Unclassified **NEA/CSNI/R(2009)10**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **09-Nov-2009**

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2009)10
Unclassified

Cancels & replaces the same document of 04 November 2009

Defence in Depth of Electrical Systems and Grid Interaction

Final DIDELSYS Task Group Report

The complete version is only available in PDF format.

JT03273860

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

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

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

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full member. NEA membership today consists of 28 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

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

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

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

FOREWORD

The July 2006 Forsmark-1 event identified a number of design deficiencies related to electrical power supply to systems and components important to safety in nuclear power plants. While plant-specific design features at Forsmark-1 contributed to the severity of the sequence of events which occurred at Forsmark, a number of the design issues are of a generic nature as they relate to commonly used approaches, assumptions, and design standards for voltage protection of safety related equipment.

The NEA Committee on the Safety of Nuclear Installations (CSNI) authorised formation of a task group in January 2008 to examine Defence in Depth of Electrical Systems and Grid Interaction with nuclear power plants (DIDELSYS). The task was defined based on the findings of an NEA sponsored workshop on lessons learned from the July 2006 Forsmark-1 event held in Stockholm, Sweden in 5-7 September 2007.

The task group members participating in this review included:

- John H. Bickel, ESRT, LLC (Sweden) - Chairman
- Alejandro Huerta, OECD/NEA
- Per Bystedt, SSM (Sweden)
- Tage Eriksson, SSM (Sweden)
- Andre Vandewalle, Nuclear Safety Support Services (Belgium)
- Franz Altkind, HSK (Switzerland)
- Thomas Koshy, USNRC (United States)
- David M. Ward, Magnox Electric Co. (United Kingdom)
- Kim Walhstrom, STUK, (Finland)
- Alexander Duchac, EC Joint Research Center Petten (European Commission)
- Robert Grinzinger, GRS (Germany)
- Ken Kawaguchi, JNES (Japan)
- Brigitte Soubies, IRSN (France)

The general objectives of the task group review were to:

- Evaluate the robustness of existing safety related electrical systems in nuclear power plants (including: design standards, acceptance criteria, design bases disturbances);
- Evaluate the basic principles used to develop a robust safety related electrical system in terms of critical design features, redundancy, diversity, and use of proven technologies;
- Evaluate methodologies used to demonstrate the robustness of safety related electrical systems, considering: definition of input transients, analytical approaches, defence in depth considerations, simulation techniques and use of computer codes (including the verification and validation of obtained results), definition of safety margins; and
- Evaluate the various modes of interactions between nuclear power plants and the electrical grid and the command and control interface between operators of the electrical grid and nuclear power plants.

From this DIDELSYS task group review, the NEA Committee on the Safety of Nuclear Installations (CSNI) desired a summary report that would:

- Provide information on the state-of-the-art regarding the robustness of safety related electrical systems (SRES), taking into account their interaction with other electrical equipment, the use of new technologies and the problems encountered when modernisation of existing plants is undertaken; and
- Provide guidelines for improving the communication and co-ordination between the grid (grid operator and regulator), the nuclear safety authorities and the licensees.

The DIDELSYS task group has now completed this technical report which is submitted to the CNRA and CSNI for further action

TABLE OF CONTENTS

List of figures

List of tables

EXECUTIVE SUMMARY

The DIDELSYS task group has studied the Forsmark event of 2006 and identified several electrical susceptibilities that warrant prompt attention for the operating reactors and new reactors under design. The primary issues are related to electric power supply to safety related equipment at nuclear power plants, the commonly used approaches, assumptions, and design standards for voltage protection of safety related equipment.

Key findings and recommendations

Electrical power systems supporting safety related systems and components in currently operating nuclear power plants are generally well designed to cope with high voltage surges caused by events such as lightning strikes on transmission systems (or switchyards) which can back-feed into plant distribution systems via auxiliary transformers. Lightning protection is accomplished via insulation ratings, grounding provisions, and incorporating design features, such as high voltage surge arrestors, sised according to internationally accepted industrial design standards such as:

- IEC-60071-1 1993-12: "Co-ordination of Insulation", part 1, "Definitions, principles and rules", part 2, 1996-12: "Application Guide";
- IEEE Std C62.23-1995: "IEEE Application Guide for Surge Protection of Electric Generating Plants"; or,
- KTA 2206 "Design of Nuclear Power Plants against Lightning Effects".

The comprehensiveness and co-ordination of electrical equipment protection features related to dielectric withstand capability against overvoltage events, such as lightning impulse, is well established. However components could be subject to other types of overvoltage events for which the withstand capability is not as clear[1]. This is particularly true for equipment based upon solid state devices which are becoming increasingly used in safety systems. These include devices such as uninterruptible power supply (UPS), rectifiers and local power supplies to equipment and control system cabinets.

The more problematic voltage surges are of a power frequency overvoltage character with quite substantial energy content, as they are driven by the main generator or transmission grid, and therefore cannot be quenched. The consequence of these surges can be the destruction or permanent tripping of essential loads. Voltage surges originating from an initiating event in the preferred power supply, main generator, or transmission system, and with a coincident failure of a non-redundant relay protection or breaker action, should therefore be particularly considered for the effects on equipment important to safety. The source of such voltage surges include (but are not limited to): capacitor/inductor bank switching, fault interruption by a vacuum interrupter or fuse, insulation

1. It is important to distinguish between dielectric withstand capability and correct operation of equipment and subsystems at temporary over-voltages. The 6, 10, and 20kV systems in Swedish NPPs are not effectively grounded. This means that all components are designed to withstand 173% voltages on the healthy phases when a single phase fault occurs anywhere on the system. It is, however, not clear how correct operation of equipment and subsystems has been verified for the overvoltage condition.

breakdown, main generator voltage regulator or excitation system failures, or voltage surges from main generator disconnecting from the grid and runback to house load following large load rejections or any other voltage demanding failures in the electrical switchyard. All of these could result in voltage surges in the range of 110% to 200% depending on the plant specific switchyards and the design of the main generator, exciter, and voltage regulator. Voltage surges in this range directly caused the 120% surge observed at Forsmark-1 in July 2006 and a 150% surge was observed at Olkiluoto-1 in May 2008. As all safety systems in currently operating nuclear power plants are powered via the preferred power supply any over voltage transient in these systems could lead to common cause failure. As an interim solution, the Olkiluoto station has modified the design to trip the generator output breaker when the terminal voltage exceeds 115% for a duration of 6 seconds. Further, a simultaneous high excitation current and more than 115% voltage for more than 6 seconds would generate a turbine trip and generator trip for protecting the onsite power system from potential overvoltage conditions.

In view of the potential severity of such events, the DIDELSYS task group recommends to:

- Conduct a Hazard Review to determine the *plant-specific range*[2] of possible voltage surge transients (considering: voltage and frequency content, rate of change, and duration) including: anticipated lightning surges, symmetric and asymmetric faults, switching faults, generator excitation system malfunctions[3] and develop a design specification to be used as a basis to qualify existing or replacement equipment. Such a Hazard Review should consider the impact of such faults in conjunction with a single failed or delayed protective device operation.
- Conduct a review of plant safety systems to confirm their capability to withstand the worst case power frequency overvoltage transients (including events such as: asymmetric or single phase faults, failure of the generator voltage regulator and excitation system with its maximum output)
- Review the potential voltage degradations, its rate and duration, and evaluate its impact on voltage sensitive devices such as local power supplies, MOVs, SOVs, contactors, etc.
- Review solid state device-based equipment such as: UPS, local power supplies, for their response (e.g. risk of tripping) to design basis voltage transients for an increasing and decreasing voltage in response to anticipated transients.
- Review the possible impact of voltage surge transients propagating through UPS, rectifiers, and other power supplies, causing detrimental effects on safety system loads and confirm that protective settings are properly co-ordinated to assure incoming supplies to battery chargers are tripped before devices powered from the batteries are lost.
- Consider the need for additional protection or equipment upgrade if the protective system response is not fast enough.
- Consider recovery procedures for equipment that could be locked out or fail during such events until any corrective actions are completed.

2. The intent of the DIDELSYS review was not to perform analysis to define specific limits to be used for qualifying electrical equipment. This is because there is plant-specific variability in plant earthing (or: grounding) designs, generator excitation and control system designs.
3. Electricité de France (Edf) reviewed the Forsmark event and additionally suggested the consideration of a simultaneous generator excitation system fault with a grid fault. The DIDELSYS working group did not have the ability to evaluate the probability or consequences of such events but would note it should if the risks of such events is assessed to be significant these should be considered in individual plant hazard assessments.

- For BWRs and PWRs that are designed with only electric power driven[4] decay heat removal systems: evaluate a diverse means for promptly supplying power to core cooling systems (e.g.: diesel driven pump, or fast starting gas turbine, etc.).

As a result of peer review feedback comments from several designer and nuclear plant operator organisations at the May 2009 DIDELSYS technical meeting, the DIDELSYS task group recognises that different groups made significant good-faith efforts to independently assess the potential hazards using different approaches, different boundary assumptions, and different selection criteria of the types of faults to be considered. Some considered only scenarios typical of Forsmark, others additionally considered the possibility of generator exciter failures such as occurred at Olkiluoto. Clearly there is a need for better definition of the types of hazards which require consideration and whether a different scope of hazard assessment is warranted for evolutionary nuclear power plant designs.

The DIDELSYS task group thus recommends to the CSNI that:

- A Technical Guidance Document should be prepared defining the recommended scope of the (previously described) onsite electric power system hazard investigation.
- It would be appropriate that such technical guidance document use a risk-based criteria for screening the types of single and/or compound faults that require consideration in the hazard analysis vs. those which need not be considered.
- The risk-based technical guidance would define the types of single and double (or compound) faults which need to be considered based upon probability (or frequency) of occurrence and electrical system consequences of such faults.
- The risk-based technical guidance document would also give consideration to the special situation of new evolutionary nuclear power plant designs which, although they will still rely upon vital buses for powering critical instrumentation and operator displays, will rely primarily upon passive features for essential safety functions such as core makeup, core, and containment cooling.

The DIDELSYS task group recognises that even with good co-ordination of insulation and voltage surge protection features it is possible for events to occur which degrade more than one set of vital instrumentation and logic power supplies. This de-energising of local power supplies will cause spurious actuation of the normal 2-out-of-4 (de-energise to trip) coincidence logic for engineered safeguards features – such as the partial actuation of the "Forced Relief System" that occurred during the July 2006 event at Forsmark-1. While in an outage in 1992 Millstone-2, which has two safety related electrical power trains, identified that 2-out-of-4 (de-energise to trip) coincidence logic would be actuated by the loss of a single electric power train. USNRC published "Information Notice 93-11" describing this type of concern and requested US licensees to review the issue and take appropriate actions. Given that it is unclear that all countries have taken comparable action on this concern, the DIDELSYS task group recommends to:

- Review RPS and ESFAS logic circuits for undesirable failure modes from loss of power, air, hydraulic pressure etc., (such as automatic depressurisation in BWRs, or actuation of automatic switchover to sump recirculation in PWRs) given loss of power to safety related electrical divisions or more than one train/channel of control and protection systems.

4. This recommendation applies to a unique group of nuclear power plants. Many existing BWR and PWR designs utilise a combination of electric and steam driven decay heat removal pumps.

- Develop procedures and/or design modifications to address concerns arising from such undesirable failure modes.
- Review the existing reliability and diversity of power supplies needed to support Operator Information Systems important to safety following a loss of one or two vital power trains.

The DIDELSYS task group recognises that efforts have been underway by WANO to improve coordination between operating NPPs and the electrical grid operators since the issuance of WANO SOER 99-1 and the 2004 Addendum which followed the major Blackout of the Northeastern United States and Canada. The DIDELSYS task group emphasises the importance of this work, which includes (but is not limited to):

- Joint planning and co-ordination of electrical power system tests and maintenance activities.
- Grid operators providing nuclear power plant operators with early warning of ongoing grid problems.
- Grid operators being informed of ongoing nuclear power plant operational limitations that might impact power operations.
- Nuclear power plants being recognised as a priority load centre requiring efforts to avoid load shedding in grid emergencies and highest priority for restoration given grid failure.
- Binding agreements regarding communications and coordination of planned activities.
- Nuclear power plants are required to have procedures for dealing with degraded grid voltage and frequency.

The DIDELSYS task group concurs with the importance of maintaining reliable, independent offsite power circuits for powering post-trip decay heat removal systems. The voluntary conformance efforts undertaken by WANO in SOER 99-1 (and the 2004 Addendum) are moving in the correct direction, however, it is necessary for national regulatory authorities to address concerns of commercial competition between electricity suppliers which may result in inadequate co-operation between grid operators and nuclear power plants. To make certain that nuclear power plants have priority for power restoration given a major grid disturbance the DIDELSYS task group recommends to:

- Confirm existence of, or immediately develop a protocol for requiring offsite power to the nuclear station as a high priority and instituting a Co-ordinated Risk Management of NPP and Transmission System covering onsite and offsite maintenance, planned outages, and maintenance on risk significant components.
- Review plans for grid recovery from brown and blackout events to assure adequate priority is given to NPPs and other essential high priority facilities.

ACRONYMS

AC	Alternating Current
ATWS	Anticipated Transients Without Scram
BWR	Boiling Water Reactor
BOP	Balance of Plant
CCF	Common Cause Failure
CDF	Core Damage Frequency
CSNI	Committee on the Safety of Nuclear Installations
DC	Direct Current
DIDELSYS	Defence in Depth of Electrical Systems and Grid Interaction
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EDS	Emergency Distribution System
EOC	End of Cycle
EPS	Emergency Power System
ESRT	Evergreen Safety and Reliability Technologies
FERC	Federal Energy Regulatory Commission
FMEA	Failure Modes and Effects Analysis
GL	Generic Letter
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit mbH
GUI	Graphical User Interface
HSK	Hauptabteilung für die Sicherheit der Kernanlagen (Switzerland)
I&C	Instrumentation & Control System
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical & Electronics Engineers
IN	Information Notice
IRS	Incident Reporting System
IRSN	Institut de Radioprotection et de Sûreté Nucléaire
JNES	Japan Nuclear Energy Safety Organisation
JRC/IE	Joint Research Center /Institute for Energy
LOCA	Loss of Coolant Accident
MOV	Motor Operated Valve
NEA	Nuclear Energy Agency
NERC	North American Electric Reliability Corporation
NPP	Nuclear Power Plant
OECD	Organisation for Economic Co-operation and Development
PPM	Plant Portfolio Manager
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment

PWR	Pressurised Water Reactor
RCP	Reactor Coolant Pump
SBO	Station Blackout
SOER	Significant Operating Experience Feedback Reports
SOV	Solenoid Operated Valve
SSM	Strålsäkerhetsmyndigheten (Swedish Radiation Safety Authority)
TSO	Transmission System Operator
UCTE	Union for the Co-ordination of Transmission of Electricity
UPS	Uninterruptable Power Supply
USNRC	United States Nuclear Regulatory Commission
WANO	World Association of Nuclear Operators

1. INTRODUCTION

1.1 Scope

This report documents the results of a CSNI sponsored review of the defence in depth of nuclear power plant electrical power supply systems as an international follow-up to the July 2006 event at Forsmark-1. The scope of the review considered the effects of: equipment redundancy, application of defence in depth principles, and robustness to withstand challenges and faults originating from both the external electrical grid and within the plant. The report has been prepared to address the specific interests of the CSNI, including:

- Definition of input transients.
- Interactions with the grid.
- Analytical approaches.
- Defence in depth considerations.
- Simulation: use of computer codes (validation and verification of obtained results),
- Safety margins.
- Testing: laboratory tests, scale tests, component testing, system testing, revisiting commissioning tests, others.
- Definition of the robustness of safety related electrical systems (considering: acceptance criteria, and design basis for establishing disturbances to be coped with, etc.).
- Basic principles to develop robust nuclear power plant electrical systems, including: typology, redundancy, diversity, and use of proven technology.
- Recommendations on methodology to be used to demonstrate the robustness of nuclear power plant electrical systems.

The report is organised to address the specific CSNI requests noted in the Scope. The introductory Section 1 provides the technical background for the DIDELSYS group report including the general principles of nuclear power plant electrical system design, highlights from the September 2007 DIDELSYS meeting held in Stockholm, and a discussion of international operating experience with similar types of events.

The details of the July 2006 Forsmark-1 event including a time-sequence of events is included as Appendix A. Proper understanding of the Forsmark event, and similar events which have occurred elsewhere, requires an understanding of industrial design codes and standards which are relied upon to design nuclear power plant electrical systems. These codes and standards represent a consensus understanding of the common assumptions and assumed safety margins recommended by experienced electrical design engineers. A discussion of how these industrial codes and standards compare is provided in Appendix B along with insights where experience would seem to indicate a need for revisions to account for recent operating experience.

Section 2 provides a discussion of the general principles of defence in depth used in the preparation of this report. Section 3 addresses the specific technical issues associated with the CSNI's charge to the working group. Section 4 documents the DIDELSYS working group's final conclusions and recommendations for future efforts.

1.2 Objectives

The objectives of the DIDELSYS working group's report are to identify a number of findings and recommendations that should be considered by the nuclear industry and regulatory authorities of member countries represented by the CSNI. In a number of areas, there appears to be a common reliance on possibly incorrect design assumptions regarding the types of electrical transients (from both the external grid and from within the plant) which should be considered as design bases for nuclear power plant electrical systems. Many of these design assumptions appear in industrial codes and standards (such as IEEE and IEC standards) used by electrical designers and are frequently relied upon by nuclear regulatory authorities as the current "state of the art" to address issues of reliability and robustness in safety equipment design. Where operating experience indicates the possibility of more severe design conditions than originally envisioned, these codes and standards should be considered for revision in light of new experience. The DIDELSYS working group did not undertake new analyses to define recommended changes to specific levels of safety margins provided for in codes and standards as this was beyond the group's charter and would have required significantly more funding support, a larger organisation, and work duration. Matters related to breakdowns in engineering quality assurance are similarly beyond the scope of the DIDELSYS working group's review – as these are required in implementing any design according to any code or standard.

