environmental impacts (9/9)
• Environmental effects
• Radiation (13 events)
– 3 different types of transmitter: differential pressure (4); overpressure (4); rotational speed and speed measurement (5)
• Humidity (3 events)
– System: Steam, water, gas cycles
• Lightning (2 events)
– Failure of analogue channels; System: Supporting systems
– Transmitter shows flow increase; System: Cooling water system
• Heat (7 events)
– Variation of output current; 43°C room temperature
→ Environmental effects show only minor impact of functionality of software-based components
15


GRS
Selected software events in German NPPs fulfilling the incident reporting criteria of German authorities (1/2)
• Temporary disturbance in electronics modules in the limitation system
• Communication block in the affected module began emitting constant signals when the malfunction occurred
→ blocked the entire communication of the backplane bus in the cabinet
• Cause unclear. Assumed error in the adaptation of the firmware when switching from ASIC to FPGA technology
• Approved change request without testing
• Unknown whether error could have been found during testing
• Component used in more than one redundancy in safety systems
16

Selected software events in German NPPs fulfilling the incident reporting criteria of German authorities (2/2)

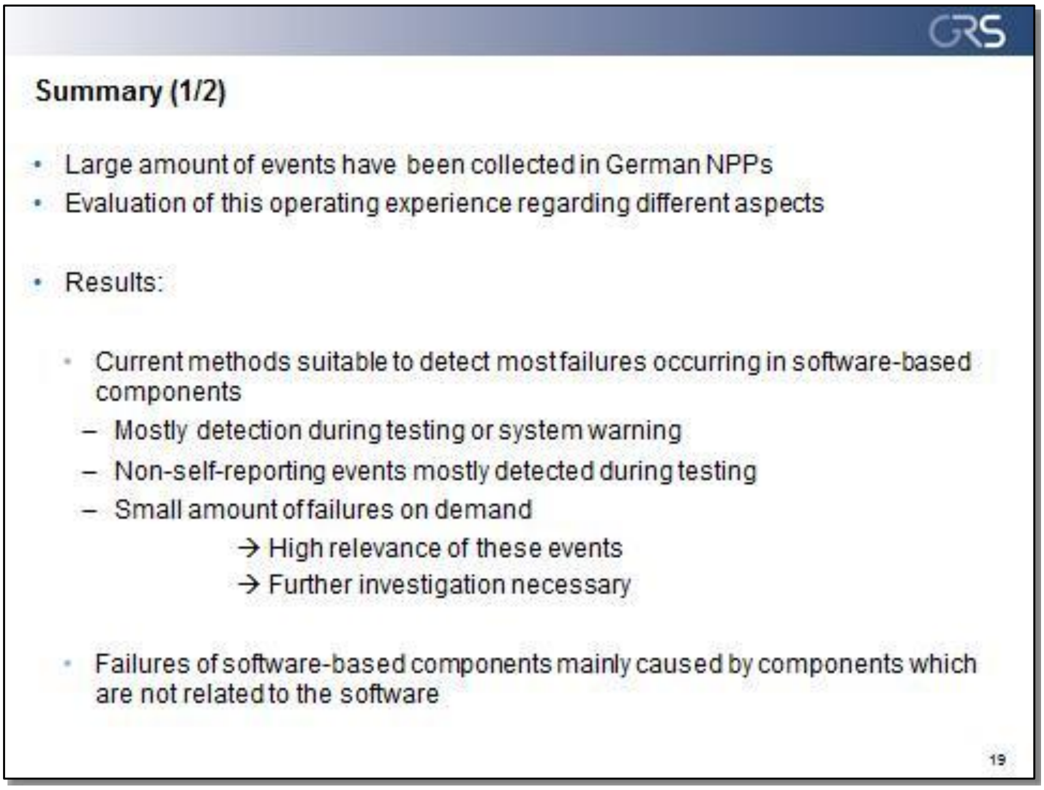
- Behaviour of a medium-range channel not in line with the specification (software-based neutron flux monitoring system)
  - Repeated control rod insertion in the area of low, increasing reactor power (below 5%)
  - Low input signal: relative neutron flux change rate showed overshoot
  - Cause: programming error within algorithm to calculate relative neutron flux change rate

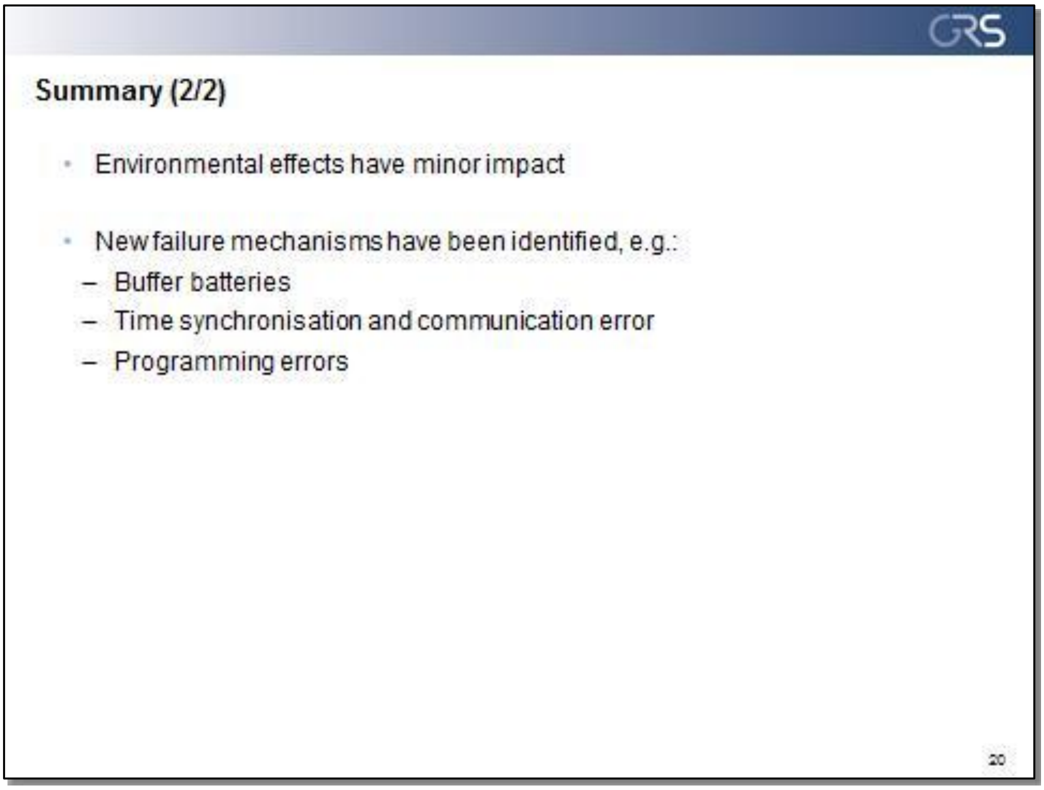
17

New failure mechanisms

- Evaluation of operating experience showed new failure modes
- Two new failure modes are presented exemplarily:
  - Buffer battery
    - Loss of safety control system of refuelling machine due to two empty buffer batteries
    - Surveillance of buffer batteries as a result of defects
    - CPU program loss: operations control error
    - CPU stops
    - 1.6% off all evaluated events
  - Communication problems
    - Wrong data input when changing to daylight saving time
    - Restart and/or new synchronisation to remove error

18


GRS
Summary (1/2)
• Large amount of events have been collected in German NPPs
• Evaluation of this operating experience regarding different aspects
• Results:
• Current methods suitable to detect most failures occurring in software-based components
– Mostly detection during testing or system warning
– Non-self-reporting events mostly detected during testing
– Small amount of failures on demand
→ High relevance of these events
→ Further investigation necessary
• Failures of software-based components mainly caused by components which are not related to the software
19


GRS
Summary (2/2)
• Environmental effects have minor impact
• New failure mechanisms have been identified, e.g.:
– Buffer batteries
– Time synchronisation and communication error
– Programming errors
20

GRS

Stefanie Blum

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Schwertnergasse 1
50667 Cologne
Germany

Phone: +49 (0) 221-20 68-724
E-Mail: Stefanie.Blum@grs.de

21

Office for
Nuclear Regulation

ONR Perspective on the Justification of "Smart" devices

Steve Frost
Principal Inspector
Office for Nuclear Regulation,
UK
steve.frost@hse.gsi.gov.uk

ONR Perspective on the Justification of SMART devices

- What are the issues?
- Common points for consideration.
- ONR perspective.
- Requirements for justification of SMART devices:
  - Class 1;
  - Class 2;
  - Class 3.
- Some examples of good practice.

Office for
Nuclear Regulation

What are the issues?