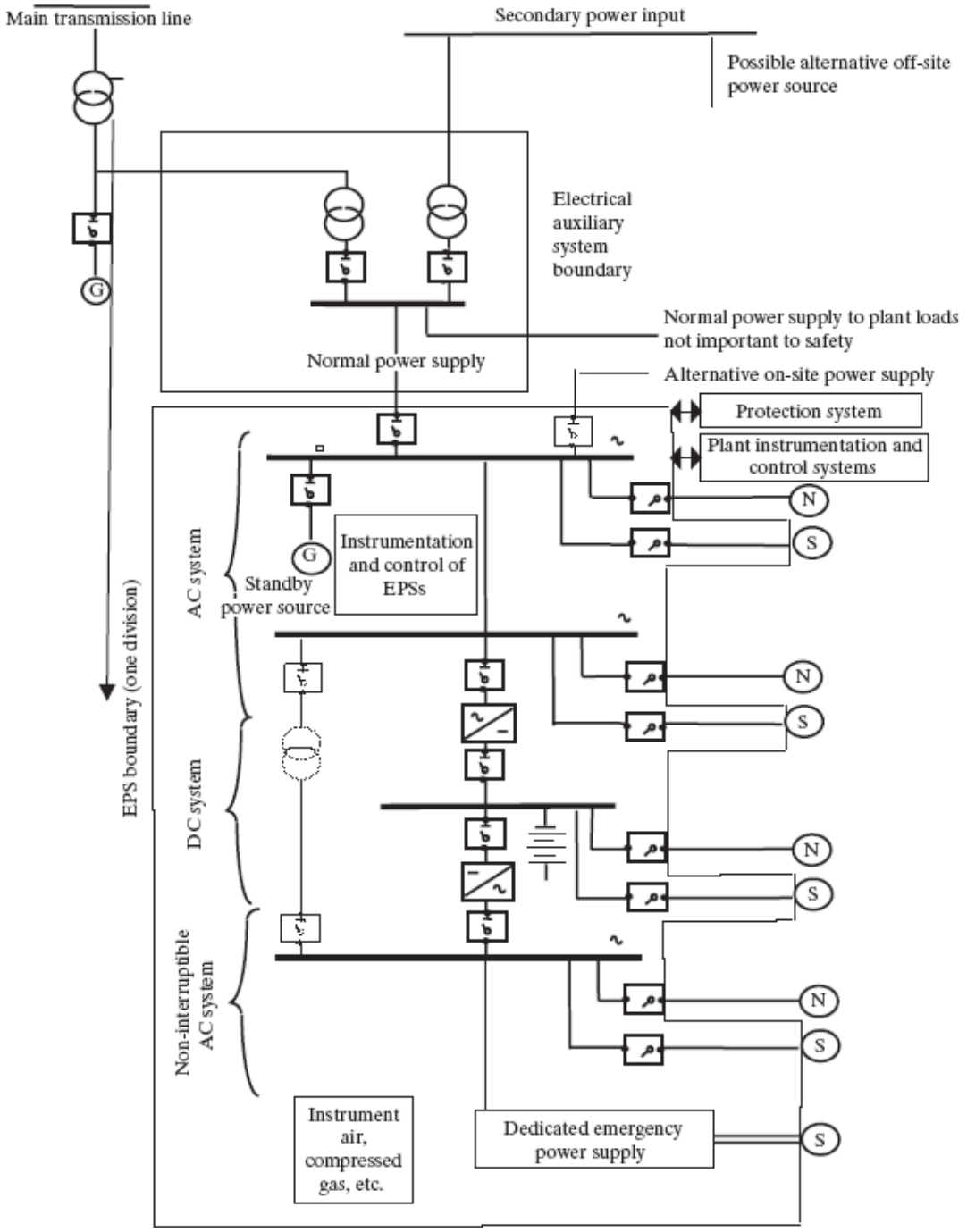
1.3 General features of NPP electrical power systems

1.3.1 Introduction

Nuclear power plants (NPPs) rely on electrical power for various safety functions and the reliability of power supply has always been a focus of safety engineering and assessment. Electric power is needed for operation of pumps and valves. A regulated, but low voltage power is needed for the operation of control systems, to supply starting and control signals to pumps and valves, and to support operator information systems needed by the operators to control the plant. Consistent with IAEA Safety Guide NS-G-1.8[5], nuclear power plants are normally equipped with a minimum of two separate power supply connections with the outer grid, with one of the circuits designed for rapid connection to supply shutdown loads through a start-up transformer when the main generator is not available for supplying house loads. Figure 1.3-1 taken from Safety Guide NS-G-1.8 shows a typical organisation of a nuclear power plant electrical power system. During normal plant operation, a portion of the high voltage power generated by the plant's main generator is fed back through unit auxiliary transformers to supply all normal house loads such as running pumps and local power supplies for instrumentation and control systems.

5. International Atomic Energy Agency, Design of Emergency Power Systems for Nuclear Power Plants, Safety Standards Series No. NS-G-1.8, Vienna, 2004.

Figure 1.3-1: Typical nuclear power plant electrical power system per safety guide NS-G-1.8



All Swedish NPPs, and many European NPPs, are designed with a main generator circuit breaker. This type of feature is rare in US NPPs (Millstone-3, Seabrook only). In the event of a generator, turbine or reactor trip, provided the unit is equipped with a generator breaker, power supply for house loads continues to be supplied from the grid via the unit transformer. If the unit breaker is opened as a consequence of the unit trip, the auxiliary load must be transferred to the alternative grid supply via the start-up transformers. The station auxiliary transformers are energised from the (typical)

20kV side of the generator step-up transformer and the external electrical grid (compare this with Figure 1 in Appendix A). When the generator circuit breaker operates correctly, no bus transfer is necessary and the only transient is the voltage drop caused by the loss of active (real) power injection into the grid. In the event of a unit trip on an NPP without a generator breaker configuration, power supply for house loads must be transferred back to the grid via the start-up transformers.

In the event power from the grid is unavailable, the onsite power system is also designed with redundant on-site power supply systems consisting of standby diesel generators and/or gas turbine generators (supported by batteries) in order to secure power in a variety of situations. Instrumentation and control power, which is needed on a continuous basis for safety instruments and operating the onsite power system, was historically provided by a combination of motor-generator sets and transformers backed up by battery-inverter units. Motor-generator sets have the advantage that sudden momentary voltage surges or dips cannot be transmitted across a rotating flywheel due to their inertia. Motor-generator sets have the disadvantage of requiring routine maintenance as would be required of any large piece of rotating equipment. Efforts have been underway in a number of OECD countries to replace vital AC power from motor-generator sets with solid state uninterruptible power supplies (or UPS). In making such a design upgrade, the response of solid state UPS units to momentary voltage surges and dips must be considered.

An event took place at the Forsmark Unit 1 nuclear power plant on 25 July 2006 that raised a number of issues related to the robustness of the electric power systems. Forsmark had replaced the original motor-generator sets with solid state UPS units as a part of a modernisation program carried out in the early 1990s. A short circuit in the offsite switch yard in combination with independent faults resulted in a momentary voltage surge of ~120% on the onsite power supply systems, which resulted in common cause failures of 2 of 4 redundant UPS units and all safety components powered by these UPS units. A detailed description of the Forsmark event is contained in Appendix A. The investigations of the causes of the event highlighted some issues of a potentially generic nature. The international experience also includes similar events in other nuclear power plants that have indicated weaknesses related to electrical systems.

In the Forsmark event, as in some other events reported from other plants, the impact on the calculated core damage probability has been quite significant. It is therefore important to gain understanding of potential weaknesses in the design, in the safety justification analysis and in the operation of electrical systems important to safety, and to establish approaches to address and correct these weaknesses.

1.3.3 The DIDELSYS Workshop, Stockholm 5-7 September 2007

The importance of the findings and experience from the Forsmark event, and from other nuclear power plant events that have taken place, motivated the Swedish Nuclear Power Inspectorate (SKI) to invite to a workshop in Stockholm on September 5-7, 2007. The objectives of the workshop were to gain understanding of potential weaknesses in the design, in the safety justification analysis and in the operation of electrical systems important to safety, and to establish approaches to address and correct these weaknesses. SKI considered a workshop to offer a direct way of sharing insights in the Forsmark event and the best possibilities for exchange of experience with experts from the nuclear power industry, from regulatory organisations and from consultant organisations.

The workshop was organised along the following main headings

- Events of generic importance
- Design and analysis
- Interaction between the NPP and the grid
- Concluding session

The technical experience and conclusions were in summary the following:

1. All types of possible situations resulting from anomalies in electrical components are very difficult to anticipate. Experience shows such situations, of which some included hidden failures with CCF[6] character, resulting from deficiencies in functional requirements and specifications and in processes for equipment design review, verification and testing.
2. Plant modernisation often includes replacement of older equipment with modern technologies that include programmable systems. This can be done in larger projects but also gradually in smaller steps. In the later case, new failure modes could be introduced inadvertantly. Often the new equipment includes several functionalities (embedded functions) that go beyond the capabilities of the old equipment and, in some cases, also beyond the awareness of the designer. Introduction of such equipment ("black boxes") could introduce unexpected or even unwanted functionalities with potential negative safety impact. The designer and the operator must be fully aware of the specified functionalities of the equipment, as well as of its non-wanted functionalities.
3. Most plants were designed many years ago. The knowledge of design bases and engineering practices are gradually lost. The technical standards have very limited guidance on specific design issues. The full understanding of the electrical systems design is of prime importance for their correct maintenance and replacement.
4. A potential conflict between requirements originating from the grid and plant safety requirements must be avoided by finding a common understanding between the grid and the plant operators. This is necessary in order for the plant operator to define correct design events and conditions related to the grid that the plant has to cope with. Increased contact between grid and plant operators for coordination of requirements were recognised to be beneficial for reactor safety. The wider co-operation in grids across borders in some areas will also require increased international contacts.
5. The need to enhance the analyses of grid and plant interaction was recognised in order to better define the enveloping profiles that could challenge the plant's safety systems. Simulation of dynamic behaviour outside and inside the plant has become a necessity to cope with the ever-changing grid conditions and plant modifications.
6. The event showed that contacts between the plant operator and the grid operator needed to be improved. This is probably true also for other operators. Co-operation is vital in e.g. planning of operation and maintenance of the grid and for a common understanding of the consequence of disturbances in order to properly define the design basis for plant equipment and to optimise the protection schemes.
7. In many countries the grid operator or the nuclear regulator asks for the possibilities for NPPs to switch over to house load operation (islanding). This enables a continuous supply of auxiliary power for safety needs at grid disturbances. But it also could expose the onsite systems to the instabilities in voltage and frequency associated with such disturbances. Both aspects should be considered in design of the electrical systems. Disconnection of a plant from the grid may induce challenging transients in the onsite electric systems, even if islanding is not part of the safety strategy.
8. Even after comprehensive reviews of electrical systems during commissioning and for example in the context of modernisation, the risk for latent CCF remains. Such failures

6. Common Cause Failures.

can be very difficult to reveal. Factors such as design features, modes of operation, environmental conditions, etc., could, in unfavourable combinations, weaken the ability of the plant to handle disturbances and transients.

9. The robustness of the electrical systems must be maintained through quality in design, operation, maintenance and testing. The robustness should be demonstrated by a broadminded event analysis based on a thorough knowledge of electrical engineering and on insights from experience feedback, preferably complemented by using methodologies such as FMEA, dynamic transient analysis and PSA.

1.4 Highlights from international operating experience

1.4.1 Incident reporting system

The IAEA/OECD/NEA Incident Reporting System (IRS) was chosen as a reference database to identify relevant events that occurred at the electrical grid or plant electrical systems. With the courtesy of the IAEA, selected JRC/IE personnel working on EU Clearinghouse was granted access to the IRS database.

IRS contains a number of events that are directly related to the disturbances in the plant electrical systems. The Incident Reporting System (IRS), operated jointly with the OECD/NEA, was set up in 1983 to exchange information on unusual events at NPPs and to increase awareness of actual and potential safety problems. In 2006, the Web based IRS was created to facilitate data input and report availability. As a consequence, the number of reports has increased and the dissemination delays have reduced[7].

The World Association of Nuclear Operators (WANO) has established and operates database of event that occurred at nuclear power plants operated within the WANO club. In addition, WANO regularly publishes Significant Operating Experience Feedback Reports (SOER) in order to share valuable learning points gained from the operating experience of colleagues in WANO.

When screening the IRS database, there were 88 events identified that have a common denominator – disturbances in the plant electrical systems or/and problems with electrical power supply, including grid disturbances. It appears that the disturbances in plant electrical systems are quite common events. It is important to note that the IRS database is not complete. The IRS database contains only those events that were voluntarily reported by participating countries; i.e. there are only events reported that power plant operators or regulatory bodies considered important to safety.

Licensee Event Reports (LERs) issued by NPPs in the US were complementary to the IRS data base, and served as another important source of information about events that involved disturbance in the plant electrical systems. About 19 relevant reports that the plants reported to the USNRC were also included to better illustrate the variety of events involved in grid or plant electrical system disturbances.

For the purpose of this report, some events involving disturbances in the grid or/and plant electrical systems were identified that may be used by participating countries for further considerations in their operational experience feedback. The time period chosen for this screening includes events reported between 1994 and June 2008.

7. Nuclear Safety Review for the year 2006, IAEA publication

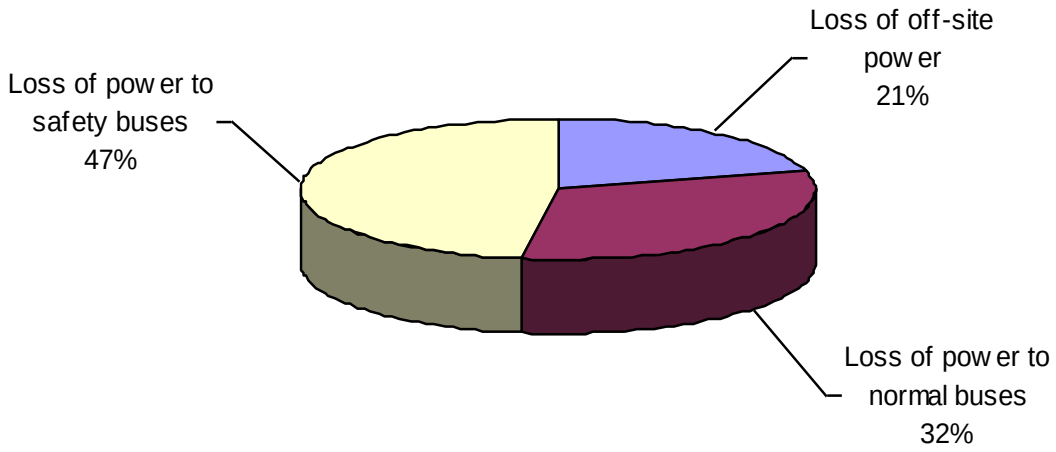
1.4.2 Results of the event database screening

The IRS database screening showed that 88 events involved disturbances in the grid or plant electrical systems. These events occurred at nuclear power plants worldwide. This amount is quite significant, especially when considering the consequences of some identified events to the plant safety.

Sorting the events by different categories provides interesting insights on initiators, failure modes, contributing factors, electrical equipment involved, specific human factors and event consequences to the plant safety.

Reported disturbances in the plant electrical systems involved the following major failure modes with varying levels of impact (see Fig. 1.4.2-1 for illustration)[8]: Loss of off-site power[9], Loss of power to normal electrical buses (with offsite power available) that generally affect power production, and Loss of power to safety buses (with offsite power available). Although the 14 year time interval during which all these 88 events were reported is considered as relatively long, the number of events that involved failures of electrical supplies - in particular to the plant safety buses - seems nevertheless to be quite high. Even the number of reported events that caused Loss of off-site power at the plant seems to be significant.

Figure 1.4.2-1: Dominant failure mode distribution



It is important to mention that the plant safety buses provide electrical supply to the systems important to safety. De-energising the safety buses for a longer time or during accidental conditions without possibility to recover the power supply either from standard power supply or EDG[10] might lead to deterioration of several safety functions at the plant. Fortunately none of those events reported database did occur simultaneously with another initiating event (e.g. LOCA) that would require the operation of plant systems important to safety.

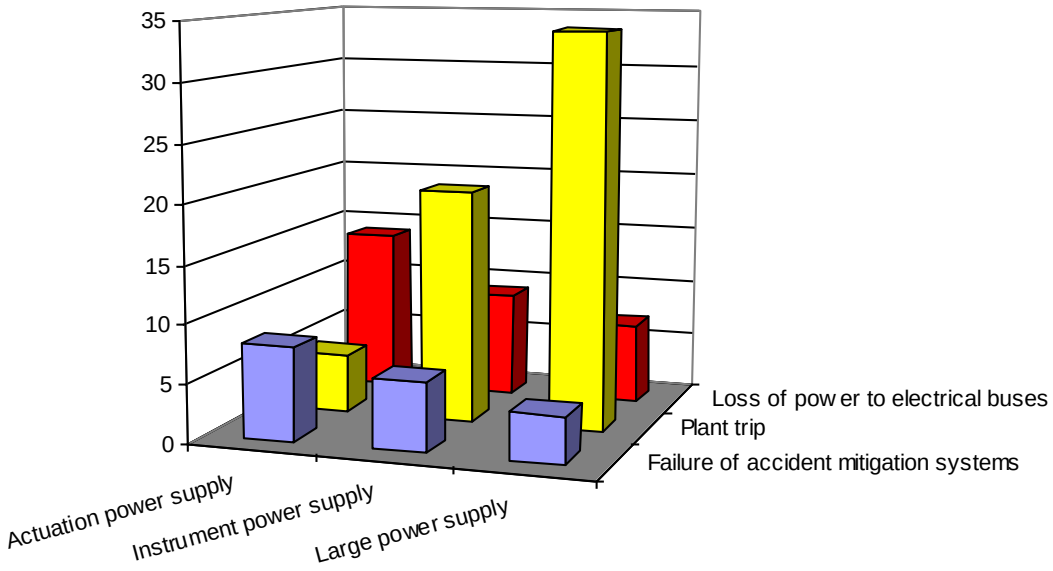
The dominant failure mode for loss of specific power supply is another category that requires attention. Fig. 1.4.2-2 shows the distribution of dominant failure modes for loss of instrument channel

8. The intent is to highlight the large general classes of failure modes studied. Given that the IRS data base is incomplete, the relative fraction of specific failure modes should *not be used for statistical calculations*.
9. Loss of offsite power includes all events in which electrical power from the grid, the preferred power source for accident mitigation, is disconnected as a result of events external to the NPP such as severe weather and external grid faults.
10. Emergency Diesel Generator

supply, large power supply, and actuation power supply. For the purpose of analysis, the loss of instrument channel represents a failure or spurious actuation of any measurement (I&C) component; the loss of large power supply represents an internal or external event that led to the loss of main power lines, malfunction of major electrical equipment (generator, transformer, switchyard, etc.) or human error (operational or maintenance); the actuation power supply represents failures of electrical components (circuit breakers, transformers, etc.). The ageing effects and human errors also contributed to above failures.