- Defining a "Smart" device:
  Smart devices contain a microprocessor(s) or other form of complex programmable electronic components that provide specific forms of functionality. Typical examples of smart devices for use in electrical applications can include protective relays, emergency diesel generator controllers and controllers associated with uninterruptible power supplies. See Note to IEC 61508-4:2010 sub-clause 3.2.12
- Inclusion of embedded digital technology using Smart devices appears to be a relentless commercial trend.
- Smart devices can provide increased functionality (signal processing, communications, diagnostics) **and complexity!!**
- Can introduce challenges in their use within nuclear safety applications? Justification is essential and can be achieved through equipment qualification.
- Increased risk of common cause failure.
- Can be considered as a type of pre-existing software
  - closer relationship to supplier(s);
  - difficulties in access to design documentation;
  - usually not nuclear-specific;
  - hidden changes.

Office for Nuclear Regulation

Common points for consideration (1)

- Clearly identify:
  make;
  model;
  application;
  software versions.
- Demonstrate fitness for purpose.
- Safety class – essential part of system – need to properly specify the properties required.
- Identify failure modes.
- Analyse common cause failure.

Office for Nuclear Regulation

Common points for consideration (2)

- Compare production to an applicable safety standard
  - address deficiencies by compensating activities or arguments:
    - manufacturer rework;
    - static and dynamic testing;
    - restrict functionality.
- Confidence building independent of the supplier:
  - commissioning tests;
  - static analysis;
  - analysis of operating experience;
  - statistical testing.

Office for Nuclear Regulation

Common points for consideration (3)

- For safety systems: same assessment of final product as for new software
  - may involve reverse engineering;
  - alternatively use additional compensating evidence.
- Document safe envelopes and limits for acceptable use
  - functionality;
  - maintenance;
  - environment.

Office for Nuclear Regulation

UK perspective: an evolution of the two-legged approach described in ONR guidance NS-TAST-GD-046 rev 3

Production Excellence

Compliance with IEC 61508 using EMPHASIS assessment tool

Manufacturer's type tests

Compensatory activities

Depends on gaps found in production excellence

Examples:
Review of CVs (by licensee)
Module tests (by manufacturer)
Statistical tests (by either)

Independent confidence building measures

Select from:

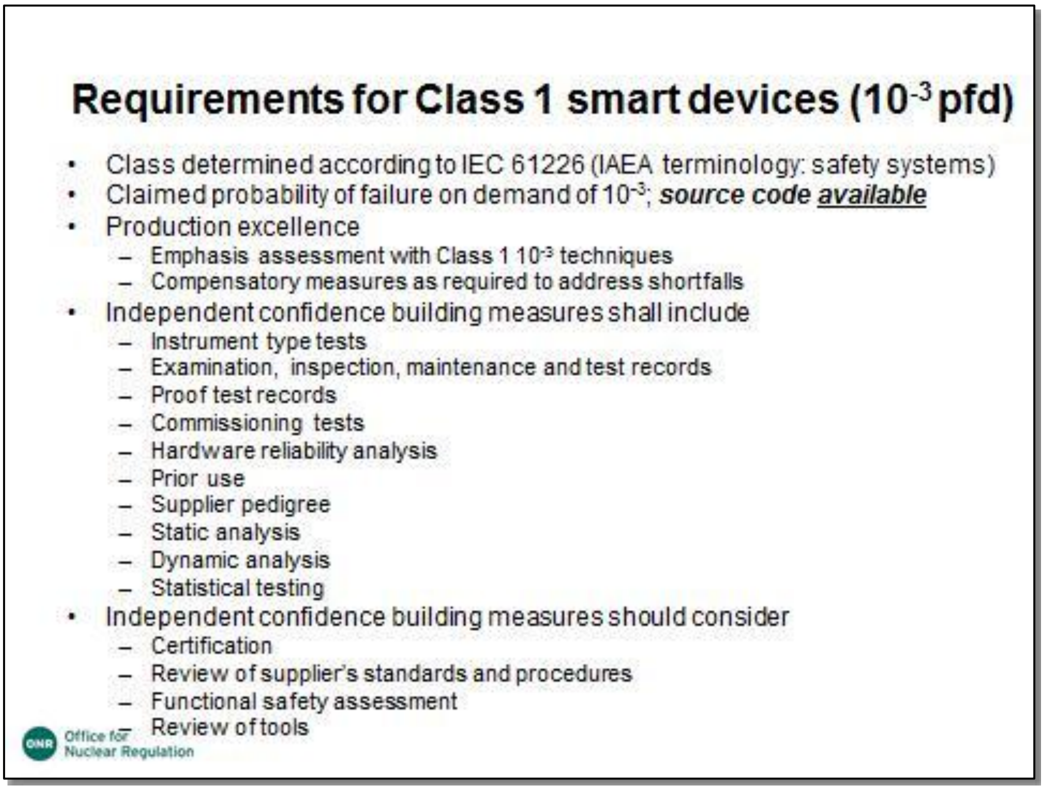
Examination, inspection, maintenance and test records
Proof test records
Commissioning tests
Hardware reliability analysis
Prior use
Certification
Supplier pedigree
Review of supplier's standards and procedures
Functional safety assessment
Review of tools
Static analysis
Dynamic analysis
Statistical testing

Office for Nuclear Regulation

Requirements for Class 1 smart devices (10^{-4} pfd)

- Class determined according to IEC 61226
  - IAEA terminology: safety systems
- Claimed probability of failure on demand of 10^{-4}
- Production excellence
  - Emphasis assessment with Class 1 10^{-4} techniques
  - Compensatory measures as required to address shortfalls
- Independent confidence building measures shall include
  - Instrument type tests
  - Examination, inspection, maintenance and test records
  - Proof test records
  - Commissioning tests
  - Hardware reliability analysis
  - Prior use
  - Supplier pedigree
  - Independent certification
  - Independent review of supplier's standards and procedures
  - Independent functional safety assessment
  - Independent review of tools
  - Static analysis
  - Dynamic analysis
  - Statistical testing

Office for Nuclear Regulation


Requirements for Class 1 smart devices (10-3 pfd)
• Class determined according to IEC 61226 (IAEA terminology: safety systems)
• Claimed probability of failure on demand of 10-3; source code available
• Production excellence
– Emphasis assessment with Class 1 10-3 techniques
– Compensatory measures as required to address shortfalls
• Independent confidence building measures shall include
– Instrument type tests
– Examination, inspection, maintenance and test records
– Proof test records
– Commissioning tests
– Hardware reliability analysis
– Prior use
– Supplier pedigree
– Static analysis
– Dynamic analysis
– Statistical testing
• Independent confidence building measures should consider
– Certification
– Review of supplier's standards and procedures
– Functional safety assessment
– Review of tools
Office for Nuclear Regulation


Requirements for Class 1 smart devices (10-3 pfd)
• Class determined according to IEC 61226 (IAEA terminology: safety systems)
• Claimed probability of failure on demand of 10-3; source code unavailable
• Production excellence
– Emphasis assessment with Class 1 10-3 techniques
– Compensatory measures as required to address shortfalls
• Independent confidence building measures shall include
– Instrument type tests
– Examination, inspection, maintenance and test records
– Proof test records
– Commissioning tests
– Hardware reliability analysis
– Prior use
– Supplier pedigree
– Statistical testing
• Independent confidence building measures should consider
– Certification
– Review of supplier's standards and procedures
– Functional safety assessment
– Review of tools
Office for Nuclear Regulation

Requirements for Class 2 smart devices (10^{-2} pfd)

- Class determined according to IEC 61226 (IAEA terminology: safety-related systems)
- Claimed probability of failure on demand of 10^{-2}
- Production excellence
  - Emphasis assessment with Class 2 techniques
  - Compensatory measures as required to address shortfalls
- Independent confidence building measures shall include
  - Instrument type tests
  - Examination, inspection, maintenance and test records
  - Proof test records
  - Commissioning tests
  - Hardware reliability analysis
  - Prior use
  - Supplier pedigree
- Independent confidence building measures should consider
  - Dynamic analysis
  - Static analysis
  - Statistical testing
  - Certification
  - Review of supplier's standards and procedures
  - Functional safety assessment
  - Review of tools

Office for Nuclear Regulation

Requirements for Class 3 smart devices (10^{-1} pfd)

- Class determined according to IEC 61226 (IAEA terminology: safety-related systems)
- Claimed probability of failure on demand 10^{-1} or less
- Production excellence
  - Demonstrated good commercial quality
  - Compensatory measures as required to address shortfalls
- Independent confidence building measures shall include
  - Examination, inspection, maintenance and test records
  - Commissioning tests
- Independent confidence building measures should consider
  - Prior use
  - Supplier pedigree

Office for Nuclear Regulation

Some examples of good practice

- Limited operational experience of Smart devices in electrical applications within UK's operational nuclear power plants, exception is recent introduction of VFCs in gas circulator control.
- Licensee generic pre-qualification of a range of microprocessor-based electrical protective relays at Class 3 – work currently in-hand to extend to specific relay types at Class 2.
- ONR's Generic Design Assessment of UKEPR has highlighted need for use of the approach described to other electrical applications, e.g. EDG control.
- Recent work in UK has also focussed on security of computer-based systems important to safety (CBSIS).
- Being considered within standards and guidance, e.g. ONR NS-TAST-GD-046 rev 3, IAEA NS-G-1.1 & NS-G-1.3.

Office for Nuclear Regulation

Thank you…

…..Any questions?

Office for Nuclear Regulation

Mass Alarms in Main Control Room Caused Condensate on the Instrumentation and Control Cards in Turbine Building

Cheol-Soo Goo
Korea Institute of Nuclear Safety, Korea

Abstract

A bunch of alarms and trouble lights on the main control room simultaneously turned on during inspection and exchange of the coolers of the turbine building at pressurized water reactor of the Hanbit nuclear power plant No. 6. The main cause was condensate on instrumentation cards of plant control system (PCS) installed at enclosures in the turbine building which have mux cabinets to transmit signals between the main control room and local equipment. To control the temperature and humidity of the MUX cabinets, two coolers of the plant chilled water system supply air to the compact enclosures at turbine building where temperature and humidity is high in the summer.

It is an unusual experience that mass alarms abnormally were occurred in the main control room during normal plant operation phases. Spurious signals with unknown cause at control and instrumentation system occasionally may have an unnecessary actuation of monitoring equipment and a plant scram even. One of the main causes is humidity by a rapid temperature change of the control and instrumentation cards. Dew on the instrumentation cards could form an abnormal short circuit in printed circuit board with the compact circuits and make any malfunction of the related system. Instrumentation and control cards with integrated circuits are vulnerable to high humidity and temperature where the system is enclosed in a small housing or enclosure surrounding with hash environment such as a turbine building. It was found that there was no functional degradation of the safety systems and no outsides releases of radioactive materials by this occurrence.

1. Introduction

Hanbit units 5&6 are located on the shores of the Yellow Sea in the western part of Korea peninsula. The two-loop pressurized water reactors were manufactured by Doosan Heavy industries/Combustion Engineering Corporation. The reactor core is designed for a thermal output of 2,825 MWth. The turbine generator has a rated electrical output of 1,050 MWe, supplied by Doosan Heavy industry in Korea [1]. Figure 1 shows the layout of the unit 5&6 of Hanbit site.

At 13:28 on August 7, 2013, trouble lights and related alarms were raised simultaneously on the switch board of the main control room at unit 6 in Hanbit nuclear power plant site, operators have not been experienced such a large number of indications of an unexpected occurrence during normal operation since the unit commercial operation. Maintenance engineer stopped a cooler No.05 at turbine building for an inspection which is a three monthly checking of the coolers as to maintain integrity of plant chilled water cooling system before replacement of other chiller. Root cause of the alarm and indication was a rapid increase of humidity and temperature of the inside of enclosure at the turbine building. There are many instrumentation and control cards and modules of the plant control system (PCS) installed in the enclosure at which local equipment such as valves and pumps were operated signals from main control room through MUX cabinets of the PCS.

The PCS, illustrated in Figure 2, is designed to perform data acquisition and transfer function via communication data links to control most of the field components such as pumps, fans, valves, dampers and circuit breakers. The system is composed of the safety related and non-safety related cabinets that are installed to the printed circuit boards based on microprocessor. Safety related functions are provided by redundant trains of microprocessor based single loop controllers with direct connections to the field input/output instruments to control the components associated with Engineered Safety Feature Actuation system. Most of non-safety related components are controlled remotely over communication network which performs the signal transmission with the input/output boards and fiber optic cables through several interfaces from the controllers to the field sensors [2].

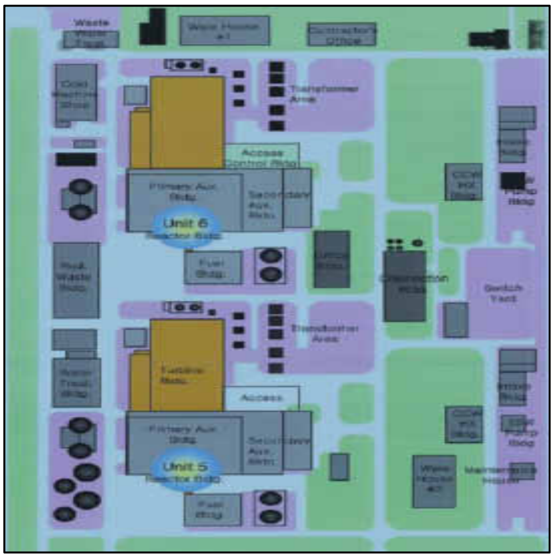


Figure 1. Hanbit 5&6 site layout

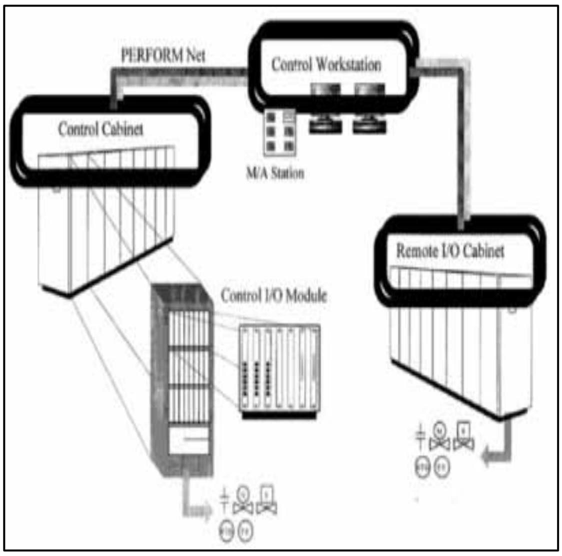


Figure 2. Configuration of the PCS

2. Overview of Event

2.1 Event Sequence

The turbine building chilled water system is designed to provide adequate quantity of chilled water at approximately 42 ˚F(6 ℃) to the turbine building area coolers, the high voltage distribution room air handling units, and area cooler cooling coil. The turbine building chilled water system consists of two 100% capacity chiller with its corresponding chilled water circulating pump, an air separator, a compression tank, a chemical additive tank, associated piping, controls and instrumentation. During normal operation, one of two chillers is operating and the other is on standby. Air separator and compression tank are provided to accommodate trapped air, and accommodate system expansion and contraction due to temperature variation in the system. The turbine building chillers condensers are cooled by the turbine building closed cooling water system [3].

The following sequence illustrates the situation at that time.
Event sequence (August 7, 2013)
13:20 Perform the test procedure of inservice surveillance-3632 in the plant chilled water system, cooler No.5 was stopped in the turbine building.
13:28 Alarm occurred “PCS MUX 16 Humidity Hi”
13:31 Alarm occurred “PCS MUX 13 Humidity Hi”

13:28 ~ 13:35 A bunch of alarms and indicators turned on simultaneously on the switch boards in main control room.
13:40 Immediately start of cooler No.4 immediately at the turbine building.
13:46 Alarm reset “PCS MUX 13 Humidity Hi”
13:52 Alarm reset “PCS MUX 16 Humidity Hi”
13:46 ~ 14:00 Control switch trouble reset in the mail control room.

2.2 Cause and Analysis of Event

There are eight cabinets of PCS MUX in the turbine building which are installed in the separate five enclosures scattered in several locations in the building. Two chillers supply cooled water to the coolers and air handling units (AHU) for the cooling of the major equipment of PCS MUX cabinets, main feed water pump turbine control panel and exciter. Table 1 shows the cooling air supply facility and the major loads in the turbine and generator building. Each four coolers were serving to the turbine generator building level 73´ and 100´ respectively where four cooler supply cooling air to the building of 73´ and 2 cooler and 2 AHU in 100´. Two chillers supply cooled water to the heat exchanger coils of the cooler and AHUs in the turbine generator building in which only one chiller operates and the other is on standby during summer. Figure 3 illustrate the layout and arrangement of the coolers and AHUs in the building.

Table 1. Cooling air supply facility and loads

Cooling air supply facility	Major loads
TGB 100´ Cubicle Cooler HV01	PCS MUX Cabinet 15/16
TGB 100´ Cubicle Cooler HV02	PCS MUX Cabinet 13 MFWP TBN Control Panel
TGB 73´ Cubicle Cooler HV03	PCS MUX Cabinet 11/12
TGB 73´ Cubicle Cooler HV04	PCS MUX Cabinet 09/10
TGB 73´ Cubicle Cooler HV05, HV06	
TGB SWGR Room Supply AHU HV08, HV09	PCS MUX Cabinet 14
TGB Supply AHU HV10, HV11	
Exciter Room Cubicle Cooler HV12	Exciter

For removing of the heat in the cabinet, cooler and AHU supply air to the enclosures through ducts and two additional air conditioners in the enclosure where one always operates in summer and the other is standby. According to the National Weather Service, the local temperature and humidity near the plant was 36.0 ℃ and 84.1 % respectively. PCS MUX Humidity alarms were occurred after 8 minutes of the chiller stopping to exchange with a standby chiller by manually. Normal replacement time is usually about 10 minutes, but the time was delayed 20 minutes at that time. The air in the turbine building with a high temperature and humidity rapidly permeated to the enclosure with a small space. The temperature and humidity increased to 6.1 ℃and 35 % in an enclosure contained PCS MUX 16 shown in Table 2.