The number of dominant failure modes for loss of specific power supply is shown on Fig. 1.4.2-2. This chart shows more or less expected results, such as: the loss of large power supplies mostly led to the plant trip, while the loss of actuation and instrument power supply led in particular to loss of power to electrical buses and consequently to failure of accident mitigation systems.

Figure 1.4.2-2: Dominant failure modes on loss of power supply



As a result, the loss of actuation and instrument power supply has in general more significant consequences than loss of large power supply.

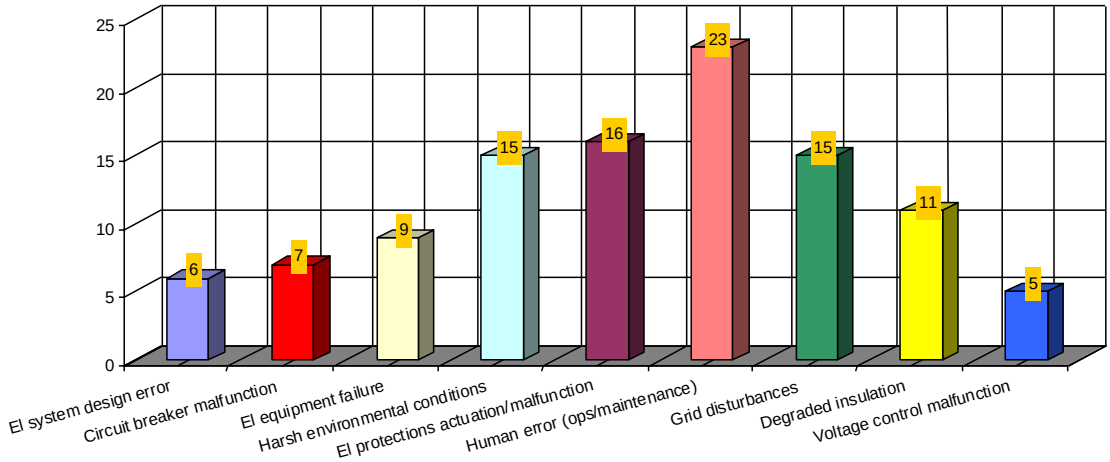
What actually caused all these failures? A closer look at the event analyses showed number of failure modes that involved different types of electrical equipment and that had an effect on the proper functioning of actuation power supply, instrument channel supply, and large power supply. In the following sections, failure modes and their contributing factors will be discussed. In addition, some examples of each contributor category are presented to illustrate circumstances and their role to the sequence of the event. Examples used in this report contain a narrative description of the event without mentioning the specific reactor brand or nuclear power plant name.

1.4.3 Contributing factors to the selected events

Closer evaluation of the selected events related to disturbances in plant electrical systems helped revealing common contributing factors (in some cases initiators) for a certain group of reported events. It should be understood that the list of events reported in IRS database may not be complete, since not all the loss of offsite power events are reported.

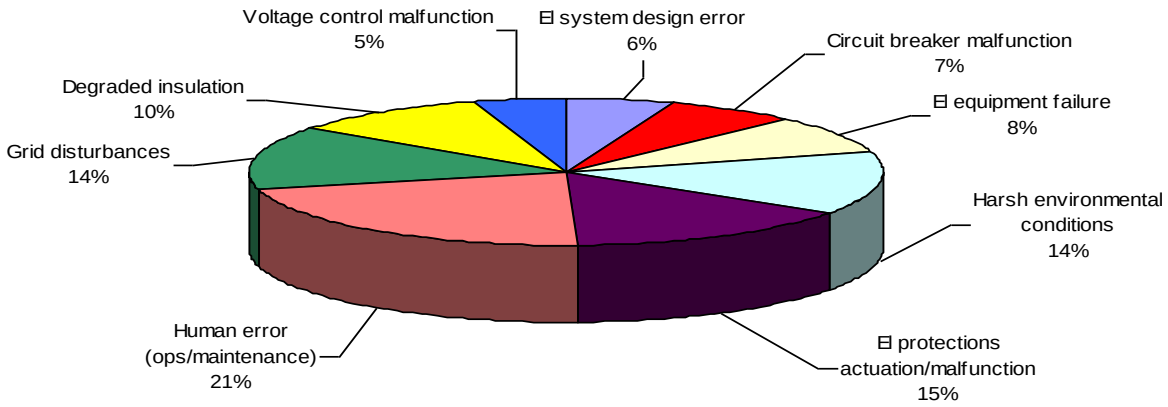
Reporting to the IRS system is voluntary and therefore the information obtained should be cautiously considered. Not all over-voltage events are explicitly identified. Therefore, this report presents information on results of IRS screening and US NPP Licensee Event Reports without making general conclusions, to show that there is international operating experience additional to Forsmark-1 event. In this survey, and for certain groups of events, a number of representative contributing factors have been identified; e.g.: Fig. 1.4.2-3 shows the distribution of these contributing factors by different categories.

Figure 1.4.2-3: Contributing factors identified in the selected events



A pie chart in Fig. 1.4.2-4 represents a percentage share of each of the contributing factors from among all events identified during the screening process.

Figure 1.4.2-4: Percentage share of contributing factors to the selected events



The following sections provide a discussion of these contributing factors and also present examples of relevant events from the IRS database.

1.4.3.1 Human errors

As can be seen, the category of human errors constitutes an important contributor to the group of initiators of the reported events. These human errors involve errors of plant as well as contractor personnel (misalignment of electrical systems, tasks performed in different than required sequence, omitting/incorrect operation, switching error, maintenance error, etc.).

Human errors may have adverse and sometimes unpredicted consequences. Actually, the Forsmark-1 event was initiated by an external contractor error during maintenance activities in the switchyard. It is very important to carefully analyse every event that involves human errors and to take appropriate corrective measures. The following are examples of events involving human errors.

- Reactor trip occurred due to generator protection system activation in coincidence with permissive P-7 (with the power higher than 10%). Activation was due to human error during corrective maintenance on the main generator protection system, while trying to find the cause of asymmetry of the phases on an electrical pump motor.
- The plant lost its connection to the 400 kV grid due to a maintenance personnel error made during open switchyard tests. One of the two start-up transformers (110 kV supply) had been erroneously disconnected for maintenance work and consequently the power supply to two electrical sub-systems was lost. EDGs started and powered safety buses as designed.
- An I&C technician attempted to bypass a breaker electrical protection signal to prevent an unexpected plant trip during replacement of a transmission line protection panel. He removed the breaker protection lead wires according to instructions. At that time, both the generator and main transformer tripping relay actuated, causing the trip of both operating generators and consequently tripped the reactor.
- While dismantling a crane, a beam fell down and damaged 6kV cables beneath. Electrical protection isolated the Unit transformer (6/330kV) from the grid. Reactor protection systems tripped Units 2 and 3 on loss of power supply. The emergency power supply was restored by starting up EDGs at both units.
- At several plants there was a loss of power from five UPSs which powered the main control room information and alarm system and other systems important to safety. The failures occurred because of inadequate maintenance of the batteries that supply power to the control logic. A non-safety-related power supply failed to provide power to a radiation monitoring cabinet, which in turn caused several engineered safety features to be actuated. The failure occurred because of inadequate maintenance of the power supply output breakers. The loss of this power source, combined with the failure of one UPS to transfer to its backup supply, resulted in a loss of power to some AC instrument panels.
- A momentary grid voltage disturbance occurred that caused a reactor trip of both reactors from full power. Each reactor tripped when both channels of safety related 4kv bus under-voltage relays actuated after a one second time delay. Protection against a momentary grid disturbance is a feature of the plant electrical system, however, the duration of the condition exceeded the time delay resulting in the actuation of the 4kV bus under-voltage relays. The grid over-voltage disturbance occurred due to human error when a protecting and control field engineer disabled both levels of protection at an electrical substation which then failed to actuate when a fault occurred during equipment troubleshooting.

1.4.3.2 Electrical protections

Failures of electrical protection features constitute the second most important category of contributing factors. The corresponding failure modes involve incorrect set-points, failures to actuate due to malfunction or ageing of internal components (mostly relay elements), as well as spurious actuation. This is probably not surprising, because there is a large number of electrical protections installed at the plant, and there are demanding design requirements for electrical protections. The electrical protection is designed to actuate precisely when they ought to in terms of milliseconds. The reason is that the plant should stay connected in case of some smaller disturbances in the grid. The electrical protection should however not actuate too early; it may cause unnecessary power reduction or plant trip and loss of production. On the other hand, the electrical protection should actuate early enough to isolate the voltage/current disturbance or faulted equipment to avoid propagation of the electrical fault to the plant electrical systems.

Electrical protection is designed to isolate faults with minimum disturbance to the overall system. When the primary system fails to act or when it experiences delay, a second protection system will respond with more isolation.[11] The relays which actuate in milliseconds sometimes involves simultaneous measuring of different parameters such as voltage and current in the different parts of the plant electrical system. The configuration and setpoints of electrical protection should ensure appropriate selectivity to avoid unnecessary propagation of electrical disturbance to the entire plant electrical systems.

In order to avoid single failure of a safety bus or an EDG due to spurious/real actuation of electrical protection, there are specific design requirements at the various plants. The US plants have no electrical protection on safety buses, only on feeders. Corresponding circuit breakers are designed to open in short circuit without damage (or fire risk). Some European NPPs however have electrical protection at safety buses[12]. There were cases of spurious actuation of electrical protection preventing the energising of the safety bus. It is a matter of the design approach on electrical protection at the plant. Nevertheless, it is important that appropriate defence in depth in the plant electrical systems is considered during the design of new power plants as well as during the scheduled periodic safety reviews of the older plants. The following are examples of events involving electrical protection.

- An inspection of electrical protection settings revealed that the current thresholds had been set to a value between 6 and 30% less than that required for all 6.6 kV equipment powered by the electrical switchboard of Train A (11 actuators, including those of the back-up pumps) and the equipment powered by five other switchboards (23 actuators).
- While the plant was operating at full power, two random failures of separate and independent differential protection relays caused both EDGs to be inoperable for about 16 hours. Following the second failure the controlled shutdown was initiated, and it was terminated at 22% power when one EDG was returned to service. The spurious operation of the generator differential relays was caused in both cases by a zener diode that failed for no apparent reason. The zener diode failures probably resulted from component end-of-life or from cumulative damage from normal transients. The incorrect wirings of the lockout relay, discovered during troubleshooting, may have contributed to the diode failure.

11. Electrical protection systems in NPPs consist of two main protections or one main and one back-up protection feature. Modern electrical protection systems are designed according to the defence in depth principle, but the term is seldom used in the relay protection community.
12. This is a requirement on Swedish NPPs based on national laws and regulations.

- A failure of electrical protection relay resulted in the loss of a safety switchboard in Train A and led the operator to apply an incident procedure. The safety switchboard (6.6 kV power supply) remained unavailable during 9 hours. The intermediate shutdown state was reached with only the safety switchboard on train B being supplied by the auxiliary transformer. The electrical power supplies, the secondary core cooling and the safety systems were degraded.

The U.S. Nuclear Regulatory Commission (NRC) issued an information notice to inform addressees of a loss-of-offsite-power and dual-unit trip event that occurred at one plant due to circuit transformer failures and improper switchyard bus differential relay settings. The NRC expects that addressees will review the information for applicability to their facilities and consider actions, as appropriate, to avoid similar problems. However, the suggestions contained in this information notice are not formal NRC requirements; therefore, no specific action or written response is required.

1.4.3.3 Adverse environmental conditions

Adverse environmental conditions, such as high winds and snow, freezing rain, lightening, earthquake, and flooding have been reported to the IRS system. This category belongs together with grid disturbances to the third largest category after human error, and the safety significance of some events is obvious.

In most cases, harsh environmental conditions affected the plant main and auxiliary power supplies, and lead in some cases to a forced house load operation or a long term mission of the EDGs to maintain electrical power supplies. The following are examples of events involving harsh environmental weather conditions.

- A combination of freezing rain, low temperatures and strong winds caused short circuit on the open air SF6 penetrations in the power transmission switchyard serving the four units one of a nuclear power plant. This resulted in a loss of 400 kV power transmission line from unit 1, followed in sequence by the loss of the lines from the remaining three units. As the 400 kV power supply to the auxiliary transformer on one unit is provided from the transmission sub-station on the other unit in the pair, both offsite power sources were lost by all four units simultaneously. Units 1, 3 and 4 successfully entered house load operation following the loss of their main offsite power source. A turbine at Unit 2 tripped on overspeed protection while the power transmission line circuit breaker opened which caused the reactor trip. Because there was no longer any supply to the auxiliary transformer (due to the loss of the main power transmission line from the other unit in the pair), power was supplied to the back-up auxiliary systems from the EDGs buses via switchboards. Analysis of this incident has shown that the effects of freezing rain were not included in the climatic considerations taken into account at the design stage. The shape and positioning of the insulator sheds was a contributing factor to the arcing between the high voltage end of the insulator and ground.
- During very severe weather conditions (high winds), all electrical grid connections to the site were progressively lost. Both reactors were manually tripped. Later on, the grid connections were lost again for a second time due to the same cause. Following this loss of off-site power, it was necessary to manually reconfigure essential electrical supplies from the diesel generators because the bus transfer system had not been fully reset and was unavailable for automatic operation.
- A severe tornado caused extensive damage along the 500 kV/230 kV transmission corridor and affected a site with 6 operating units. The damage resulted in operation of the load and generation rejection system which separated three generators from the bulk electrical system. Other Units suffered a turbine trip 1 second after the rejection and

experienced various difficulties including a loss of Class IV power, overheating and damage to one turbine bearing. Sometime after the initial rejections, further faults and losses of transmission lines occurred and resulted in the entire plant site being isolated from the grid. Unit 6 in fact "motored" and Unit 2 supplied its own and Unit 6 service loads as designed.

- Stormy wind (33.7 m/s) caused the fall of a lightning arrester and hence a short circuit on phase A of the 750 kV line. A differential electrical protection actuated to isolate the short circuit. A 750 kV circuit breaker failed to open and the single-phase automated restoration system did not operate successfully. Both Unit 3 turbine generators tripped.
- A lightning that stroke the plant has been reported by several plants. For example, two lightning strikes on two separate high voltage transmission lines caused a full generator load rejection. A design deficiency of the generator excitation logic delayed a unit response to the load rejection and resulted in a turbine-generator trip and in a short power interruption on a 13.8 kV electrical bus. The power interruption, which lasted only 1.2 seconds, however affected the main reactor coolant system pumps and resulted in a reactor trip.
- During rated power operation, a "Neutron Flux High" signal caused a reactor trip. The reason behind it was as follows. A portion of surge current due to the lighting strike reached the outside wall through the main exhaust duct from the vent stack, resulting in the generation of an induced current in the transmission cables for neutron flux monitoring system, and generated signal from 3 out of 6 channels, which are installed in the same cable duct close to the outside wall of the building. Subsequently, a high neutron flux signal was annunciated by spurious signals due to the induced current.
- Lightning stroke one phase of 24 kV conductors (power output of main generator) and caused initially one-phase short circuit that further developed to a two-phase short circuit. The main generator, the main transformer as well as house load transformers were isolated by the unit electrical protection system and eventually tripped the reactor.

Some unusual events induced by environmental conditions were also reported to IRS. For example, water dropping from a ventilation unit caused an electrical fault on a 13.8 kV electrical distribution switchboard with subsequent several major power interruptions within the unit and the trip of both reactors. Or, an earthquake caused a bus duct collision with transformer secondary bushing, which resulted in a short circuit at the secondary side of the house load transformer.

1.4.3.4 Grid disturbances

Only a few events were reported in IRS database about grid disturbances. One possible explanation is that a grid disturbance – unless it has impact on the plant operation – is not always reported. A grid operator has no obligation to report to the IRS. Therefore, many grid disturbances that did not develop into events triggering the plant electrical systems (main power lines, auxiliary and backup power supplies) remain hidden.

There were about 12 events reported about electrical grid disturbances in Licensee Event Reports from US nuclear power plants (that were not reported to the IRS). These reports are very relevant, and therefore included in this report. They provide valuable insights how the plant electrical system, as well as the plant itself responded to the electrical grid disturbances.

The design of grid systems is country specific, as well as the configuration of the plant output and the external power supply. It may vary significantly among countries and plant sites. The interaction of the grid system and the plant may therefore be very specific. The grid disturbances may impact several local substations causing partial disruption or simultaneous loss of main output as well

as auxiliary (start-up) power lines. Such disturbances may lead to common mode failures and should be carefully considered in the design of the plant power supply system.

The industry has to restore the understanding of the design of NPP electrical systems and their interactions with the external grid. Lost knowledge from the design era tends to be replaced by the application of standards. However, standards do have limitations as to completeness and guidance. Full understanding of the design of NPP electrical systems was recognised to be of prime importance for formulating correct and comprehensive specifications for new equipment[13].

The following examples are presented on grid disturbances that caused problems at the plants.