Table 2. Variation of the temperature and humidity

Enclosure	Temperature [℃] ※ Alarm Set Point: 35	Humidity [%] ※ Alarm Set point: 75	Position
MUX 09/10	23.4 → 24.0 (Δ 0.6)	55.7 → 68.8 (Δ 13.1)	TGB 73'
MUX 11	27.1 → 27.5 (Δ 0.4)	59.4 → 63.3 (Δ 3.9)	TGB 73'
MUX 12	27.3 → 27.3 (Δ 0)	54.0 → 55.3 (Δ 1.3)	TGB 73'
MUX 13	24.0 → 27.8 (Δ 3.8)	60.2 → 83.3 (Δ 23.1)	TGB 100'
MUX 14	27.3 → 29.2 (Δ 1.9)	45.0 → 64.9 (Δ 19.9)	TGB 100'
MUX 15	23.2 → 27.5 (Δ 4.3)	65.8 → 67.9 (Δ 2.1)	TGB 100'

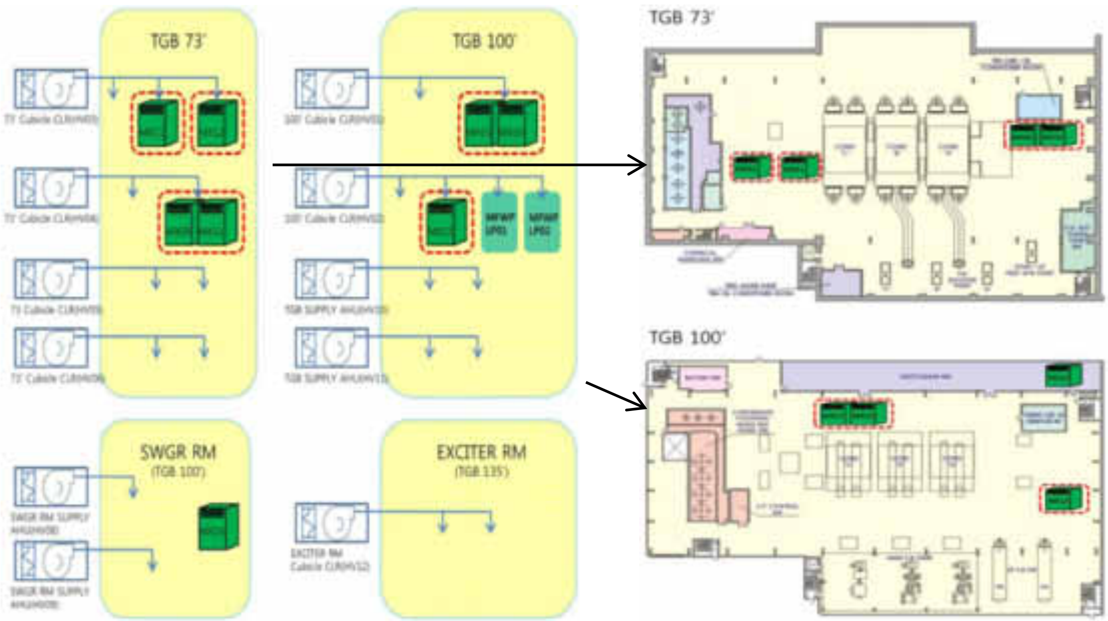


Figure 3. Cooler and Mux cabinet arrangement in the turbine and generator building

We can see a variation of temperature and humidity shown in figure 5 and 6 before and after the events in which humidity in enclosure increase rapidly than temperature and made condensation on the surface of cards in the MUX cabinets. Condensation water could be a circuit in the printed circuit board that may be a root cause of the alarms and indication in the main control room. Operating and maintenance manual describes a ground fault detection to detect ground failure that a power supply monitor contains three ground fault detection circuits. One circuit determines if catastrophic current leakage has occurred between control common and case ground. Similarly, the other circuits detect catastrophic current leakage from logic common and field common to case ground. Any current leakage between control common and case ground appears as a voltage across a resistor. No leakage yields a relative ground. Leakage of approximately 3.14 µA in either direction trips the window comparator sinking current to ground. As a result, the CONTROL POWER GND FAULT indicator lights on the front panel. And the window comparator energizes a solid state relay grounding the ground fault indication (GFI) line. The logic and field ground failure detection circuits operate in the same manner as the control ground-failure detection circuit. However, 7.5V biases the logic circuit. As a result, the window comparator limits are approximately ∓0.981 V and the current leakage limit is approximately 0.981 μA.

The three solid state relays that control the GFI line are wired in parallel. As a results, control, logic or field common leakage to case ground, grounds the GFI lines. The corresponding GND FAULT indicator lights on the front panel, to identify the faulty ground connection [2]. Figure 6, logic diagram, shows the process of the indication as a result of faults from the remote MUX cabinets, verifying an assumption that the root cause of the event is the condensation by rapid change of temperature and humidity in the enclosure. Leakage current through the bridge of water made a circuit to flow current over the ground fault limit.