- Grid disturbance problems resulted in partial loss of off-site power at a plant operating two units. A complete loss of voltage in the 400 kV grid occurred due to a lightning strike in a grid station. Power plant electrical buses I and II of the 110 kV switchyard were fed from the 400 kV grid and from the 220 kV line from a hydropower station, respectively. Safety buses 7 and 9 were fed from buses I and II respectively. The loss of voltage in the 400 kV grid caused a loss of voltage in safety bus 7 and consequently the start of the EDG. There was an instantaneous loss of voltage in the 220 kV line too that lasted more than 0.2 seconds. The corresponding EDG started but because the voltage recovered in less than 2 seconds the EDG did not load. Following the loss of the 400 kV grid, the three reactor coolant pumps tripped, and the plant remained in natural circulation about 15 minutes. The fast transfer from 400 to 220 kV did not work, most likely due to unavailability of the 220kV line.
- A plant operating two units was connected to two grids, A and B. The A grid feeders were manually tripped by the A grid State Electricity Board because B grid State Electricity Board was drawing power in excess of its power generation quota. The plant remained connected to the B grid system only. A sudden drop of frequency from 50.4 Hz to 49 Hz and further down to 47.5 Hz actuated the under-frequency protection and tripped both generators. Two grid B feeders simultaneously tripped on under-frequency relay protection, thereby leading to total loss of power.
- A short circuit occurred in the grid at the 500 kV substation, causing the grid voltage to degrade. During voltage decrease the generator transferred to voltage boosting mode with doubled rotor rated current. With the generator operating in the boosting mode, some elements of the generator excitation system however failed and caused loss of generator excitation and transfer to asynchronous mode, which resulted in voltage oscillations and generator trip. The reactor tripped and the plant 6 kV normal buses transferred automatically to their back-up power source.
- An electrical power grid disturbance occurred at the full power operation, resulting in a momentary lowering of voltage on both 2400 volt safety related buses. The reduced voltage on the 2400 volt buses caused both emergency diesel generators to start. However, the 2400 volt safety related buses remained energised from offsite power throughout the event. Local grid conditions stabilised within approximately five minutes. The plant remained at full power throughout the event.
- A nuclear power plant automatically scrammed from full rated thermal power when the turbine tripped on a load rejection. A large disturbance in the electric grid had caused the turbine to trip. Both emergency diesel generators automatically started and supplied the emergency buses. The electric grid disturbance ultimately led to the loss of the reactor recirculation pumps, condensate pumps, and circulating water pumps. Reactor pressure and water level were maintained using the electromatic relief valves,

13. Workshop Summary Notes, Stockholm, 5-7 September 2007

emergency condensers, and the control rod drive injection system. After grid stability had been established the emergency diesel generators were secured. The cause of the event was the severe disturbance on the northeast electric grid.

- A nuclear power plant experienced an automatic reactor trip event initiated by a main turbine trip on auto stop oil. The auto stop oil turbine trip was caused by an electrical disturbance associated with the 345kV substation. Subsequent failure of a carrier power supply prevented the generation of a transfer block signal, which would have prevented the occurrence of this event. Prior to this event, the plant was operating at full, steady - state power conditions. During the unit trip the internal 5 .9kV buses were de-energised resulting in a loss of all four reactor coolant pumps. This placed the plant in natural circulation. The loss of the internal 6 .9kV buses resulted in the loss of 480V buses 2A and 3A as per plant design. All three emergency diesel generators started and buses 2A and 3A were manually energised by two emergency diesel generators. No steam generator or pressuriser safety valves lifted and actuation of the safety injection system was not required.
- A nuclear power plant experienced an automatic reactor trip initiated as a result of low reactor coolant loop flow due to the trip of the 22 reactor coolant pump breaker. The 22 reactor coolant pump breaker tripped due to electrical supply bus under-frequency caused by an unstable off-site power grid (Northeast blackout). Off-site power was lost and all three emergency diesel generators started and energised their assigned safety buses. Main feedwater isolated and the auxiliary feedwater pumps automatically started. The cause of the event was a loss of off-site power due to an unstable power grid.

An event with significant consequences to national electrical grid system occurred in United Kingdom in May 2008. The Sizewell nuclear power plant was directly affected. An exceptional loss of some 1582MW of generation within two minutes (11:34am and 11:36am) resulted in a major system disturbance. The immediate effect of this loss was to take the system out of normal operating conditions which eventually led to the triggering of automatic low frequency relays to preserve the integrity of the wider electricity system.

As a consequence some 581MW of demand was automatically shed at 11:37 a.m. This very significant generation loss coupled with the pattern of other within day losses, and in particular the level of generation loss from 2 hours ahead of real time, led to a shortage of generation, the use of system warnings by National Grid under the Grid Code and the application of demand control across up to nine Distribution Network Operator regions at any one time.

The event is currently being analysed in detail. The aim is to provide the grid operator with the detail information to further validate the findings and, as necessary, make recommendations in respect of further work required which will be taken forward through the Energy Emergencies Executive Committee and the Grid Code Review Panel.

1.4.3.5 Electrical equipment failures

This category involves failures of still different electrical equipment such as transformers (internal winding short circuit, high voltage penetration short circuits), fuses, inverters, motor short circuits, etc. It was observed that while failures of minor electrical equipment (motors, fuses, small transformers) could be easily isolated without impact on the plant electrical systems, problems with main or house load transformers may cause significant disturbances in the plant electrical systems. In addition, a fire risk is always present due to inflammable oil contained in transformer vessels. The following are examples of events involving electrical equipment failures.

- A loss of offsite power and a safety injection occurred at a plant due to transformer resistor bushings in the 22-kV isolated-phase bus simultaneously shorting to ground. This caused a phase-to-phase fault that resulted in a generator lockout followed by a turbine and reactor trip. Power supply to the 22-kV isolated-phase buses was interrupted and led to the loss of offsite power. The consequence of this event was an excessive cool down and depressurisation of the reactor coolant system and the main steam system.
- Another plant reported a fire after short circuit in the auxiliary transformer. As a result of the short circuit, accumulated gases failed the transformer tank seal and the transformer oil ignited. The plant electrical protection system isolated the affected transformer, and a fast transfer to supply safety buses from the standby transformer was actuated.
- Some plants reported events involving loss of power supply to 6 kV safety buses due to single-phase short circuit in the electrical motor. The electrical protection isolated the faulted electro-motor in all cases.

1.4.3.6 Degraded insulation

There were 11 events reported that involved problems in the plant electrical systems due to degraded insulation of electrical conductors, cables, and penetrations.

- One plant reported that during normal operation at its rated power, a short circuit incident occurred in one of the medium voltage AC buses, and resulted in decrease of bus voltage, and reduced coolant flow in one of the reactor coolant loops, causing an automatic trip of the reactor. Inspection proved a burnout on the u-v phase conductors near the connecting portion to the tie breaker due to short circuit of conductors.
- One IRS report addressed potential problems common to several nuclear power plants resulting from the failure of electrical bus bars caused by cracked insulation and moisture or debris build-up in bus bar housing. Insulation failure, along with moisture or debris, provided undesired phase-to-phase or phase-to-ground faults which resulted in catastrophic failures of buses. Another plant reported that degraded insulation resistance of the current transformer on phase A output caused a short circuit and subsequent disconnect of the main and house load transformer.

Events like the examples above show that electrical cables and connectors are amongst the electrical and I&C equipment that constitute the most limiting factors for the long term operation of the power plant. For many older units, electrical cables for equipment and motors – including the safety related equipment and motors –were insulated with PVC, without qualification, real knowledge of environmental conditions, or determination of projected lifetime. There is therefore a risk that a non-qualified cable may not be able to correctly operate under accident conditions. Hence special attention is given to the replacement of PVC or other unqualified cables with new qualified ones, or at least to run re-qualification programmes including ageing prediction. Some power plants already implemented a specimen surveillance programme for electrical cables. A cable specimen is hereby stored in the containment to simulate accumulated thermal and radiation aging. Tests are then performed on the samples as described in relevant technical reference documentations.

1.4.3.7 Circuit breaker malfunctions

Considering the fact that there are a large number of electrical breakers at every plant, the number of reported events involving failures of electrical breakers or their actuation system is actually not so significant. An electrical circuit breaker is an active component that has a limited design life.

Many plants have already replaced old, obsolete breakers (especially oil circuit breakers) by new ones (in most cases SF6) that are highly reliable and are able to open during a short circuit.

Nevertheless, circuit breaker failures – especially in high voltage systems – may cause significant disturbances in the plant electrical system.

- For example, one plant reported a serious grid power disturbance due to 220kV circuit breaker failure to reconnect the nearby coal fired plant, and caused voltage and frequency fluctuations ranging from 45 to 53 Hz in the plant electrical system. The voltage of the unit's auxiliary power buses decreased from 6 kV to 3 kV. The 110/220 kV outdoors switchgear tripped and power was lost in all 6 kV unit auxiliary power buses. All diesel generators connected to the relevant 6 kV buses.
- Two nuclear power plants reported three cases of total loss of offsite power that were caused by problems with fibre optic based control systems used to control switchyard circuit breakers. These events seemed to be caused by interference from a hand-held radio in close proximity to the tone relaying trip receivers of the fiber optic systems.
- During plant outage an explosion occurred due to the failure of a circuit breaker, and caused a fire. The failure occurred probably when the protection relay was spuriously actuated 0.12 seconds after the start of the pump (overcurrent protection) and led to the opening of the circuit breaker. Based on the event investigation following the circuit breaker failure, it was concluded that two phases of this 6 kV circuit breaker did not open correctly, producing an arc inside the housing and intense heat release.
- A malfunction of one circuit breaker located between the auxiliary transformer and the 110 kV line from outside substation led to the declaration of unavailability of the second off-site power source. Initially, an auxiliary transformer was identified as a potential cause of the event. It was replaced by another auxiliary transformer. When testing this transformer the circuit breaker failed again in two phases. The detailed analysis of associated circuit breaker however showed breakdown of the two switch chambers.

With regard to reliability of electrical circuit breakers, the US NRC published the information notice 2007-34, which addresses issues on circuit breaker failure to open/close on demand.

1.4.3.8 Voltage control malfunctions

A special category of electrical system failures relate to voltage control system malfunctions. This involves both the main as well as emergency diesel generator voltage control systems.

- One plant reported EDG problems in maintaining the required voltage after start-up, due to malfunction of the excitation system.
- One IRS report discusses how a malfunction in the main generator voltage regulator could increase generator output voltage, which could cause an over-voltage condition at the vital buses powering the electrical equipment important to safety. The over excitation was caused by a malfunction in the voltage regulator circuitry.

In most cases the plant electrical protection system acted properly and was able to isolate the over-voltage by opening the generator or main output breaker without propagating over-voltage conditions to the entire plant electrical system. However, in a situation when a generator is operating with high excitation current, a disconnection from the grid will cause a fast overvoltage transient on the generator busbar. Such an event occurred at Olkiluoto in May 2008, causing significant disturbances to the plant electrical system. Initially, the generator excitation system failed which resulted in an increasing generator voltage. The relay protection system was not set up to disconnect the generator, instead the unit breaker was tripped after a few seconds. The disconnection resulted in

the fast increase of the generator bus bar voltage to a level that caused faults in the recirculation pump intertia mechanism. The mechanism was implemented as part of the power uprating and ensures necessary coastdown time for core cooling after trip of the recirculation pumps. Instead, the recirculation pumps stopped in a second and caused temporary inadequate core cooling. This event demonstrates the importance of adequate assessment and testing when a modification is performed on non-safety related electrical systems that, if they were to malfunction, may fail an electrical system important to safety.

1.4.3.9 Electrical system design error

Design errors in plant electrical systems were also identified among other contributing factors in selected events. Design errors are mostly hidden and only revealed after the occurrence of a failure. The plant safety re-assessment using probabilistic methods may help revealing some hidden design errors.

Other possible design errors may be implemented to the plant design during modification process. It was recognised that small gradual changes of the original design, adding up with time, could invalidate the original design assumptions and safety analyses[14].

Several examples can be found in the IRS database on design errors that caused problems in the plant electrical systems. But in general, only few design errors were identified. The following are examples of events involving design errors.

- At one plant, a potential safety-related problem was identified that could result in losing a vital electrical bus by overloads caused by connecting excessive loads to the bus during a loss-of-coolant-accident. Such an overloading would actuate the bus overload protective device and the associated lock-out device, in order to prevent energising the bus from any other source including the emergency diesel generator. Similar overloading of multiple buses during an accident could disable redundant trains of safety-related equipment.
- A failure modes and effects analysis performed at a plant showed several possibilities of emergency diesel generator EDGs overloading, potentially resulting in the loss of both EDGs of a unit due to the overloading.
- A reactor coolant pump tripped by differential protection due to earth fault at cable connections. Further investigation revealed a design deficiency in the cable connection to the containment penetration in phases A and B of that pump motor.

14. DIDELSYS Workshop Summary Notes, Stockholm, 5-7 September 2007

2. ELECTRICAL DEFENCE IN DEPTH

Defence in depth is a historical concept that has been applied to assuring nuclear reactor safety from the beginning of commercial nuclear power. The concept assumes the possibility of "something" not working correctly but being backed up by some other means to ultimately assure safety. As an example, defence in depth presumes that a single component or system might fail during an actual demand. Safety is assured by assuring it is "backed-up" by a redundant component or system. In practice nuclear power plants are designed using the following general defence in depth principles:

1. Use of an inherently safe design with large safety margins to allow coping with unexpected events,
2. Use of extensive quality assurance measures to assure critical safety components function as originally designed,
3. Use of confirmatory testing and inspections to assure original safety margins are maintained through the life of the facility,
4. Use of trained personnel supplemented by good information displays, safety policies that are adhered to, and procedures to control equipment failure events,
5. Use of automatic, redundant (highly reliability) and in some cases diverse emergency protection systems to assure safety by backing up the actions of operators,
6. Use of consequence mitigation features, design margins, and siting practices to reduce or minimise the effects of radioactivity releases if the previous defence in depth barriers should fail.

One can also evaluate defence in depth of critical safety features within a nuclear power plant. We discuss this concept as related to electrical systems further in the follow sections.

2.1 Defence in depth levels

Using the same type of philosophy as applied to a nuclear power plant as a whole, the electric power system supporting a nuclear power plant can be characterised by the following defence in depth levels:

1. Use of an inherently robust electrical system designs with large safety margins against short circuits, tripping out, isolating from preferred power sources unnecessarily, or failure given voltage or frequency deviations.
2. Use of extensive quality assurance measures to assure critical electrical components function as originally designed. This would include proper identification of all voltage, frequency, and phase requirements and use of appropriate design standards.
3. Use of confirmatory testing and inspections to assure original electrical design margins are maintained through the life of the facility. This would include confirmatory qualification testing and verification of operating set-points and response times for protective equipment.
4. Operation of the electric power system by trained personnel supplemented by good information displays, safety policies that are adhered to, and procedures to control equipment failure events.
5. Use of automatic, redundant (highly reliability) emergency protection systems to assure safety with confirmatory and supplemental back up actions from operators.
6. Use of a reactor design with adequate design margins to cope with the possibility of a temporary total loss of electrical power.

One could look at events like Forsmark-1 and recognise that a lack of "robustness" in individual defence in depth barriers could result in one or more of the multiple barriers failing. By robustness we are defining an attribute of an individual defence in depth barrier in terms of its margin against failure. Each of the defence in depth barriers can individually be evaluated for their robustness.

2.2 Robustness of defence in depth

We now describe the specific features which contribute to robustness of the defence in depth barriers in electric power systems of NPPs.

2.2.1 Robustness of electrical system designs

The first defence in depth barrier considered is the inherent robustness of the electric power system design itself. Features which contribute to design margins and robustness in this area include:

1. Multiple independent (e.g.: different power ratings, different circuit right-of-ways) connections to the external electrical grid per the recommendations of IAEA Safety Guide NS-G-1.8 (or US General Design Criterion 17),
2. Properly sized and installed lightning protection, insulation, and grounding connections consistent with accepted international standards,
3. Multiple independent onsite AC power trains consistent with accepted international standards,
4. Use of minimal system dependencies and interdependencies for stand-by onsite power sources
5. Sizing of component such as batteries, diesel generators, compressed air receiver tanks, fuel oil storage with ample design margins for starting, loading, and operation.

2.2.2 Quality assurance measures

Quality assurance is a most critical defence in depth barrier. A thorough and comprehensive analysis of functional requirements is necessary to avoid the situation where redundant equipment is systematically designed with inadequate design margins against total failure. Robustness in quality assurance is credited for assuring:

1. Analyses (defining requirements used for sizing the equipment noted above) is correct,
2. Equipment procured for the electric power system meets all established engineering requirements, and conforms to accepted industrial standards to assure robust design margins credited in meeting the functional requirements.

2.2.3 Confirmatory testing and inspections

Confirmatory testing, qualification testing and continuous inspections are credited as a defence in depth barrier to:

1. Detect errors or non-conformances in initial equipment manufacture or installation,
2. Detect degradation in equipment performance over time,
3. Detect drift in actuation setpoints which are credited as a part of the design margins in the functional analysis.

2.2.4 Electric power system operation

Proper operation of the electric power system by properly trained personnel, subject to clear procedural guidance and policies contributes to robustness in defence in depth barriers that are credited to:

1. Assure the electric power system at the nuclear power plant and the electrical grid are operated within analysed voltage, reactive power (or: "var"), and frequency limits to assure that following any plant trip there will be two independent offsite circuits such as assumed in IAEA Safety Guide NS-G-1.8 (or US General Design Criterion 17).
2. Assure co-ordination of maintenance activities at both the NPP and external grid to avoid challenges that might result in a major disruption to the electric power system.
3. Assure that in the event of a major electric power system disturbance, that priority is given to restoring at least one offsite circuit to supply nuclear power plant shutdown loads.

2.2.5 Redundant automatic emergency protection systems

Provision of redundant automatic protection systems, and trained operators to serve as a backup, contributes to robustness in defence in depth barriers that are credited to:

1. Respond to electrical malfunctions which occur at a speed faster than operator actions could be credited to control
2. Prevent incorrect electrical configurations or component alignments that could severely damage electric power system components, or cause a loss of electric power to decay heat removal systems

It must be recognised that redundancy only provides robustness against the possibility of single component failures. It provides little or no robustness against common cause failures (e.g. caused by inadequately sized equipment, design or installation errors, improperly sized, maintained, or calibrated equipment). The only recognised means of assuring robustness of redundant automatic emergency protection systems against CCFs is to provide adequate diversity.