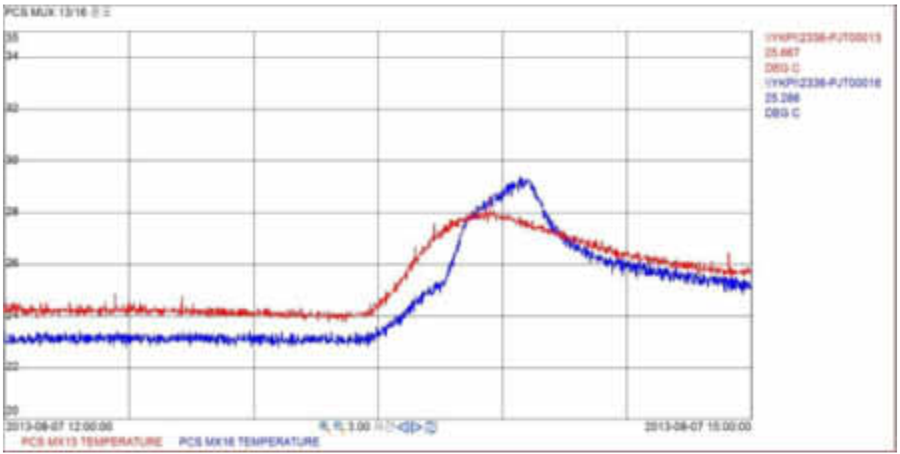


Figure 4. Temperature variation in the MUX 13(red) and 16

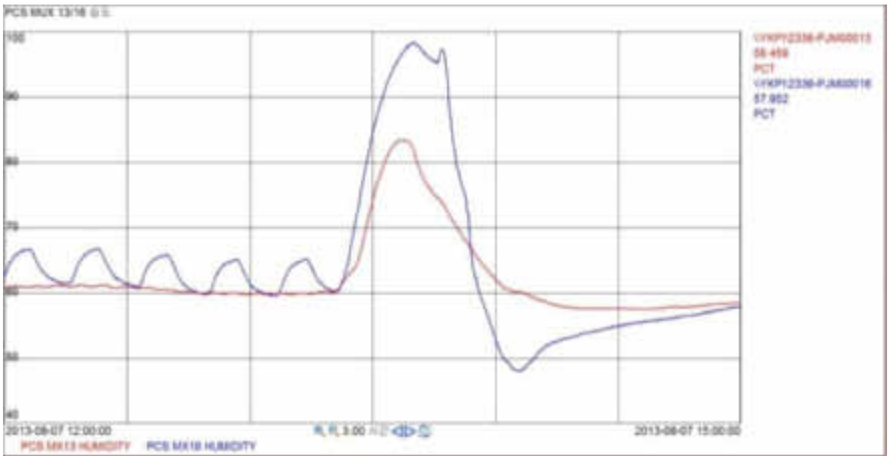


Figure 5. Humidity variation in the MUX 13(red) and 16

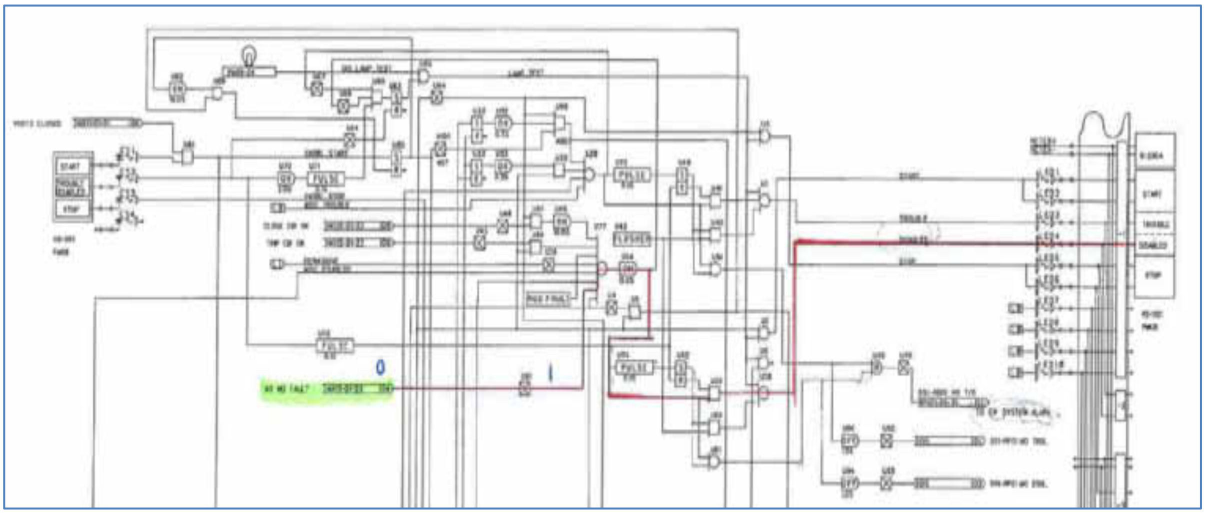


Figure 6. One of functional interconnection diagrams for fault indication

3. Corrective Actions

To prevent from reoccurrence of similar practices during plant normal operation, we have investigated the results and cause of the event and revised procedures related to the event such as a plant chilled water cooler checking that has been performed at three months intervals and adjusted a schedule of the cooler replacement to avoid a humidity increase in the MUX cabinets. Also it was recommended that staff involved into the maintenance and replacement should be trained about activities including cooler operation, replacement and emergency operation of two chiller failures.

4. Conclusion

The same operational activity can lead to a different result due to environment and times, making an unexpected event which will be a minor incident or severe accident in some cases that is depend on a plant and environmental condition. We need a consideration that cabinet located local area should be managed carefully in order to prevent a rapid change of temperature and humidity because of the control and instrumentation cards are vulnerable to the environment. Investigation of procedures and adjustment of in-service schedules can be useful to avoid unplanned scram, reducing an unexpected occurrence due to the instrumentation and control system failures.

5. References

[1] Final Safety Analysis Report of Hanbit Nuclear 5&6 units,
[2] Plant Control System Operating &Maintenance Manual, Korea Electric Power Corporation Hanbit Nuclear Power Plant Units 5 & 6
[3] Operational Experience Report of Hanbit Nuclear Power Plant No.6.
[4] Functional Interconnection Diagram, Rev. 3, Korea Hydro & Nuclear Power Co., LTD.

Mass Alarms in Main Control Room Caused Condensate on the Instrumentation and Control Cards in Turbine Building

April 4, 2014

KINS, Cheol-Soo Goo

1/14/2015 1

Contents

- Introduction
- Overview of Event
- Cause and Analysis of Event
- Corrective Actions
- Conclusion
- References

1/14/2015 2

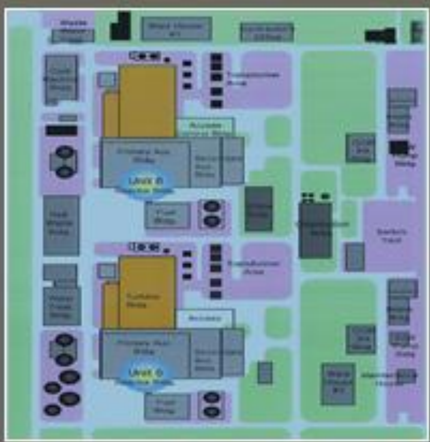
Introduction

- A bunch of alarms and trouble lights on the main control room simultaneously
- The main cause was condensate on instrumentation cards of plant control system (PCS)
- No functional degradation of the safety systems and no outsides releases of radioactive materials by this occurrence

1/14/2015 3

Introduction

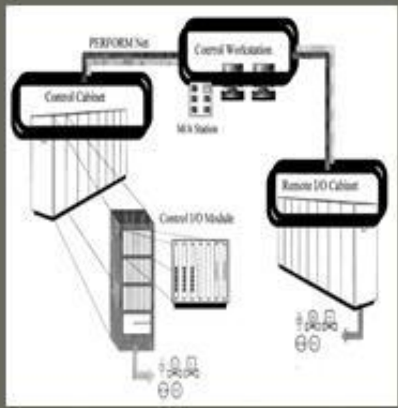
- Hanbit units 5&6 is two-loop pressurized water reactors
- Thermal output of 2,825 MWth
- The turbine generator has a rated electrical output of 1,050 MWe



1/14/2015 4

Introduction

- The PCS is designed to perform data acquisition and transfer function
- Control most of the field components such as pumps, fans, valves, dampers and circuit breakers
- Composed of the safety related and non-safety related cabinets
- Controlled remotely over communication network



1/14/2015

5

Overview of Event

- **Adequate quantity of chilled water at approximately 42°F(6°C)**
  - Turbine building area coolers
  - High voltage distribution room air handling units
  - Area cooler cooling coil
- **Two 100% capacity chiller**
  - One is operating and
  - The other is on standby

1/14/2015

6

Overview of Event

13:20 Perform the test procedure of inservice surveillance-3632 in the plant chilled water system, cooler No.5 was stopped in the turbine building.

13:28 Alarm occurred "PCS MUX 16 Humidity Hi"

13:31 Alarm occurred "PCS MUX 13 Humidity Hi"

13:28 ~ 13:35 A bunch of alarms and indicators turned on simultaneously on the switch boards in main control room.

13:40 Immediately start of cooler No.4 at the turbine building.

13:46 Alarm reset "PCS MUX 13 Humidity Hi"

13:52 Alarm reset "PCS MUX 16 Humidity Hi"

13:46 ~ 14:00 Control switch trouble reset in the main control room.

1/14/2015 7

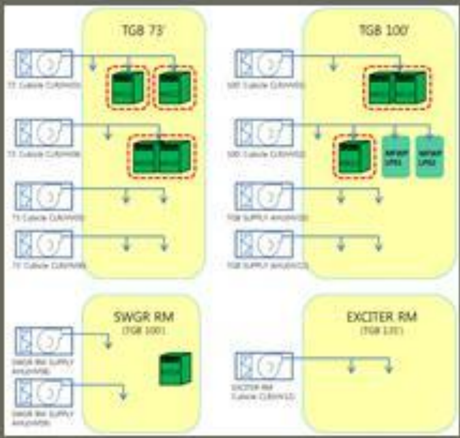
Cause and Analysis of Event

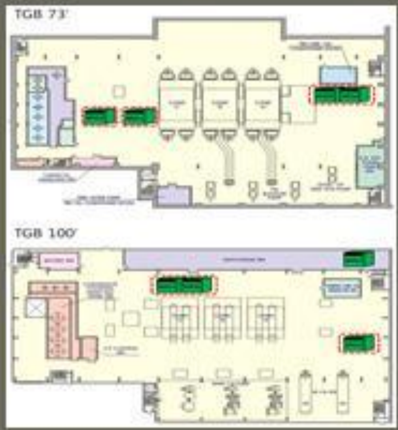
- Eight cabinets of PCS MUX in the turbine building
- Two chillers supply cooled water to the coolers and air handling units (AHU)

Cooling air supply facility	Major loads
TGB 100' Cubicle Cooler HV01	PCS MUX Cabinet 15/16
TGB 100' Cubicle Cooler HV02	PCS MUX Cabinet 13 MFWP TBN Control Panel
TGB 73' Cubicle Cooler HV03	PCS MUX Cabinet 11/12
TGB 73' Cubicle Cooler HV04	PCS MUX Cabinet 09/10
TGB 73' Cubicle Cooler HV05, HV06	
TGB SWGR Room Supply AHU HV08, HV09	PCS MUX Cabinet 14
TGB Supply AHU HV10, HV11	
Exciter Room Cubicle Cooler HV12	Exciter

1/14/2015 8

Cause and Analysis of Event





1/14/2015 9

Cause and Analysis of Event

- Local temperature and humidity near the plant was 36.0℃ and 84.1% respectively
- Normal replacement time is usually about 10 minutes, but the time was delayed 20 minutes at that time.
- The air in the turbine building with a high temperature and humidity rapidly permeated to the enclosure.
- The temperature and humidity increased to 6.1℃and 35% in an enclosure contained PCS MUX 16 shown in Table 2.

1/14/2015 10

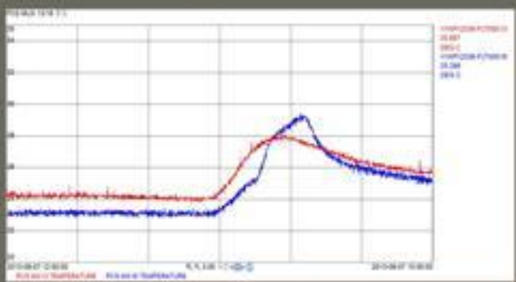
Cause and Analysis of Event

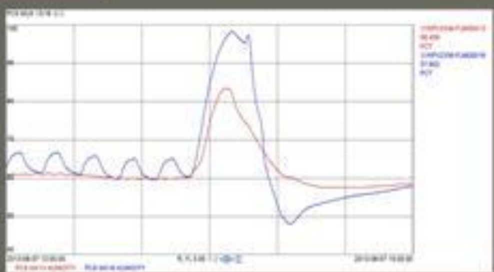
Enclosure	Temperature [℃] ※ Alarm Set Point: 35	Humidity [%] ※ Alarm Set point: 75	Position
MUX 09/10	23.4 → 24.0 (Δ 0.6)	55.7 → 68.8 (Δ 13.1)	TGB 73'
MUX 11	27.1 → 27.5 (Δ 0.4)	59.4 → 63.3 (Δ 3.9)	TGB 73'
MUX 12	27.3 → 27.3 (Δ 0.0)	54.0 → 55.3 (Δ 1.3)	TGB 73'
MUX 13	24.0 → 27.8 (Δ 3.8)	60.2 → 83.3 (Δ 23.1)	TGB 100'
MUX 14	27.3 → 29.2 (Δ 1.9)	45.0 → 64.9 (Δ 19.9)	TGB 100'
MUX 15	23.2 → 27.5 (Δ 4.3)	65.8 → 67.9 (Δ 2.1)	TGB 100'
MUX 16	23.0 → 29.1 (Δ 6.1)	63.1 → 98.1 (Δ 35.0)	TGB 100'

1/14/2015

11

Cause and Analysis of Event





1/14/2015

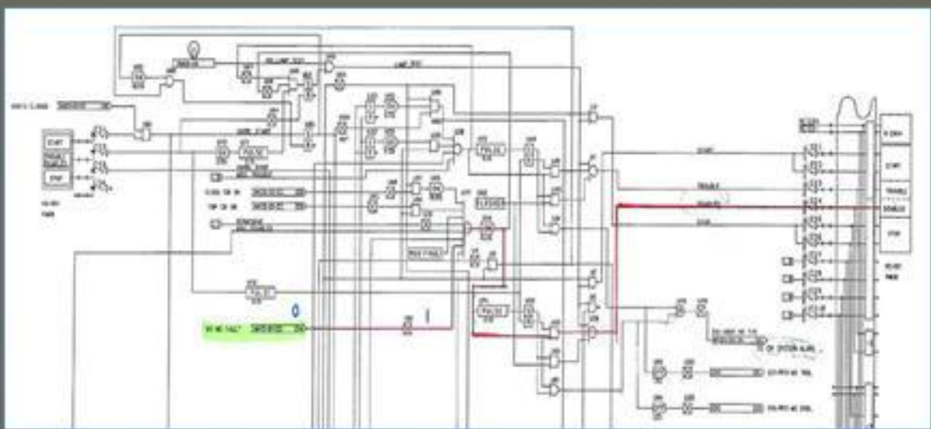
12

Cause and Analysis of Event

- Humidity in enclosure increase rapidly than temperature
- Made condensation on the surface of cards in the MUX cabinets.
- Condensation water could be a circuit in the printed circuit board
- Leakage of approximately 3.14 μA in either direction trips the window comparator sinking current to ground
- The logic and field ground failure detection circuits operate in the same manner
- Current leakage limit is approximately 0.981 μA.