2.2.6 Adequate reactor design margins

The final means of robustness in a nuclear power plant electric power system is to have a reactor design with sufficient margins that in the event of a complete loss of electric power, there will be enough time to recover electric power. This can be accomplished by assuring large water inventories available to remove core decay heat, either as steam generator secondary side water inventory in PWRs or as water in the reactor pressure vessel above the top of the core in a BWR. In this regard, it is useful to note that in many new passive reactor designs a central design feature is the ability to safely remove core decay heat for extended periods of time without any electric power being available for forced cooling systems.

3. DIDELSYS ISSUES

In this section, the specific technical issues associated with challenges to nuclear power plant electrical systems are discussed. These issues were identified by the DIDELSYS working group during the organisational meeting at the start of the project, and include the following:

- Grid challenges
- Communication Interface between Nuclear Power Plant and the Electrical Power Grid
- House Load Operation Capability: Advantages and Disadvantages
- Power Supply Requirements for Protection and Control Systems
- Design Features of High Reliability Onsite Power Supplies
- Desirable Fail Safe Conditions
- Challenges in Performing Failure Modes and Effect Analysis
- Conflicts between Protection and Reliability
- Protection of Safety Buses
- Digital Protective Relays
- Power Supply Requirements for NPP Operator Information Systems
- Nuclear Power Plant Operators Response to Electrical Events

Each of these issues is separately discussed in the following subsections.

3.1 Grid challenges

3.1.1 Introduction and general background

3.1.1.1 General principles

The electrical grid connections to a nuclear power plant (NPP) allow operation of the nuclear power station to export power, but also provide a source of electrical power to the power station auxiliaries to allow safe shutdown and post-trip cooling of the nuclear reactor. The USNRC 10 CFR 50 Appendix A GDC-17 states that "An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents." Even though NPPs always have on-site emergency electrical supplies, (diesel generators, gas turbines, etc) the reliability of power from the grid makes a significant contribution to the overall reliability of post-trip cooling.

Faults and events on the grid system can initiate reactor trips, and may make the grid electrical supplies unavailable, or unsuitable, for providing power to nuclear power station auxiliaries. The general design principle for NPPs should be that reactor can remain safely at power for the normally expected range of variation of grid conditions, and that the reactor can be safely shut down, using its own on on-site emergency supplies if necessary, when grid conditions go outside such defined limits. Thus: *Events on the grid should not inhibit the operation of, or cause failure of, systems required for safe shutdown of the nuclear plant.*

3.1.2 Scope

This section deals with the faults and events on the grid system that can put the safety of the NPP at risk. The different general design aspects are discussed and extracts from a case study in Sweden exemplifies the dimensioning profiles of power frequency transients that have to be considered.

Issues of operational and maintenance are covered in section 3.2.

3.1.3 Grid faults

3.1.3.1 Loss of grid connection

The grid connections to nuclear power station can be lost:

- If all transmission circuits connecting the nuclear power station to the rest of the grid are lost, by faults on those circuits or on the local switchyard (substation)
- If there is a blackout affecting the national or area grid system.

The loss of all grid connections to a nuclear power station may result from a variety of causes:

- Adverse weather causing faults on overhead lines and outdoor switchyards (e.g. multiple lightning strikes, flashovers in freezing fog, very high winds etc)
- Catastrophic failure of items of transmission equipment
- Third party actions (e.g. excavation works damaging underground cables, fire or smoke in the vicinity of overhead lines, cranes under overhead lines)

- Human error (switching out the wrong circuit, incorrect protection setting) which may occur simultaneously with planned transmission circuit outages.

The frequency of loss of grid connections can be estimated, and will depend on the number and length of transmission circuits connecting to the power plant, the weather conditions affecting those circuits, and the policy of the grid operator for maintenance and maintenance outages. Expected frequencies can vary between once every couple of years, to less than once in the life of the power plant.

The nuclear power plant safety case should take account of the expected frequency of loss of grid events. The loss of grid events may be "total" (i.e. affecting all electrical connections to the power plant) or it may be partial (i.e. affecting just the grid connections to the generator but not the grid connections to the auxiliary supplies or vice versa.). The safety case should account for both possibilities. It should also be considered that a loss of grid event may occur following a period of degraded grid conditions (low voltage and/or low frequency) as described below.

3.1.3.2 Over-voltages from lightning and switching

Even if design base information on over-voltages from lightning and switching seldom is missed out for the prime power plant components like main transformer and main generator it is important to point out that the rating of mitigating components, like surge arresters, should be co-ordinated with the rating of the insulation for all components directly or indirectly connected in the circuit.

Solid state components in particularly often require an additional over-voltage protection in addition to the busbar mounted surge arrester rating.

When power systems are modernised the original specification of insulation coordination might not be documented with adequate detail. Higher over-voltages than before might be generated under certain fault conditions or certain modern components might be more sensitive.

It is of course important that equipment in class 1E systems is not affected. However, also non 1E equipment must be considered from this point of view as a failure in non 1E equipment (e.g. relay protection), could lead to electrical transients, detrimental to 1E equipment.

Over-voltage protection build into solid state based equipment often are quite limited in their energy rating, such over-voltage limiting components and circuits (e.g. SCR Crowbar Over-voltage protection circuits) have to be checked for their ability to sustain possible electrical transients that could be generated due to component failures, as discussed below.

3.1.3.3 Power frequency and voltage transients and large variations

Most grid systems have a requirement for power plant to be able to operate for a defined range of voltages. A typical requirement is to be able to operate indefinitely at full power for ± 5% about nominal voltage and to operate, possibly at reduced power for a limited time at ± 10% about nominal voltage. In addition, the plant should ride through sudden step changes in voltage (which may arise from switching transmission circuits etc). A typical requirement is steps of ± 6%. For most grid systems this encompasses the full range of variation of grid voltage that is possible without voltage collapse (brownout). Nuclear plants should be designed to meet these grid requirements.

It should be noted that extremes of grid voltage could occur at the same time as extremes of grid frequency (in particular low voltage together with low frequency). The nuclear plant should be designed to meet these extremes simultaneously.

The generating unit(s) in a nuclear plant assists in controlling the local grid voltage, consequently, tripping a reactor and its associated generating unit is likely to cause a change in local grid voltage. In particular if a reactor is tripped because of a low grid voltage, the local grid voltage will fall still further. System studies of the nuclear plants should take this into account

Voltage transients induced from the grid

Faults on the grid system (e.g. lightning strike on overhead lines, flashovers due to freezing fog, third-party contact with live conductors) will not only lead to the risk of initial fast over-voltages, e.g. lightning over-voltages, but will also lead momentarily to low power frequency voltages on one, two or all three phases near to the point of fault, until the electrical protection switches out the affected circuit. If the protection systems work correctly, the fault will typically be cleared in around 100 ms. During the fault, the grid voltage local to the fault is likely to be depressed to less than 20% of nominal on the affected phases, generally recovering to better than 90% on fault clearance, and back to around 100% of nominal in a couple of minutes. Faults of this nature are reasonably common on grid systems, and it is a common grid system requirement that power plants should ride through such faults and not be tripped by them. In many countries also NPPs should be designed and to meet these grid codes.

In the event that a short circuit is not cleared by the primary electrical protection on the grid system (protection failure, or failure of circuit breaker to open) the fault will probably be cleared by the back-up protection. In this case, the fault clearance time will be much longer (typically 300-800 ms, depending on the system design and features). A slow-cleared fault of this nature would be a rare event on a grid system, and it is not a grid system requirement for a power plant to be able to run through such faults without tripping.

However, with modern relay protection and modern breakers a shorter back-up protection clearance time can be achieved. For example: the Swedish grid system design is in general able to manage a back-up protection clearance time (backup protection time plus breaker opening time) of not more than 250 ms.[15] The Swedish grid code also stipulates that nuclear power plants should be designed to ride out also this challenge.

During such a fault the generator cannot deliver the full power given by the turbine. Still the turbine-generator should not be allowed to accelerate more than that it still is in synchronism with the grid when the fault is cleared. This is a challenge for the turbine controller but also for the generator voltage controller.

The resulting initial transient voltage dip is therefore sometimes followed by a relatively slow (0,5 - 1 Hz) damped oscillation in generator power and voltage which magnitudes are dependent of the characteristics of both the grid, generator and turbine controller.

It is therefore important that the design of the NPP turbine generator system dynamical performance is verified using relevant grid parameters and grid models.

If an oscillatory post transient power and voltage variation can be generated it is important to investigate if this has any effect on the safety of the reactor process. For example BWR units often have inherent core instability in the same frequency range, which must not be entered by the electric power or voltage variations.

Frequency variations induced from the grid

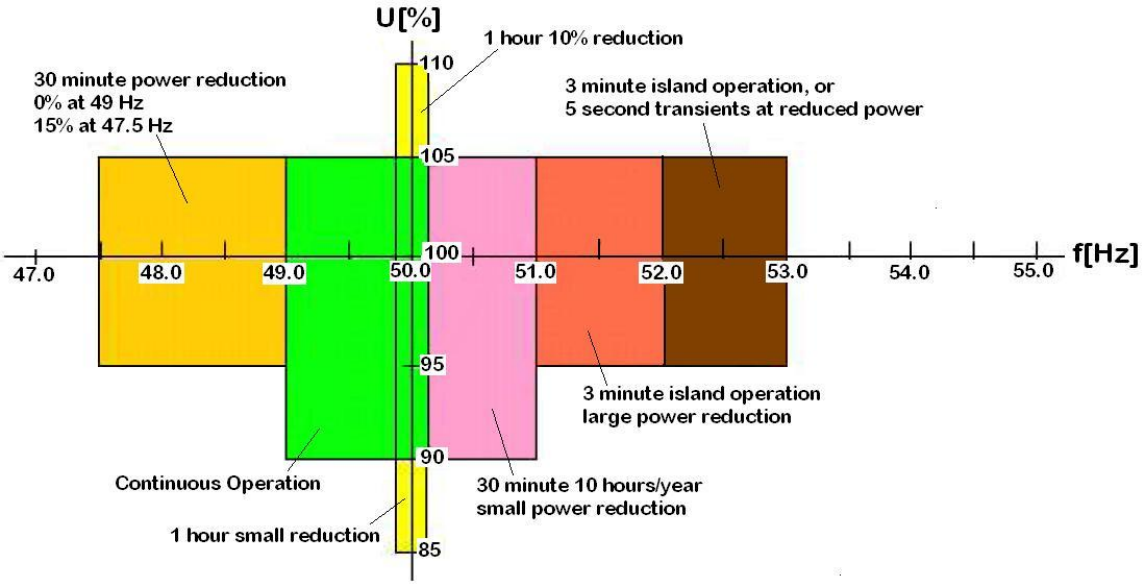
15. A shunt fault accompanied by a stuck breaker pole is permitted to have “regional consequences” (per Figure 4.3 of the Nordic Grid Code). The requirements on the NPPs to remain connected to the grid in the event of a stuck breaker is subject of current discussions between Sevenska Kraftnät (SvK) and the owners of Swedish NPPs.

The frequency of the grid system (60 Hertz or 50 Hertz) input varies slightly throughout the day with variation of demand[16] and events leading to tripping of generating units. Most grid systems have a requirement for power plant to be able to operate for a defined range of frequencies. A typical requirement is to be able to operate indefinitely at full power for ± 1% about nominal frequency and to operate, possibly at reduced power for a limited time at ± 5% about nominal frequency. For most grid systems this encompasses the full range of variation of grid frequency that is possible without grid collapse (blackout). A nuclear power plant should be designed to meet these grid requirements.

The frequency will change relatively fast if for instance large production units are lost or national or international transmission lines are disconnected. However, the spinning reserve shall be dimensioned to counteract loss of the largest production unit or transmission line in a relatively short time (20-30 s). If the NPP cannot sustain the scenarios, the problem will escalate and the grid will separate leaving large areas in a black out situation. Systems of automatic load shedding might save a severe load unbalance before the NPP under-frequency protection disconnects the NPP from the grid.

Typically the NPP shall sustain up to 5% reduction in frequency for more than 30 min. In the Scandinavian area the frequency/voltage operating limits are given in the NORDEL Grid Codes as shown in Fig. 3.1.3.3-1.

Figure 3.1.3.3-1: Frequency/voltage operating limits based on NORDEL grid code



Reductions in frequency are a safety concern as safety related pumps might not deliver sufficient flow when the frequency is low, especially combined with a low voltage. This consideration is also important for PWR reactor coolant pumps.

In particularly when safety grade loads are modernised the proper coordination between the load capability and the relay protection must be assured. As for all other excursions outside the permitted voltage-frequency range the safety grade load should be switched over to be powered from the EDGs.

Voltage variations induced from the grid

A large number of reasons might cause voltage variations on the grid. Transmission lines can be disconnected due to faults or due to operational reasons as discussed above. When the subsequent

16. The standard deviation of system frequency is about 40mHz in the NORDEL system. It is even smaller in the UTCE and the North American systems.

load changes occur not only the frequency changes, the voltage also changes. The NPP generator voltage controller, if in automatic voltage control mode, will try to compensate for the change within its capability but might not succeed.

A situation of low grid voltage, combined with that the generator is set up to produce maximum reactive power and therefore high generator voltage, is particularly difficult as the NPP auxiliary power is often drawn from the generator busbar.

Situations of high voltages might occur which are potentially dangerous for the equipment. Even if standard power components like motors and transformers are quite resilient to exposure of over-voltage for shorter periods of time, power electronic equipment might be much more sensitive. Solid state equipment often has built-in active protective actions, like blocking of firing pulses, when abnormal voltages are detected. Such built-in protection often shuts down the equipment within a narrower operational span in both voltage and time, than the traditional relay protection setting. This type of built-in protection might be unknown by the NPP end user. If Class 1E equipment shuts down in this way and stays blocked, safety functions are put in jeopardy. This was what happened in Forsmark 2006 where an over-voltage on the non-Class 1E busbar transferred to the DC side of four redundant Class 1E UPS with a sufficiently high voltage level for two of the four UPS systems built-in over-voltage protection to block the UPS inverter.

Situations of low voltage might also be equally undesirable. A low voltage will lead to abnormal high currents in motors. Starting torque might also be too low for the motor to start properly. Both situations might lead to a condition that the motor relay protection is actuated and the motor is permanently disconnected.

Situations of extended periods of extremely low grid voltage might occur. Particularly the break point when the under-voltage protection should act and Class 1E supply connected to EDGs should be looked at.

If the change-over fails, which could occur due to a fault in a single non 1E equipment, nominal voltage will not be present to supply the Class 1E loads.

As pointed out in the subsection above it is important to consider the potential common cause failures (CCFs) of Class 1E equipment due to variations or faults in the Class 1E power supply.

Subsynchronous resonance

In power grids with series capacitors the generator turbine might come in resonance with the grid and developing a torsional oscillation between the shaft ends. Fatigue in the generator turbine rotor might cause missiles. The protection equipment shall preferably disconnect or reduce the series capacitance and as a back-up disconnect the NPP from the grid.

However, this problem is not primarily a reactor safety concern although voltage variations will occur as part of this phenomenon.

Voltage and frequency transients and variations induced from the NPP

One potential issue concerns rate of change of frequency. If a nuclear plant is separated from the grid in house load operation, or islanding on a regional small local, then its local frequency might rise rapidly, controlled only by the speed governors on its generating units(s), typically to less than +5%. If there is a governor fault, then frequency could rise to a figure determined by the setting of the overspeed protection (as high as +10% with mechanical overspeed trips).

Fast transients of over-voltage in the auxiliary system of the NPP will occur when the generator, supplying power to the grid, suddenly is disconnected from the grid. A high load and level of excitation of the generator will generate a high over-voltage and frequency. Even if the NPP is not

built to operate in house load operation, and thus disconnect auxiliaries from the generator busbar on a voltage excursion, the initial over-voltage transient might disable the Class 1E loads.

Several different scenarios, for instance: with faults in the exciter, voltage regulator, etc. have to be considered. In May 2008, at Olkiluoto, a fault in the exciter thyristor bridge, suddenly applying maximum excitation, generated a fast rise in generator voltage. When the unit breaker opened a voltage transient of more than 150% was experienced on the generator busbar. Damage on Class 1E busbar loads has not been reported from this incident but the unit experienced a transient dry-out due to damage on all reactor internal pump variable speed drives.

Under-voltage situations might of course also occur. The more difficult cases are gradual voltage reductions in isolated buses that could disable multiple safety systems.

3.1.3.4 Specific design considerations

As a base for calculations all possible faults in equipment, including the relay protection and inter-protection communication, have to be considered as well as spurious opening of the unit breaker or stuck breakers. As pointed out in section 3.3 "Advantages and Disadvantages with House Load Operation", NPPs with house load capability have more scenarios to consider than NPPs without this capability. However, NPPs which will not transfer to house load are therefore not automatically excluded from possible transients.

As the grid system configuration and parameter values do vary the set up of the calculations has to consider the worst case for each specific case. The highest grid short circuit might for instance not always generate the most difficult profile. As the transformers often have variable tap settings the most unfavourable position should be assumed. If the design assumes a specific tap setting (off load) the plant real value should be checked and administrative procedures enforced to prevent a change in the plant. It is also important to systematically review the calculations when design changes in the power equipment or in relay protection are made in the grid or NPP power system, or when putting in modernised equipments or components.

All possible auxiliary power supply sources potentially powering the Class 1E busbars should be considered, typically:

- Main generator connected to primary grid (off-site power) interface
- Main generator only (plants with house load operation capability)
- Primary grid (off-site power) interface only
- Secondary grid (off-site power) interface only
- Alternative off site power dedicated generator (e.g. Station Black Out gas turbine or diesel generator)
- EDGs
- All possible combinations of the above, within the specific NPP scheme. Generally the worst case alignment is with the plant producing full power and the emergency diesel generator synchronised to the grid for test.

It is important to consider that safety grade loads primarily powered from the offsite grid or main generator are potentially subjected to several faults in the non-Class 1E equipment. The CCF risk might come from failure in a single non 1E equipment or a CCF in several identical types of non-Class 1E or Class 1E equipment, depending on the power system scheme. If for example an auxiliary or unit breaker fails to open or if an under-voltage relay protection fails to act, all safety grade load might be stuck on an inadequate supply or a supply with a dangerous high voltage. Hence back-up protection or other types of diversified designs must be employed where CCF cannot be ruled out.