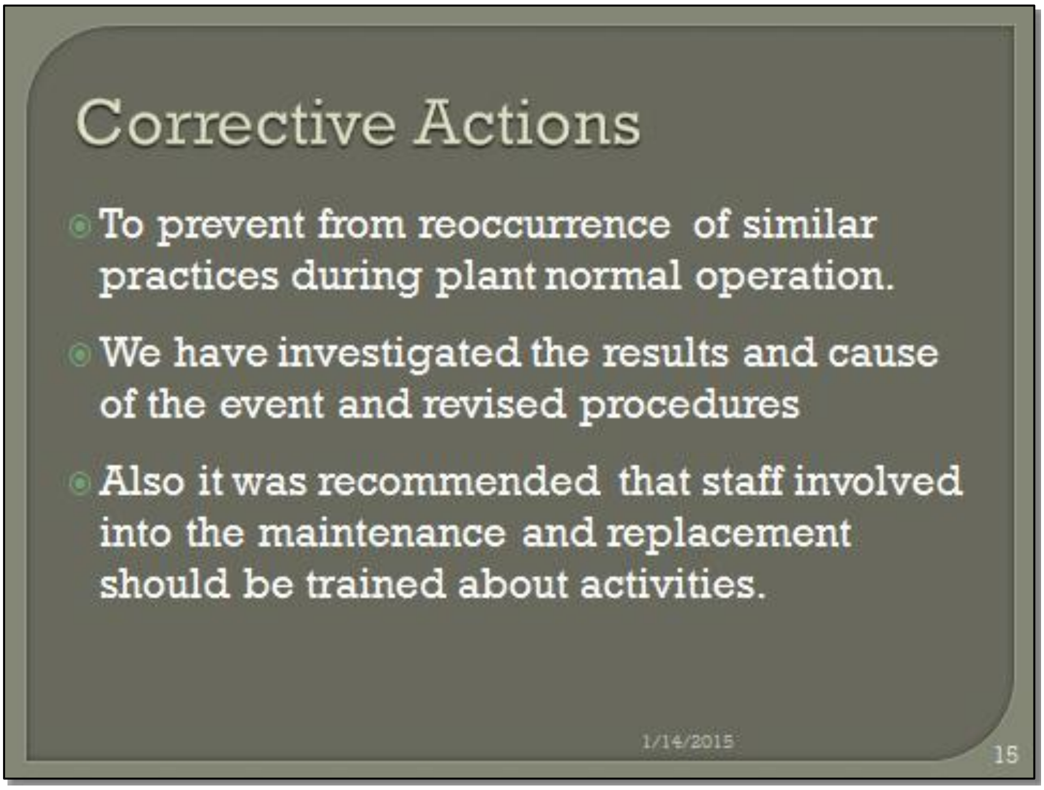
1/14/2015 13

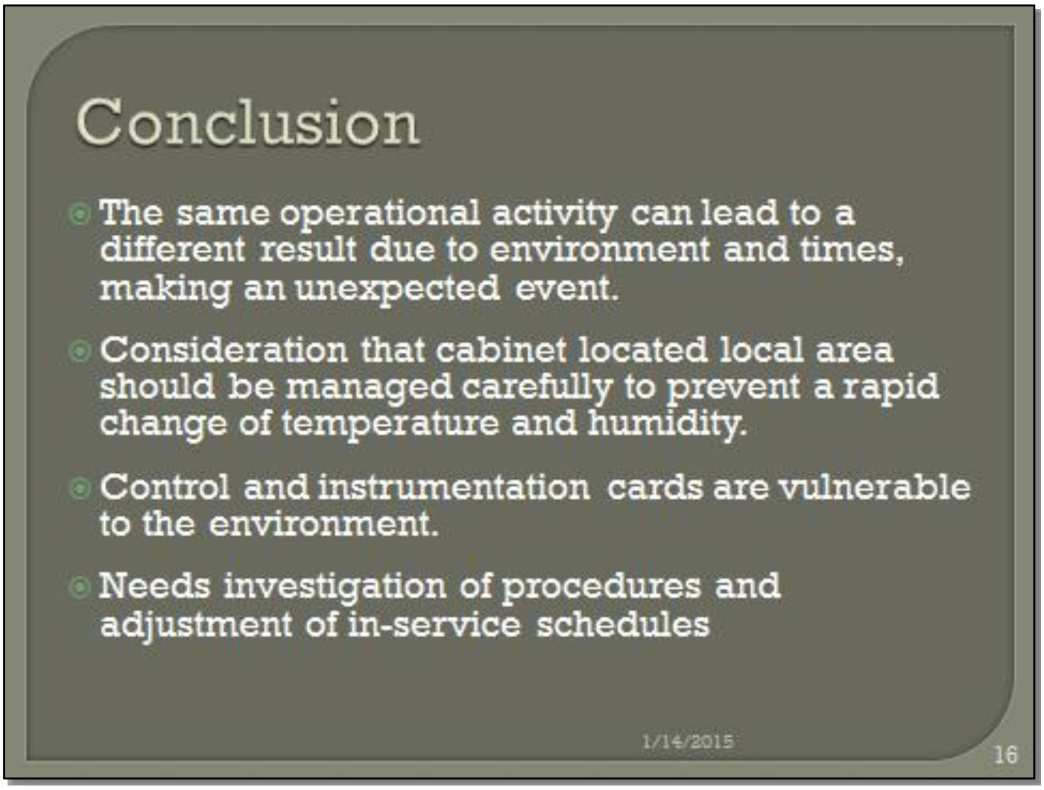
Cause and Analysis of Event

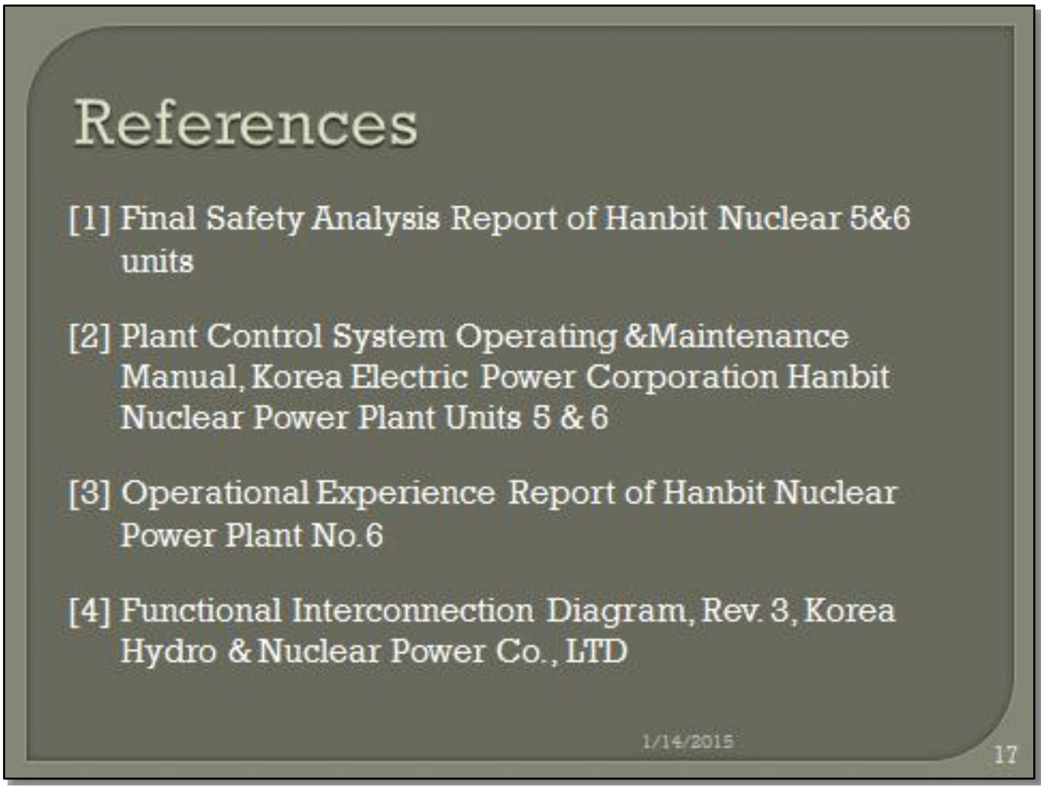


One of functional interconnection diagrams for fault indication

1/14/2015 14


Corrective Actions
To prevent from reoccurrence of similar practices during plant normal operation.
We have investigated the results and cause of the event and revised procedures
Also it was recommended that staff involved into the maintenance and replacement should be trained about activities.
1/14/2015
15


Conclusion
The same operational activity can lead to a different result due to environment and times, making an unexpected event.
Consideration that cabinet located local area should be managed carefully to prevent a rapid change of temperature and humidity.
Control and instrumentation cards are vulnerable to the environment.
Needs investigation of procedures and adjustment of in-service schedules
1/14/2015
16


References
[1] Final Safety Analysis Report of Hanbit Nuclear 5&6 units
[2] Plant Control System Operating &Maintenance Manual, Korea Electric Power Corporation Hanbit Nuclear Power Plant Units 5 & 6
[3] Operational Experience Report of Hanbit Nuclear Power Plant No.6
[4] Functional Interconnection Diagram, Rev. 3, Korea Hydro & Nuclear Power Co., LTD
1/14/2015
17

OTHERS

"Related Activities at CSNI/WGRISK"

Probabilistic Safety Assessment Relating to the Loss of Electrical Sources
Jeanne-Marie Lanore (IRSN, France)

AEN NEA Agence pour l'énergie nucléaire Nuclear Energy Agency OECD

WGRISK Task 2013-1

Insights provided by Probabilistic Safety Assessment relating to the loss of electrical sources

Presented by Jeanne-Marie Lanore IRSN
WGRISK vice-Chair

ROBELSYS Workshop - 1-4 April 2014 IRSN

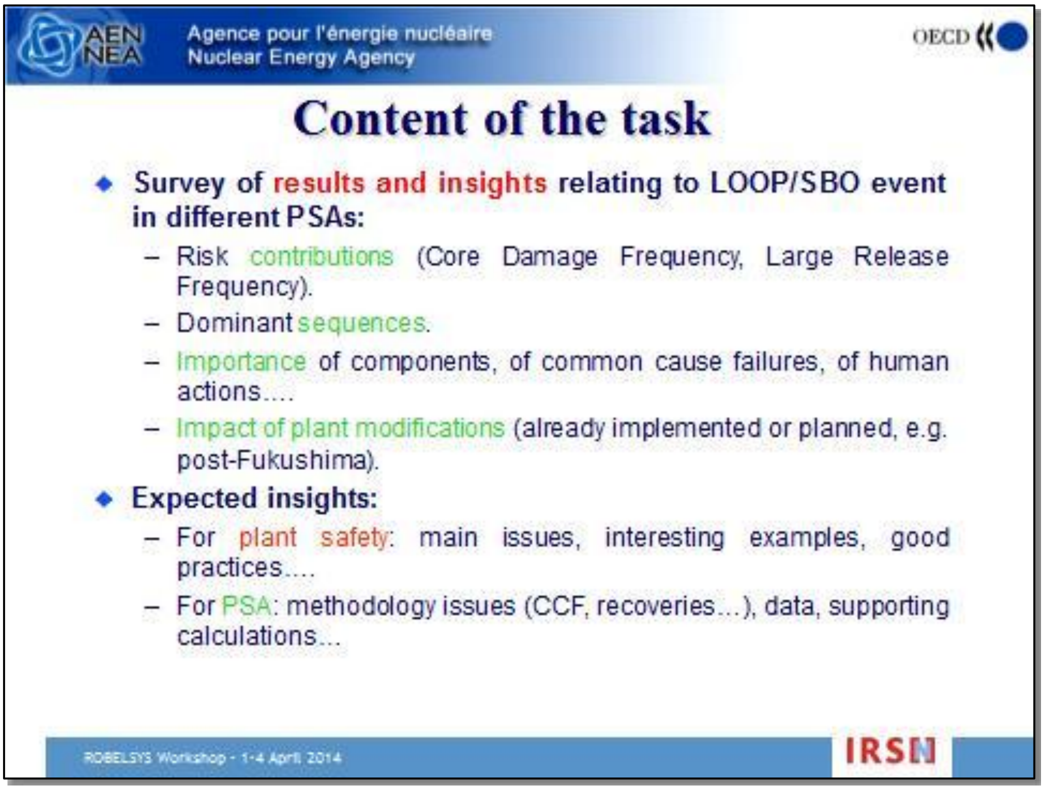
AEN NEA Agence pour l'énergie nucléaire Nuclear Energy Agency OECD

Background

- The loss of electrical sources is generally an important contributor to the risk related to nuclear plants. In particular the External Hazards initiating events lead generally to a loss of electrical sources. This importance was underscored by the Fukushima accident.
- A strength of PSA is to provide insights not only into the causes of the event but also into the potential consequences for the plant and the provisions aiming to limit these consequences (core damage prevention, large release prevention and mitigation) with the corresponding risk impact. PSA could provide a measure of Defence-in-Depth in case of loss of a safety function.

ROBELSYS Workshop - 1-4 April 2014 IRSN


AEN NEA
Agence pour l'énergie nucléaire
Nuclear Energy Agency
OECD
General objectives
The task intends to illustrate the PSA capabilities with outstanding practical examples.
The task will rely on a survey of existing PSAs.
It will provide a complementary view for ROBELSYS task.
Loss of External sources
SBO
Core Damage
Releases
ROBELSYS
PSA
ROBELSYS Workshop - 1-4 April 2014
IRSN


AEN NEA
Agence pour l'énergie nucléaire
Nuclear Energy Agency
OECD
Content of the task
Survey of results and insights relating to LOOP/SBO event in different PSAs:
– Risk contributions (Core Damage Frequency, Large Release Frequency).
– Dominant sequences.
– Importance of components, of common cause failures, of human actions….
– Impact of plant modifications (already implemented or planned, e.g. post-Fukushima).
Expected insights:
– For plant safety: main issues, interesting examples, good practices….
– For PSA: methodology issues (CCF, recoveries…), data, supporting calculations…
ROBELSYS Workshop - 1-4 April 2014
IRSN


AEN NEA
Agence pour l'énergie nucléaire
Nuclear Energy Agency
OECD
Status of the task
June 2013: CAPS (2013-1) approved by CSNI
June-November 2013: Questionnaire prepared by a core group .
– Canada, Czech Republic, France (IRSN task leader), Germany, Hungary, India, Italy, Mexico, Sweden, Taïwan.
December 2013: questionnaire sent to WGRISK members (including 5 examples of answer)
December 2014: draft report
June 2015: report submitted to PRG and CSNI
June 2014: responses collected and analysed
ROBELSYS Workshop - 1-4 April 2014
IRSN

APPENDIX 3

LIST OF PARTICIPANTS

ALGERIA

Dr Rabah BENABID

ARGENTINA

Mr Hector Gustavo CASSINI	Invap S.E., Bariloche
Mr Fernando GUTIERREZ	Invap S.E., Bariloche

BELGIUM

Mr Patrick BRUGGEMAN	Electrabel, Brussels
Dr Ouahab FOUATHIA	BelV
Mr Xavier GUISEZ	Electrabel, Brussels
Mr Robert LAUWERS	Electrabel, Brussels
Mr André VANDEWALLE	Nuclear Safety Support Services (NSSS)
Mr Jolan WILLEMS	Electrabel, Brussels

CANADA

Ms Jasmina VUCETIC	Canadian Nuclear Safety Commission

CZECH REPUBLIC

Mr Marek TENGLER

FINLAND

Mr Samuli HANKIVUO	Finnish Centre for Radiation and Nuclear Safety
Mr Ari KANERVA	Fortum Nuclear Services Ltd, Espoo

FRANCE

Mr Cedric BAYLE	EATP
Mrs Carine DELAFOND	Institut de Radioprotection et de Sûreté Nucléaire
Mrs Pauline DESCHRYVER	Institut de Radioprotection et de Sûreté Nucléaire
Mr Alexandre DUBOIS	Institut de Radioprotection et de Sûreté Nucléaire
Mrs Patricia DUPUY	Institut de Radioprotection et de Sûreté Nucléaire
Mr Jean-Michel HAURE	Electricite de France-SEPTEN, Villeurbanne

Mrs Jeanne-Marie LANORE	Institut de Radioprotection et de Sûreté Nucléaire
Mrs Caroline LAVARENNE	Institut de Radioprotection et de Sûreté Nucléaire
Mr Florent RAISON	AEG Power Solutions
Mr Pascal REGNIER	Institut de Radioprotection et de Sûreté Nucléaire
Mr Jacques REPUSSARD	Institut de Radioprotection et de Sûreté Nucléaire
Mr Thierry-Victorin RICHARD	Electricité de France-SEPTEN

GERMANY

Ms Stefanie BLUM	Gesellschaft für Anlagen- und Reaktorsicherheit mbH
Mr Lutz FÖLLNER	TÜV Süd Energietechnik GmbH BW
Mr Waldemar GEISSLER	AREVA NP
Dr Jimmy LORANGE	AREVA NP
Mr Sebastian A. MEISS	Federal Office for Radiation Protection
Mr Oliver SOBOTT	AREVA NP GmbH
Mr Pascal VOGT	Gesellschaft für Anlagen- und Reaktorsicherheit mbH
Mr Ralf-Michael ZANDER	Rheinisch-Westfaelisches Elektrizitaetswerk AG

IRELAND

Mr Jerry WAUGH	
Mr Stephen WOODS	

ITALY

Dr Luciano BURGAZZI	ENEA

JAPAN

Mr Ken KAWAGUCHI	Nuclear Regulation Authority
Mr Shinji KAWANAGO	MHI Nuclear Engineering Co., Ltd.
Mr Masaru MOMIYAMA	Japan Nuclear Safety Institute
Mr Tsutomu NOMOTO	Mitsubishi Heavy Industries
Mr Masashi SUGIYAMA	Hitachi-GE Nuclear Energy, Ltd.
Mr Hideaki SADAKANE	JEPIC

KOREA (REPUBLIC OF)

Mr Cheol-Soo GOO	Korea Institute of Nuclear Safety
Mr Lee JAEDO	Korea Institute of Nuclear Safety
Mr Woo Sung JEONG	KEPCO Engineering & Construction Company
Mr Sang Hak KIM	KEPCO Engineering& Construction Company
Mr Cheoung-joon LEE	KEPCO Engineering & Construction Company

MEXICO

Mr Francisco LOPEZ	Comision Nacional de Seguridad Nuclear y Salvaguar

NETHERLANDS

Mr Marcel VAN BERLO	VROM - KFD

PAKISTAN

Mr Iftikhar AHMED	Pakistan Nuclear Regulatory Authority

SLOVAK REPUBLIC

Mr Miroslav MIKLOVIC	Vyskumny Ustav Jadrovych Elektrarni

SLOVENIA

Dr Andrija VOLKANOVSKI	Jozef Stefan Institute

SOUTH AFRICA

Mr Sobhuza TSHOBENI	National Nuclear Regulator

SPAIN

Mr Manuel Rodrigo MARTINEZ MORENO	Consejo de Seguridad Nuclear

SWEDEN

Mr Tomas ALBERTSSON	Vattenfall AB
Mr Gazwan ALGILANY	Swedish Radiation Safety Authority
Mr Pehr ANDERSSON	Forsmarks Kraftgrupp AB
Mr Johan BERG	Forsmarks Kraftgrupp AB
Mr Per BYSTEDT	PERBYS Konsult
Mr Hans EDVINSSON	Vattenfall AB
Mr Tage ERIKSSON	Swedish Radiation Safety Authority
Mr Örjan ERIKSSON	EnerSys AB
Mr Peter FREDRIKSSON	Forsmarks Kraftgrupp AB
Mr Parviz GHASEMI	Swedish Radiation Safety Authority
Mr Fredrik HEYMAN	OKG Aktiebolag
Mr Roland JÄGERSTÅHL	Forsmarks Kraftgrupp AB
Mr Tomas JELINEK	Swedish Radiation Safety Authority
Ms Sofia JOHANSSON	Ringhals AB
Mr Salah KANAAN	OKG AB/EON
Dr Daniel KARLSSON	Gothia Power AB
Mr Johnny Mattias KARLSSON	Swedish Radiation Safety Authority
Mr Magnus KNUTSSON	Ringhals AB
Mr Per LAMELL	Forsmarks Kraftgrupp AB
Mr Magnus LENASSON	SOLVINA
Ms Anna Maja LUNDBÄCK	Swedish Radiation Safety Authority
Mrs Raija OINAS	Forsmarks Kraftgrupp AB
Mr Amer OMANOVIC	SOLVINA
Mr Tommi TALONEN	Westinghouse
Mr Mikael TOLLMAN	Forsmarks Kraftgrupp AB
Mr Igor TRISIC	OKG AB/EON

SWITZERLAND

Mr Franz ALTKIND	Swiss Federal Nuclear Safety Inspectorate
Mr Gert ANDERSEN	GUTOR Electronic LLC
Mr Gery BONDUELLE	Enersys
Mr Jörg LAASER	GUTOR Electronic LLC
Mr Daniel SCHMID	Swiss Federal Nuclear Safety Inspectorate

TURKEY

Mr Ertugrul AKBULUT	TAEK
Mr Mahmut DOGAN	TAEK

UNITED ARAB EMIRATES

Mr Mohammed ALSHERAIFI	Federal Authority for Nuclear Regulation
Mr Slawomir ROKITA	Federal Authority for Nuclear Regulation

UNITED KINGDOM

Mr Thomas Brough DAVIES	Magnox Limited
Ms Rebecca DUNN	Magnox Limited
Mr Steve FROST	Office for Nuclear Regulation
Mr Takafumi IHARA	TEPCO
Mr Kevin PEPPER	Office for Nuclear Regulation
Mr John REILLY	EDF Energy
Mr Gary WALKER	EDF Energy
Mr Simon WHITE	EDF Energy

UNITED STATES OF AMERICA

Dr John BICKEL	Evergreen Safety & Reliability Technologies
Dr Allen Egon CHOLAKIAN	IRDF Project Harvard - Columbia
Mr Gary JOHNSON	
Mr Gurcharan MATHARU	United States Nuclear Regulatory Commission
Mr Roy MATHEW	United States Nuclear Regulatory Commission

INTERNATIONAL ORGANISATIONS

IAEA

Mr Alexander DUCHAC	International Atomic Energy Agency
Mr Thomas KOSHY	International Atomic Energy Agency

OECD/NEA

Mr Toshiyuki KOGANEYA	OECD Nuclear Energy Agency
Mr Andrew WHITE	OECD Nuclear Energy Agency