The NPPs safety systems should be able to operate as intended following rapid rises or falls of voltage and frequency. Assuming that the NPP non-Class 1E and Class 1E busbars are powered via the generator all loads have to be able to withstand the transient. No damage on Class 1E equipment must occur and no 1E relay protection or internal equipment protection must be actuated rendering Class 1E equipment inoperable. For example, motors and transformers will exhibit a high current, like a start current, when the voltage returns after a dip.

Also the reactor, turbine and generator controllers must be able to handle the initial transient and the following post transient phenomena without causing a reactor or turbine trip.

And even though a nuclear plant may ride through such a fault without tripping and without any effect on essential electrical systems, a lot of "non-essential" electrical systems may be affected which may cause problems for the plant operators, and that is a potential safety issue.

Defence in depth thinking should therefore be applied resulting in ample margins in both non 1E and 1E system designs**.**

3.1.4 Oskarshamn NPP case study

Since year 2000 a number of power system studies of Units 1, 2, and 3 of Oskarshamn have been performed. The generator voltage had been studied during three-phase short circuits in the grid with both correct operation and failure to operate of the power system protection. After the incident in Forsmark 2006-07-25, studies with Oskarshamn 3 were carried out on phase-to-phase short circuits and single phase ground faults in the grid and inadvertent breaker operation of the circuit breaker at the high voltage side of the step up transformer. The requirements according to grid disturbances in the Safety Analysis Report (SAR) for Oskarshamn 1, 2 and 3 were assessed and up-dated. Depending on the difference in parameter values for the NPP power systems of the units it is not possible to find one dimensioning event for all type of transients. With the background of this, the dimensioning profiles have been determined. Appendix C describes the type of transients assessed.

3.1.5 Conclusions and recommendations

- The susceptibility of the power system from all available grid faults, followed by single failures such as stuck breaker, failure of protection system, voltage regulator, or other non safety system failures, shall be assessed. Comprehensive analysis of possible transients in the power system, using verified models and methods, are strongly recommended.
- The susceptibility of voltage and frequency transients and the acceptable voltage and frequency limits have to be assessed to confirm that 1E electrical equipment (UPS and others) will be protected against unacceptable conditions and that recovery procedures are in place for emergency conditions.
- Safety related electrical protection systems shall be evaluated to ensure priority for nuclear safety in relation to continuity of power operation and market advantages.

3.2 Communication interface between nuclear power plant and the electrical power grid

3.2.1 Introduction

This section will discuss technical and organisational aspects about the operation of the interface between a nuclear power plant (NPP) and the electrical high voltage power grid. It will take into account main parameters like electrical power and frequency, reactive power and high voltage limitations on the one side and general reactor mechanical and control items on the other side. With upcoming changes in the marketing, legal frameworks, and electricity markets, organisational items have to be reflected too. New phenomena in the electrical high voltage grid like major power flow changes introduced by less predictable energy production from wind parks or new market trends have an influence to all grid nodes with greater impact on NPPs.

3.2.2 Scope

In general, the interface between a NPP and an electrical grid is an interface which has a high relevance to each other in terms of nuclear safety, national infrastructure, and commercial aspects. The following part will handle only safety aspects. From this point of view four different cases have to be considered. Case 1 is "normal operation", case 2 "start-up and shut-down procedure", case 3 "alarms and disturbances" and case 4 "planned maintenance and other types of work at the point of connection". For example, details and values we mention are typical settings of Swiss NPPs which are boiling water reactors (BWR) and pressurised water reactors (PWR). The situation may be slightly different in other countries.

It is assumed here, that NPPs are generally used for base load operation to stabilise their operating parameters. If they are used for load following additional requirements will apply. Of course NPPs by design are capable to vary the production level from zero to full load, but this is designed mainly for start-up and shutdown cases. In normal operation mode it is unusual to vary the production level without technical need; this also avoids mechanical stress to the components, unbalanced fuel burn up and waste production from de-boration and is therefore beneficial for safety.

Despite these facts, it is possible for NPPs to adjust their production level within a range around 100% load. This range is limited on the upper side by maximum thermal limit and on the lower side partly by control algorithms which are optimised for around 100%. To operate a NPP in a load following mode or even in a system service delivery mode (control energy and reactive power) becomes a more important issue in a de-regulated energy market environment. NPPs like other power plants have to qualify for grid operating parameter compatibility (e.g. frequency and voltage quality parameters). NPPs are also capable to deliver and receive reactive power in a limited range, which today is made use of to stabilise the voltage. Extension of voltage range will become marketable reactive power and it would need further consideration to analyse its impact on plant systems associated with nuclear safety.

Now it is not common for NPPs to act as a primary control for frequency node on the grid[17]. On the one hand most NPPs will not cope with the necessary power gradients and on the other hand because this would mean to quasi remote control of the NPPs from the grid. The control of reactor power output from an unlicensed transmission system operator (TSO) may need further evaluation to identify if this can be done within acceptable protocols. The case is similar for secondary control energy but with some more relaxed gradients and remote control by the transmission system operator

17. One exception is in Belgium where NPPs are used for primary frequency control. The reactors used for this are operated at between 97.5 – 100% rated core power and primary system parameter variations have not been significant.

(TSO). Technically it might be possible for NPPs to act as a tertiary control power node in the grid. But this would mean to set up the defined control procedures also within the NPPs main control room (MCR) and to train the staff. The tertiary control power has to be delivered within 15 minutes for NPPs. This procedure will add mechanical stress to the plant and absorb operating shift resources. Furthermore, to run the NPP in a more flexible production mode would mean to shorten plant live expectation and increase maintenance. It would also mean to extend the physical core calculations and open the range for end of cycle (EOC) parameters.

Nevertheless there are impacts from the energy de-regulated market to the NPP introduced by the legal framework. Generally grid ownership has been transferred to TSO. Therefore, the maintenance and operational activities have to be closely co-ordinated between grid owners and NPP operators. This definitely will trigger to review the operational procedures for the interface.

3.2.3 Issue-specific section

Hence we consider all four cases which should be part of the operational procedures to handle the interface of NPP with the grid. An example of the Swiss practices is listed below:

In the case of normal operation: The TSO will electronically acknowledge daily (normally until 15.30) the power program for the next day from the requesting energy parties. As commonly a NPP belongs to a power plant portfolio, the plant portfolio manager (PPM) will do this daily scheduling to the TSO.

The power values from the NPPs (which are base-load operated) are normally transmitted well in advance (long-term power program according to cycle planning) and (especially if there is a deviation from the long-term scheduled power program) once per week (on Friday) for the next week to the portfolio manager as well as to the TSO.

Values and direction of reactive power is given from the TSO. Depending on the plant, there are limits for inductive as well as for capacitive power. These limits are different for full power and for partial load. Supervision here is done by the NPPs power recorder. There are also limits from the maximum voltage level in the high voltage switchyard (e.g. the 400kV collecting bar not higher than 420kV) and the generator excitation current.

In the case of start-up and shut-down procedures: The NPP's operating department informs the PPM 36 hours before power change by fax or telephone about reason and schedule. At least one hour in advance to the power change, the NPPs shift supervisor informs the PPM by telephone. The PPM has to confirm the value of the power change. Each phase of change has to be confirmed separately. In the case of an amendment the chief of shift informs the PPM about the new schedule. If time for amendment will overflow 36 hours, a new registration has to be made by the NPP. In case of an interrupt during the power modification the PPM has to be informed immediately by telephone concerning the next actions. This whole procedure goes within the portfolio owner's organisational unit. The PPM has to cope then with the TSOs scheduling procedures as mentioned above.

In the case of sudden power reduction or trip: The NPP's chief of shift informs by telephone the PPM about the reason and the difficultness of the disturbance. The same has to be done after the situation analyses and the calculation of the estimated disturbance time. As soon as the NPP is ready to restart, the NPP's operation department informs the PPM about the details of the start-up procedure. Here again the PPM has to comply with the TSOs scheduling procedures.

In the case of an unstable high voltage grid: in such an emergency case the TSO can by telephone require the change of the NPP's effective power. The NPP has to confirm such a request. For NPP's working in 100% base load operation only the reduction of the effective power is relevant. Before such a reduction the NPP's operating department has to be informed (or the engineer who is in

stand-by for emergency duties, if it is off-time). The reduction has to follow a defined gradient and if possible it has to be limited to a power value.

In case of switching activities in the high voltage grid area there are general requirements. For planned shutdowns of parts of the NPP's grid area, the NPP's electrical department needs a notification inquires with a minimum of eight days in advance to approve the switching. With acknowledgement of the operating department this request goes to the PPM and the grid control station (currently, the portfolio owner but in future it might be with the TSO). The authorisation for the switching activities in the high voltage switchyard – including work description and responsibilities – is given by the grid control station and confirmed to the NPP and the PPM. The NPP reconfirms the work activities not later than 36 hours before execution. During business hours this procedure can be deviated by direct requesting via telephone to the grid control station with concurrence of the PPM. Furthermore, the work in the high voltage area requires the the NPP has to order for earthing (grounding) switch "on" or "off" in written form (fax or courier) to the grid control station with due concurrence of the the NPP's electrical departmentThe people who are approved for the working are well defined and have to have a special authorisation for each task. The completion of the work has to be verified and recorded. There is a list of material at a designated location for maintenance on the high voltage grid including voltage tester and grounding cable, and the form for the required registration and fax.

The switching off procedure for the main grid connection starts with the verification if disconnecting of the NPP is permissible and if the grid control station is notified. Then the transfer for house load operation from the second grid takes place. The opening of the main circuit breaker is performed after communicating from NPP to the grid control station. After opening of the isolators, earthing must be done after verifying if the system is voltage free (this does not replace the working earth). Depending on the switching reason additional safety actions are required, e.g. additional earthing. Also note that the key "release for the local actions on the 400kV unit switch" is available only in the NPP's main control room and is allowed only if the generator breaker is off or by switching network operation.

The specific "switching on" procedure for the main grid connection starts with the check if connecting of the NPP is permissible and the written information to the grid control station is transferred. After switching "on" the isolators and confirmation to the grid control station, the block main circuit breaker is switched "on" by the grid control station. Depending on the situation switch-over from the auxiliary power takes continues and completion of procedure is registered in the checklist and it is stored for at least 2 years.

In the case of disturbances within the high voltage grid area the grid control station has to be contacted immediately by telephone with concurrent notification to the NPP's operation and electrical departments. These departments are responsible to make decisions for the next steps.

The USA approach to these conditions is covered in NUC-001.

3.2.4 Conclusions

Summarised points for the "Interface NPP – Grid":

- A detailed coordination paper including all cases of operation modes is necessary.
- This paper shall include administrative protocols and technical requirements. For maintenance within the high voltage grid area a safety action table is necessary (which includes e.g. generators with its breakers, block transformers with its cooling system, current and voltage transformers, transmission lines, etc.).

- The staff authorised for any switching actions shall be duly identified and certified for the performance of this task. The communication between NPP and the involved parties shall be affirmed through fax and telephone or other secured means.
- Independent verification is an important part for success.

The following recommendations are of immediate interest for de-regulated energy markets:

- With ongoing changes in the energy landscape, review, periodic approval, and training of such communication and interaction procedures are even more important.
- All design, maintenance and operational activities affecting the zone of influence of NPPs or grid have to be planned, co-ordinated and executed with mutual agreement from the respective authorities.
- The recovery plan for the grid after brown or blackout should include priorities for NPPs and other essential high priority facilities.
- Offsite power supply to the NPPs should remain as priority in order to preserve nuclear safety under unanticipated power outage situations.

3.2.5 References

1. UCTE operational handbook v2.5/20.07.04 with its chapters and appendices *www.ucte.org/resources/publications/ophandbook/*.
2. Swiss transmission code 2008, v1.0/13.06.08 *www.swissgrid.ch/activities/market_customer/transmission_code/docs/Transmission_Code_2008_v1_0.pdf?set_language=de*
3. NUC-001-1 Nuclear Power Plant Interface Conditions – NERC[18] (02.05.07) *www.nerc.com/files/NUC-001.pdf*

18. North American Electric Reliability Council

3.3 Advantages and disadvantages of house load operation capability

3.3.1 Introduction

The capability for power plants to operate completely isolated from the grid only supplying its own auxiliary power, often referred to as house load operation, is generally implemented on conventional plants worldwide.

In case of severe grid disturbances or other problems with the offsite power supply the plant can be isolated from the grid but kept on stand-by. This capability allows fast reconnection and thereby the prompt recovery of an unstable grid and is therefore often imposed by the energy regulatory grid codes or the Transmission System Operator (TSO). The power plant owner benefits from the higher availability and the probability of selling more energy. However, regarding Nuclear Power Plants (NPPs) the requirements and practices differs from country to country, e.g most European NPPs have this capability (which is sometimes required by the regulator) compared to approximately half of the units in Japan and no plants in the USA[19] exercising this capability.

It shall be noted that some grid codes (predominantly European) in general also put requirements on NPPs to sustain, without tripping, a near-by power line short circuit cleared by the primary line protection[20] (disconnecting one of two or more parallel outgoing lines). In this case the turbine-generator should not be allowed to accelerate without losing synchronism with the grid when the faulty line is disconnected.

The power operation of NPP insensitive to grid disturbances and equipped with house load operation capability is favourable from a grid operation point of view. On the other hand house load operation capability increases the cost of the NPP and will generate transients in the onsite electrical system, which are potentially unfavourable from a reactor safety point of view.

In the 2006 Forsmark incident, two out of four redundant safety grade UPS systems tripped due to a voltage transient that followed from a switchyard short circuit with complications from related control system failures. The experiences from this event highlighted certain aspects of the design of the NPP electrical system where flaws might be hidden, and relevant to both plants with or without house load operation capability.

19. Although Palo Verde Units 1, 2, 3 were originally designed with the capability to ride through a full load rejection without reactor trip via a fast reactor power cutback system and properly sized main condenser and steam bypass control system – *the capability has never worked successfully* because of either reactor protection system trips being generated by abrupt sensed changes to core power distribution.
20. This is the classical "n-1" criterion.

3.3.2 Scope

This section addresses the benefits and risks of NPP house load operation capability from an electrical system and reactor safety perspective. The discussion is focusing on the electrical system behaviour.

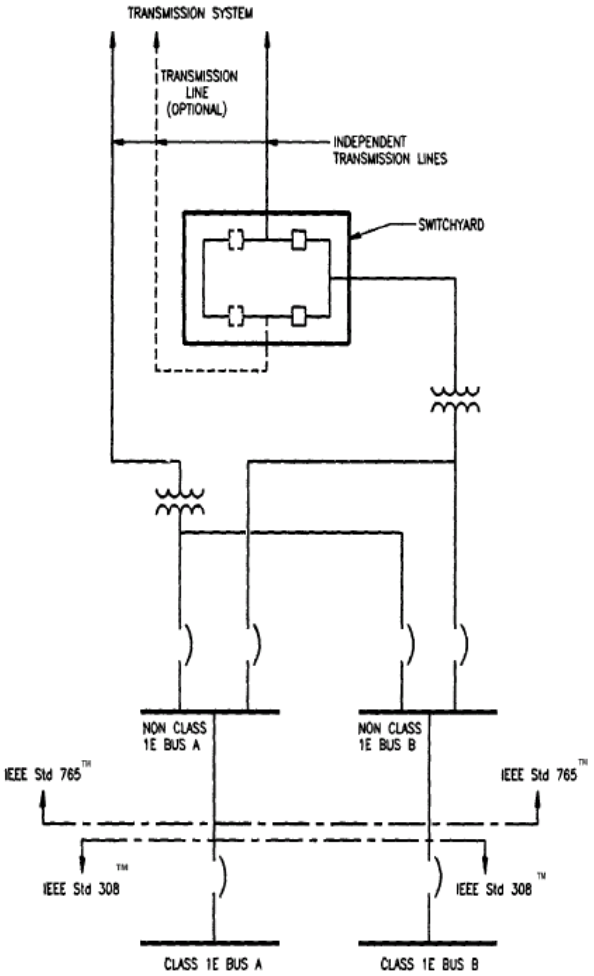
The most commonly used electrical system designs and plant types are used to discuss the potential problems. Possible impacts on non-electric process equipment and systems are only indicated.

The wider issue of NPPs participating in a regional island feeding a local areas while broken off from the rest of the grid (often referred to as a regional islanding), is not discussed. However, it shall be noted that the designation "islanding" in some cases (predominantly in North America) are used as a synonym for what more commonly and in this paper is called "house load operation".

3.3.3 General design structure of NPP electric power systems

The basic typical structure of the NPP electrical systems is illustrated in IEEE Std 765-2002 (Standard for Preferred Power Supply for Nuclear Power Generating Stations) Fig. 3.3.3-1.

Figure 3.3.3-1: Acceptable preferred power supply from IEEE Std. 765-2002



In NPPs designed for runback to house load operation, a main generator breaker is generally preferred[21] in order to facilitate a full flexibility in supplying auxiliary power from either the normal offsite circuit or the turbine generator or both. In a situation of grid disturbances the NPP unit can therefore quickly come back to powering the grid.

Key design features to allow this capability include: the sizing of the main steam turbine condenser, steam bypass (and/or atmospheric dump) valves, and the design of the turbine and reactor controls to accomplish the runback to house loads. Additionally, the electrical control system should be capable for responding to a mode transfer that involves 100% power generation to approximately 5% power for house load operation. Additionally, the design of the relay protection system tripping logic and phasing systems are more complex.

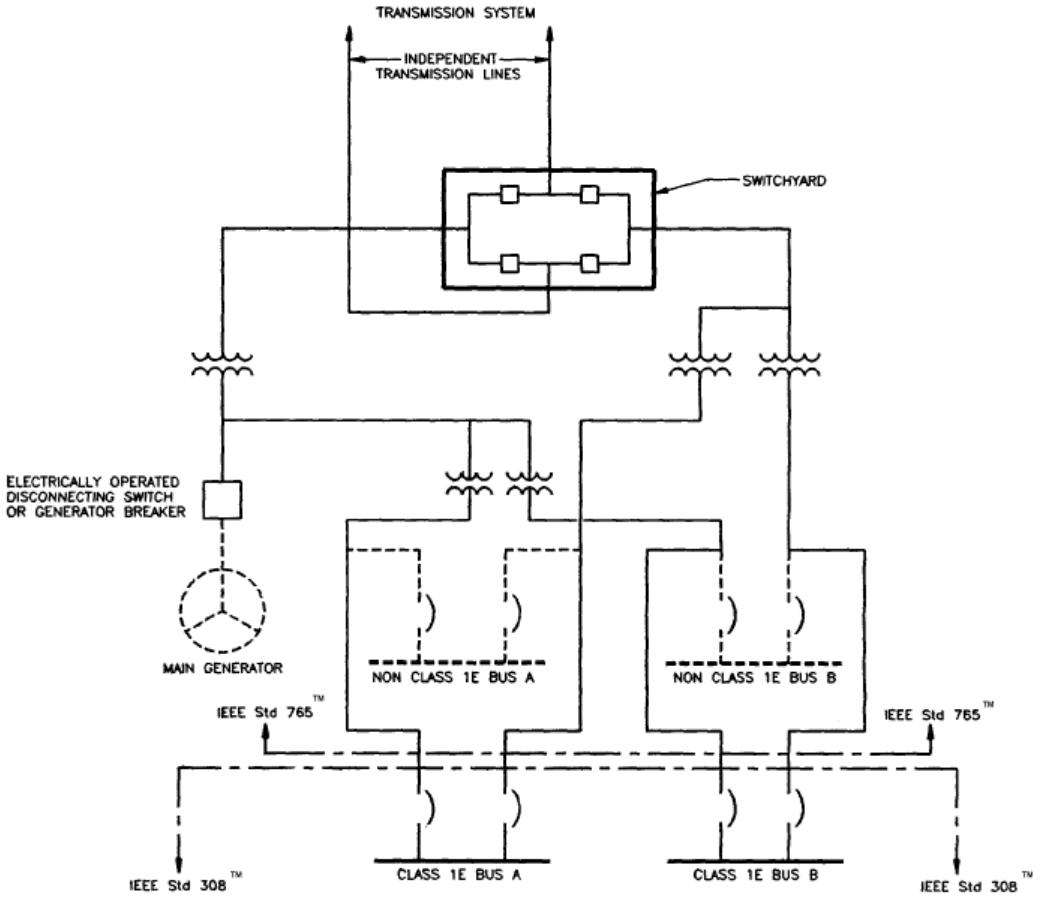
In NPPs not designed for house load operation a main generator breaker is not required. In a situation of grid disturbances the NPP unit is disconnected via the unit breaker(s) on abnormal voltage or frequency. The turbine and reactor are tripped and the generator is shutdown without any stringent requirements on control systems and turbine condenser. A few US nuclear stations are designed to reduce reactor power rapidly through a reactor power cutback system and to keep the reactor at 40-50% power with all plant auxiliaries powered by the alternate offsite power with the steam dumped to the condenser. This approach provides the flexibility to return the main generator to power without further delays as soon as the grid conditions permit.

In both types of plants the Class 1E busses are normally fed via the non class 1E bus and automatic fast or slow bus transfer systems secures the alternative power supply to the non 1E buses. If the voltage on the generator busbar is not adequate the backup power is provided through the emergency diesel generators.

It can be noted that the IEEE Std. 765-2002 alternative, with a direct primary feed of the Class 1E busbar from the alternative offsite preferred power supply circuit is one approach to improve availability of external power supply to the safety buses. This is shown in Figure 3.3.3-2.

21. Runback to house load operation can be accomplished without a generator breaker design. The main advantage with the generator circuit breaker design is that the generator can be disconnected from the grid without affecting the auxiliary power supply.

Figure 3.3.3-2: IEEE Std. 765 alternative preferred power supply



3.3.4 General NPP process system considerations

The abrupt load reduction during a transfer to house load operation puts stresses on several of the NPP systems. The main problems in achieving house load operation is in the management of excess power from the reactor, not absorbed by the turbine-generator, should be dumped as steam to the condenser. The main condenser and /or atmospheric steam dump valves (in PWRs) has to be adequately sized and equipped.

The generator busbar voltage and frequency will initially increase as the load drops of. This will tend to increase the speed of motors and pumps which will affect the fluid dynamics and the related core heat transfer and core reactivity effects.

Margins in process variables and design of components have to be sufficient to cope with the electrical and fluid system excursions. This is particularly the case in the PWR where the increase in Reactor Coolant Pump speeds will lead to an increase in reactivity and the consequent thermal output.

In BWRs, it could cause a potential risk of instability when the reactor coolant flow is rapidly reduced as a consequence of Reactor Coolant Pump (RCP) run-back.

In order to cope with the transient the reactor and turbine control systems have to function smoothly and well synchronised.

The following main control systems are involved in BWRs and PWRs:

- reactor pressure controller (BWR)
- reactor level controller (BWR)
- pressuriser level control (PWR)
- steam generator level controller (PWR)
- turbine speed governor
- turbine pre-heater and drain tank level controllers
- main generator voltage regulator
- reactor power regulation
- steam bypass
- feed-water flow control

The inevitable electrical transient that is generated when transferring to house load operation puts added strain on the process systems from several electrically driven components. This includes reactor safety system components which might be in service during normal operation, e.g. component cooling pumps and PWR charging pumps. And there is an additional possibility of a further electrical transient if an ongoing transition to house load operation has to be aborted due to electrical or process system failures.

It is therefore important to point out that the process components dependency on electric system variations has to be well known so that the overall process behaviour during electrical system transients or faults can be modelled and managed with precision in a brief period. The power uprates and modernisations of process equipment could give rise to an increased risk from the loss of original design margins and introduction of new failure modes.

Electrical system performance may also change when modernised due to that modern electrical equipment often includes modern type components, e.g. solid state power converters and software based processor controllers. Because of this change in technology the specified functionality needs to be extended beyond what was listed for the original components. This applies both to areas of functionality which was inherent with old technology and therefore not explicitly specified in the original design basis and new areas of functionality which inherently comes with the modern technology.

In order to maintain control on the overall plant performance the knowledge and facilities to understand the integrated electrical and process system behaviour needs to be maintained, as changes in component and system functionality are more or less inevitable when modernisations are performed.

3.3.5 Electrical system considerations

3.3.5.1 Units designed for runback to house load operation

The runback to house load operation in principle starts when the unit breaker gets a trip signal or signals to open provided there is no fault signal from within the power plant.

Often the reason for the unit breaker to open is a short circuit somewhere in the offsite substation or in the nearby grid which cannot be cleared or is not properly cleared by the line protection. Typically the unit breaker is tripped by an underimpedence, over-current relay and in the case the under-voltage remains beyond the anticipated breaker failure protection clearing time (typically 250 ms), an under-voltage protection initiates unit breaker opening and subsequent transition to house load operation. Hence the generator busbar voltage might already be far below the normal operating range when the transition starts.

Subsequently, the generator excitation may be giving full excitation current before the unit breaker opens.

However, the reason for the unit breaker to open is often a short circuit somewhere in the offsite substation or in the nearby grid which cannot be cleared or is not properly cleared by the line protection.

The turbine–generator speed might also have started to be affected somewhat, as the load from the grid changes faster than the turbine governor can follow. Assuming an initial grid short circuit the load of the generator decreases as the voltage on the grid is lowered substantially (e.g. determined by the arc-voltage) and the generator current is not increased to the same extent. Consequently the turbine-generator starts to accelerate as the mismatch in power over time is taken up as increased rotating energy in the turbine-generator rotors. However, the major part of this mismatch in power (frequency increase) occurs after the transition to house load operation has started, rather than before the transition, as the offsite network is completely disconnected when the unit breaker opens.

When the unit breaker opens the voltage on the generator and auxiliary busbars is governed only by the generator excitation, without any influence from the grid. Often the plant is set to produce reactive as well as active power in normal operation. All together the generator exciter is therefore very likely to be set to produce much higher excitation current than is required in house load operation, even without taking account of the demand for more excitation due to a possible initiating grid short circuit.

In the initial phase of house load operation the generator voltage regulator function is therefore challenged to quickly reduce the generator voltage by reducing the excitation current.

Here the principle design of the high power part of the exciter plays a major part in what can be achieved. In a rotating exciter the excitation current is driven from a rotating AC winding and diode bridge, piloted from a stationary thyristor bridge. This thyristor bridge is in normal operation (voltage control) powered from an auxiliary rotating winding. This arrangement is not quite so favourable from a dynamic point of view as the arrangement lacks possibilities to quickly reduce the excitation current, as no negative voltage can be applied.

However, when the excitation current is fed via brushes from a stationary thyristor bridge based exciter, a negative voltage can normally be applied. This type of excitation system has a more direct coupling to the generator voltage as the excitation transformer often is fed off the generator busbar. In the case of an initial extremely low generator voltage (due to a grid fault) this leads to the driving voltage for the excitation current being automatically reduced.

Assuming a transition to house load from normal operation but without any grid fault, i.e. load shedding, the frequency typically ramps up to a maximum of 3-4% over-speed in about one second and then decays (which could be in an oscillatory way with under- and over-shoots) over many seconds. The voltage on the generator and non 1E auxiliary busbars typically ramps up 15-20% over one period and then slowly reduces, initially generating a relatively much higher increase in auxiliary transformer currents. Also on the 1E auxiliary busbars similar excursions can be seen, not even leaving the DC busbar voltages unaffected.

The previous figures are only indicative and will vary from plant to plant and depending on how much excitation (e.g. reactive power) is required.

Now a large number of possible cases, with a variety of excitation levels faults in the grid and faults in the generator exciter, can be assumed. This is further exemplified in the Section 3.1 on “Grid Challenge”.

A high voltage transient is generated and passed down into the auxiliary system at the time when the unit breaker opens. This is also the case when the transition to house load operation is not

successful. If care is not taken in the design and setting of control and protection, mainly relay protection, the voltage transients on the generator busbar can be in the range of 150% depending on the specific voltage regulator design and the field excitation control system. Redundant protection and carefully designed schemes of backup protection features are strongly recommended in order to prevent damage to sensitive protection and control systems.

If a transition to house load operation fails the whole auxiliary supply is attempted to be transferred to the alternative offsite power supply. If this is successful for sufficient number of auxiliary busbars the reactor can remain in operation dumping its power into the steam condenser.

If the transfer to the alternative offsite power supply fails the respective 1E busbar is isolated from the non 1E busbar, EDG starts on low voltage, loads are shed, the EDGs connected, followed by the load-sequencer reconnecting the 1E loads.

Certain other process signals could give anticipated EDG start to provide rapid re-energisation of safety buses.

Even if the transfer to the alternative offsite power supply or the re-energising from the EDGs normally should be verified to confirm that it is within the analysed transients of the plant.

3.3.5.2 Units not designed for transition to house load operation

If the unit is not designed for house load operation the electrical system relay protection is set to disconnect the unit as soon as an unfavourable condition is detected in the grid. Typically the reactor is tripped and an attempt is made to transfer auxiliaries to the alternative offsite power supply. EDGs are started as backup for powering 1E busbars failing the transfer.

In cases where the reactor is scrammed there is no possibility to supply the auxiliaries from the main turbine-generator. However, if the design allows the reactor to remain at reduced power while dumping steam into condenser and auxiliaries on offsite power, the flexibility to promptly repower the grid remains available.

If no offsite power supply is available the whole plant relies solely on the EDGs, provided no Station Black Out (SBO) supply exits. Further, the possibility to quickly come back into operation and to give support for a weak grid is lost. If the reactor is scrammed, typically 2-3 days are needed for the NPP to come back to operation after a unit trip, mainly due to unfavourable core reactivity conditions. In many plants with no house load operation capability the added operational feature of a generator breaker is not essential.

The benefit from reactor safety point of view is that the number of serious electrical system transients is potentially avoided in the absence of house load operational capability and it simplifies the control and protection design. However, it would be misleading to automatically exclude that electrical system transients can occur. In case of an abrupt loss of load for the main generator, the fast voltage rise due to the opening of the unit breaker might very well have propagated down to the class 1E busses if before the transfer of auxiliary power starts or if transfer is delayed. Another example could be a fault in the excitation system of the main generator driving the exciter to full output. The impact of the overvoltage will be moderated by the grid when the generator remains connected to the grid. If the non 1E bus supply from the generator is not disconnected before the unit breaker opens, the whole of the auxiliary system is subjected to a fast voltage transient, well above typical equipment ratings and the only protection may be through an over-voltage protection relay or other voltage clipping circuits for the control systems.

If all equipment works as intended there is no major difference in the electrical systems transients that are produced. The argument for not permitting house load operation rather lies in that

the number of functions that can fail is lower than in NPPs where house load operation is not considered. Subsequently, the probability for a detrimental electrical system transient is lower.

3.3.6 Summary of major benefits and risks

3.3.6.1 Benefits

An NPP designed for runback to house load operation in general (following a unit breaker opening):

- has one additional line of defense (an immediate source of power to station auxiliaries)
- has capability to return to full power supporting the grid without delay
- has instantaneous power to all auxiliaries when offsite power is lost.

An NPP without house load operation capability in general:

- needs a somewhat simpler design on control and protection
- is therefore less likely to be subjected to power system transients due to failures
- has lower investment costs, such as generator breaker and larger condenser

3.3.6.2 Drawbacks

An NPP with house load operation capability in general:

- needs a more complex design on control and protection
- is therefore more likely to fail and thus generate power system transients
- has higher investment costs.

An NPP without house load operation capability in general:

- trips for any significant grid disturbance
- therefore has to rely more on the availability of transfer capabilities
- has a 2-3 days delay to restart due to reactor limitations and synchronise to the grid after a grid disturbance.

3.3.7 Challenges

Looking at the two schemes there are apparent contradictions between safety and availability. There seems to be no simple solution and no ground for abandoning one scheme or the other. The proposed way forward is rather to challenge the existing designs and make improvements based on a good understanding of the weakness and strength in both schemes, the importance of interaction with the grid, knowledge of the grid availability, and contingency planning.

3.3.7.1 Challenges in NPPs with house load operation capabilities

NPP's allowing house load operation have been experienced to be subjected to over-voltage conditions as high as 150% (e.g. Olkiluoto 2008) and potential over-frequency considerations.

The power supply scheme that allows house load operation opens up a large number of possible fault combinations. The design and equipment quality must therefore effectively prevent safety systems from facing transients that will impair their safety function. In order to achieve this action, several issues have to addressed.

The knowledge of what detrimental transients that can be generated in existing and future schemes must be derived through comprehensive analysis using verified models and methods. The analysis must be made plant by plant taking into account the individual initial conditions and variations of each plant.

Designs aspects including component quality, the use of redundant and/or diverse equipment and even assessing the suitability of the overall power supply scheme (e.g. using the IEEE 765-2002 Figure 4) must be considered. Some plants (e.g. US and Spanish) use this scheme but a comprehensive study of the use of this scheme and the experiences made could be of value.

Grid system reliability and variations aspects must be known as well as NPP equipment reliability, and used as inputs in the evaluation of the proposed scheme.

The success rate for the plant to transfer to house load operation needs to be considered. The house load operation capability should not be credited for safety analysis. The variation in initial process status and the possibility of several component malfunctions are very significant uncertainties.

The automatic transfer schemes would need additional design provisions to operate a delayed transfer if the initial fast transfer fails. The grid condition might be much more favourable after just a few seconds following the transient. A manual reconnection to the grid after the initial failure to transfer is currently proceduralised at US nuclear power plants

The resulting design and implementation must result in a power supply system that handles or prevents electrical transients in general, including the particular aspects of house load operation capability. The proposed electrical systems, both non 1E and 1E shall have ample margins (as given by the first line of defence in depth requirement) so that Core Damage Frequency (CDF) can be demonstrated not to be impaired by the capability of house load operation.

3.3.7.2 Challenges in NPPs without house load operation capabilities

The NPP without house load operation capability has a power supply scheme that opens up for less number of possible fault combinations. However, in the light of the Forsmark and Olkiluoto transients possible detrimental transients can not be automatically ruled out. As discussed above for NPPs with house load operation schemes, thorough comprehensive analysis are strongly recommended.

Grid system aspects are also here very important. A grid with many power plants (NPPs and others) with house load operation improves power availability.

3.3.8 Conclusions and recommendations

- The house load capability is a desirable option for increasing the availability of grid through rapid re-powering of the grid after plant isolation from grid. However, the main negative nuclear safety aspect is that the probability and magnitude of the electrical transient generated when the turbine-generator is disconnected from the grid might under certain circumstances, e.g. assuming a component fault, be so large that it adversely affects all the redundant safety systems. The onsite electrical system should therefore be evaluated for the worst cases of voltage and frequency occurring immediately upon house load operation.
- Plants without house load operation capability have less probability of experiencing transients but should still consider the consequences of over-voltage and over-frequency before an isolation can occur e.g. from a power transfer delay, failure, or faults in the voltage controller or turbine governor. The designs that have the capability to rapidly runback reactor power and to remain bypassing steam to the condenser with auxiliary

power systems on the offsite power, could retain the flexibility to repower the grid just as the plants with runback to house load capability.

- The use of preferred power supply schemes which differs from the normal, e.g. supplying alternate offsite power directly to the 1E busbars, should be assessed for possible use in order to eliminate transients detrimental to the 1E loads, or to reduce their probability of occurrence.

3.4 Power supply requirements for protection and control systems

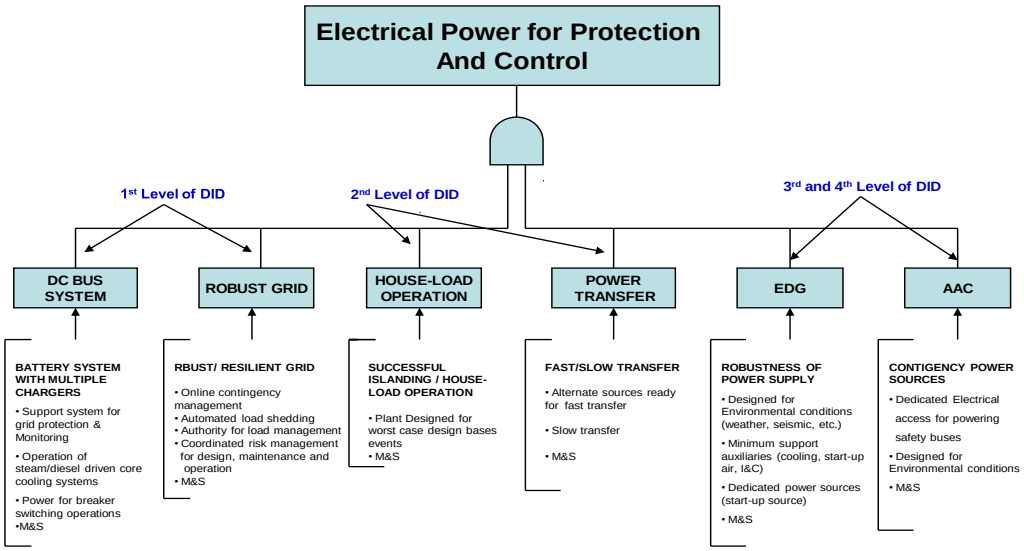
3.4.1 Introduction

One of the problems identified in the Forsmark event was the loss of power to two trains of power and control systems that were relied on for emergency core cooling. The factors that influenced loss of power are: 1. Switchyard maintenance, 2.Unsuccessful House Load Operation, 3. Unsuccessful transfer to auxiliary power supply, 4. Dependence on UPS for the operation of the emergency diesel generator, and 5. Performance of UPS.

3.4.2 Scope

This section will address the Power Supply Requirements for Protection and Control. This section explores the factors that influence the reliability of safety related power and control system, and provide guidance on a robust design to ensure reliable power system to power and control an emergency core cooling system. The essential elements that contribute to robust power supply are: A. Rugged DC bus system B Robust Grid,. C. Successful House Load Operation D, Power Transfer,. E. Onsite Emergency Power source (EDGs), and F. Alternate AC Power Sources (AAC). See Fig. 3.4.2-1.

Figure 3.4.2-1: Robust power supply



A. DC system

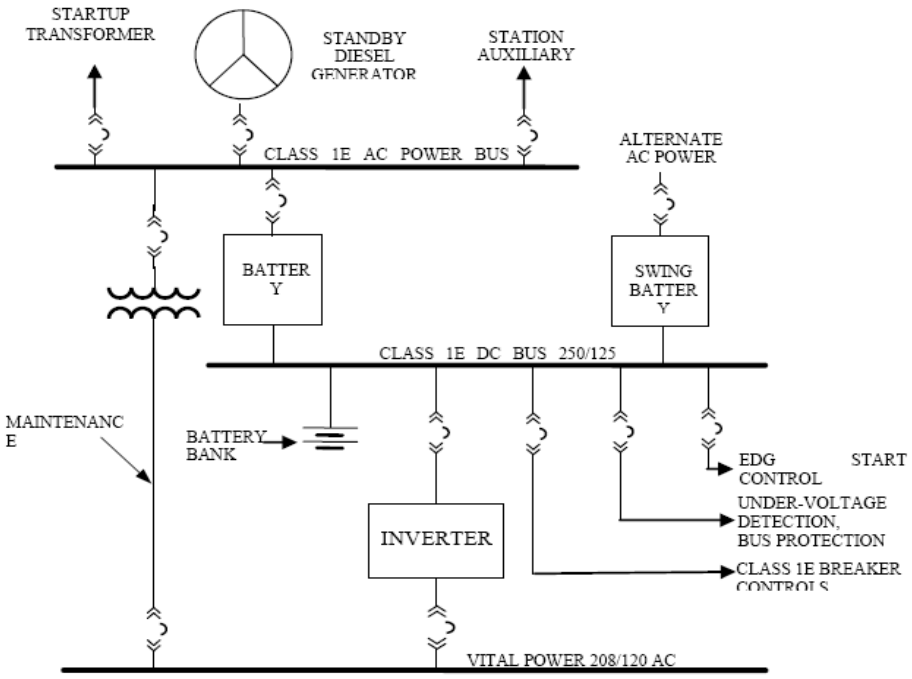
A reliable DC power system is one of the primary lines of defences for electrical defence in depth. A DC power system would have a minimum of two trains with its own dedicated battery, with access to more than one charger per train and multiple sources of power for the charger to ensure battery recovery to full capacity. The DC system has two primary functions.

The first function is in accident mitigation where a Class 1E DC bus system provides the power supply for the steam driven/diesel engine driven core cooling systems that are exclusively powered by DC power. Generally, there is at least one steam driven/diesel engine driven cooling system to supply primary system cooling for BWRs or secondary cooling for PWRs with adequate capacity to stay in hot-shut down conditions for a significant duration. Fig. 3.4.2-2 shows a simplified Class 1E DC power system.

The second function of equal significance is to provide control power for the operation of electrical breakers that allow switching of circuits; starting power, field flashing, and breaker operation for emergency diesel generator; protection and under-voltage detection for class 1E buses; power supply for AC instrument buses; breaker operation for and ECCS pumps. The failure of DC bus could disable the entire electrical train and steam/diesel driven systems.

DC buses generally demonstrate very low failure rates in the rage of 10E-8/hr. See Fig. 3.4.2-2 for one train of a DC system. A DC power system designed to support monitoring of AC buses, AC bus protection, breaker controls, core cooling logic system, and core cooling actuation would increase the availability of core cooling system.

Figure 3.4.2-2 Simplified Class 1E DC power system



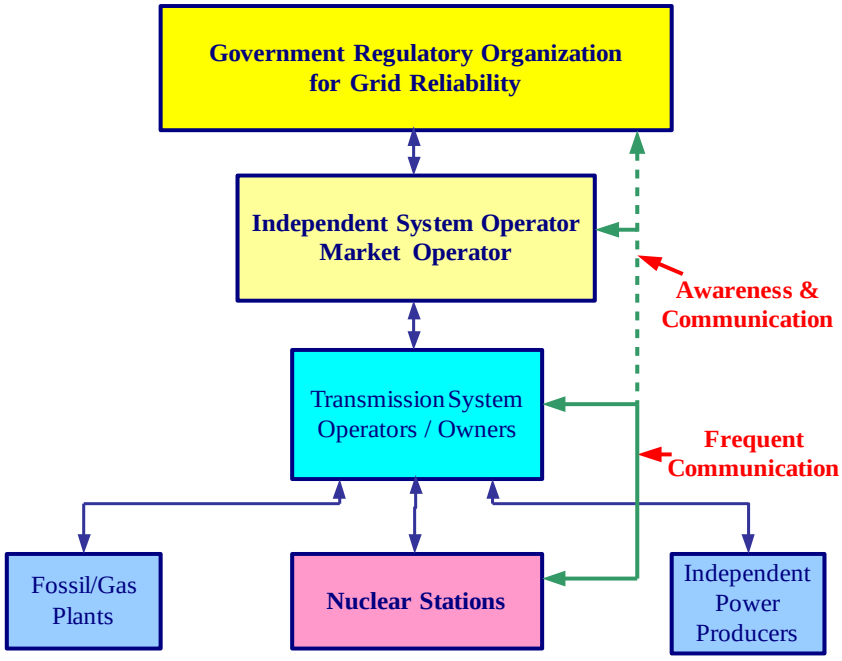
B. Robust grid

In order to encourage competition and produce competitive pricing in production of electricity, certain countries have deregulated the energy sector. Electrical power, the most flexible energy source, has now become a commercial product with variable prices based on supply and demand. The duly licensed power marketers in the respective countries enter into contractual agreements to generate or distribute for very short terms as low as hours and long term contracts into several months for bulk power. The power producers now have the opportunity to sell their uncommitted power to any locations in the market area where it is more profitable. Such hourly changes in markets, modifies the power flow pattern based upon market decisions and consequently, the offsite power voltage and capacity available to the nuclear station. The extremes of market driven power trading may not be global at this time; however, the expected benefits for the average consumer is providing a strong momentum for deregulation to spread around the globe.

In the current economic environment in spot pricing and power trading, the reliable power to the nuclear stations could become a second priority because of the ever changing profile of power flow. In order to promptly address such variations and preserve robustness, interactive software with a

back up should be continuously run by the transmission system operators to analyse grid contingencies and implement remedial actions through manual and automatic actions based on the emergency nature of the problem. See: Fig. 3.4.2-3. The transmission authority should have legal authority to remove grid loads and require increase in power generation from stand by units to maintain the stability of the grid.

Figure 3.4.2-3: Grid contingencies scheme

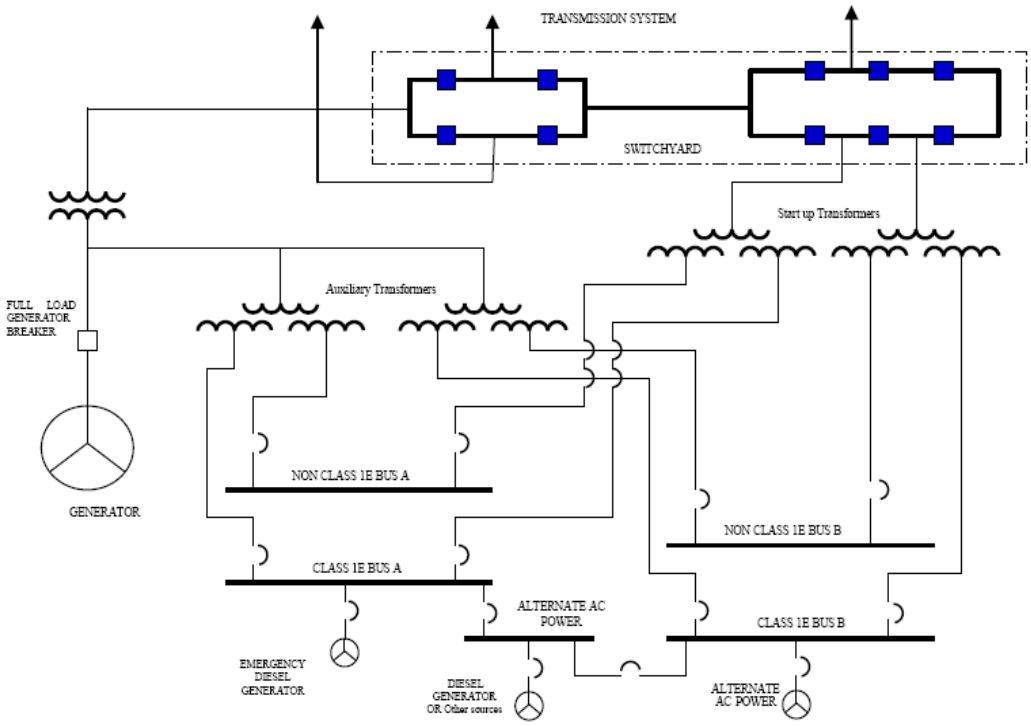


Maintenance activities could cause power reliability problems. A risk assessment on grid maintenance is essential to manage the risk within acceptable limits. A co-ordinated risk management at the nuclear station and at the grid operation is essential for ensuring the reliability of the offsite power from the grid.

NRC Information Notice (IN) 2005-15, "Three-Unit Trip and Loss of Offsite Power at Palo Verde Nuclear Generating Station," and IN 2007-14, "Loss of Offsite Power and Dual-Unit Trip at Catawba Nuclear Generating Station," discuss two events in which an electrical fault at a significant distance from an NPP caused a multiunit trip and loss of all offsite power. In each case, one of the units at a multi-unit plant encountered a problem with one of its emergency diesel generators.

These examples illustrate that external faults located at a significant distance from the plant have been the cause of several plant trips and/or losses of offsite power. Such instances pose challenges to control room operations. The substation serving the NPP has a significant influence in plant trips and the availability of offsite power. While a plant trip may accrue a significant loss of revenue, the loss of offsite power has far more significant nuclear safety implications because the plants rely on offsite power as the preferred source of power for emergency core cooling, Fig. 3.4.2-4.

Figure 3.4.2-4: One-line diagram for single unit nuclear station



One approach to solve this issue is to modify the basis for the substation's electrical protection system to achieve greater protection than the power availability for customers. In order to localise electrical faults, a selective tripping technique is used, which involves providing sufficient time delays for the first level of protection to clear the fault. The traditional time permitted for first-level and second-level protection could be reduced to induce a pre-emptive trip to limit the influence of electrical faults at a distance to the NPP substation. Although this approach would reduce availability for certain loads, it would yield a greater benefit by preventing a nuclear unit trip resulting from either loss of load or actuation of backup protection to clear an electrical fault in the switchyard.

Along with differential current protection and stuck breaker protection, ground fault detection could be installed in each segment of the substation to instantaneously clear any significant ground fault and provide backup for an over-current relay failure. Auto-reclosing circuits, which are generally prevalent in the transmission system, could be executed differently. TSO could verify that the fault is cleared before connecting the circuit to the nuclear plant substation. These steps can significantly reduce challenges to offsite power and trips of nuclear stations.

C. Runback to house load operation

House Load Operation is a design capability for the nuclear stations to continue to produce power at reduced reactor power levels and feed the onsite electrical support systems. A distinct benefit from this design is to have uninterrupted power to the plant support systems even when the grid is disconnected from the nuclear station. The plant electrical equipment should be qualified and

protected to operate when shifting to house load operation with maximum voltage output of the main generator during the run back.[22]

D. Fast/slow power transfer

Many nuclear power stations are designed to stay at low power while dumping the steam output to the condenser and/or to the atmosphere. However, an alternate design to house load operation is to transfer over to the preferred offsite power within a few cycles. This fast transfer capability provides continued power for the safety buses and allows the plant to pursue normal shutdown. A slow transfer capability is also designed to transfer power if the primary approach was unsuccessful. These design provisions provide a second layer of defence in depth for the onsite AC system. These capabilities have to be periodically tested to ensure its prompt operation.

It is desirable to transfer a full train of safety bus (100% ECCS capacity) to a power source that it is not experiencing voltage or frequency fluctuations in order to preserve the reliability of a train. If the offsite power sources appear to be unreliable or inadequate in capacity or voltage, the automatic system should align the safety train to an on-site emergency power source.

E. Emergency diesel generators

The onsite Emergency power sources form the third level of protection for a defence in depth of AC electrical system. These sources are designed to withstand seismic events, hurricanes and other external events considered in the design bases of the plant and it is classified as safety grade. Generally these units are located onsite and they undergo a higher pedigree of controls in its qualification, procurement, installation, periodic maintenance and surveillance. The support systems, such as air, DC power, etc., that are essential for its prompt starting are also subjected to the same level of quality assurance to preserve its availability.

F. Alternate AC sources

In anticipation of any potential problems with on site AC system, a fourth level of robustness is brought to the AC system by providing other diverse means of electrical power that are in standby mode. These units are expected to be available in a period of 10 to 20 minutes. A coping time of 2-4 hours on station battery could be acceptable for plants that have diverse means of core cooling without relying on the plant AC power. These sources would be in service in rare cases when onsite and offsite power have failed. This scenario is also referred to as Station Blackout. Historically, there have been very few cases at nuclear stations when an alternate AC source was essential for emergency core cooling.

3.4.3 Conclusions and recommendation

The explicit requirements for addressing defence in depth of electrical power supplies are non-existent. However, there are certain high level requirements and industry standards that address general requirements. The adequacy of design on reactor control system was specifically reviewed during the licensing phase of every plant. The relatively newer design versions of control systems progressed with a strong foundation for reliability but certain common mode failures and consequences of common-mode failures were not adequately evaluated.

Consider revising IEEE Std. 308 and 765 and other suitable standards to indicate a rugged onsite electrical power system for nuclear power stations.

USNRC 10 CFR 50 Appendix A General Design Criterion (GDC) 17

22. See also the discussion in Section 3.3 "Advantages and Disadvantages with House Load Operation Capability"

The GDC-17 requires that "provisions shall be included to minimise the probability of losing electric power from any of the remaining supplies as result of, or coincident with, the loss of power generated by the nuclear power unit, the loss of power from the transmission power net work or the loss of power from onsite electric power supplies."

A comprehensive regulation is necessary to prescribe the minimum defence in depth required for nuclear safety.

3.4.4 References

1. United States Code of Federal Regulations Title 10, Part 50, of the (10 CFR Part 50) General Design Criterion (GDC) 17 in Appendix A
2. USNRC Regulatory Issue Summary (RIS) 2004-5, "Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power"
3. USNRC Generic Letter (GL) 2006-02, "Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power"
4. USNRC Licensee Event Report (LER) 05000382-95-002-01
5. IEEE Std. 765–2006, "Standard for Preferred Power Supply (PPS) for Nuclear Power Generating Stations"
6. http://www.nerc.com/~filez/standards/Reliability_Standards_Regulatory_Approved.html
7. USNRC Information Notice (IN) 2005-15, "Three-Unit Trip and Loss of Offsite Power at Palo Verde Nuclear Generating Station"
8. USNRC Information Notice IN 2007-14, "Loss of Offsite Power and Dual-Unit Trip at Catawba Nuclear Generating Station"
9. USNRC Regulatory Guide 1.155 "Station Blackout"
10. USNRC NUREG-0800, "Standard Review Plan", Chapter 8 "Electric Power"

3.5 High reliability onsite power supplies

3.5.1 Introduction

Planning a reliable onsite power supply architecture for a nuclear power plant is not a simple task. Normally the electrical power originating from plants main generator and grid connections are flowing thru nearly all different defence lines. If there are not adequate barriers between the systems, one failure can easily propagate from one system to another. So knowledge of failure mechanisms has to be in high level, and continuous learning is needed (e.g. case Forsmark).

It is not enough to consider the different onsite power supplies as fully independent systems. The most important level from safety and reliability aspects is architecture (or plant) level. Independent true diversity has to be considered and the possibility of a common cause failure (CCF) can't be ruled out. The electrical equipments important for safety must be designed and tested to really tolerate the extreme transient conditions that can exist in a nuclear power plant.

The periodical test of the electrical systems should be planned so, that they really simulate the true operation condition of the onsite power supply. The connections to the other systems e.g. auxiliary or control power feeds must be in realistic state during the test.

3.5.2 Design bases

The electrical equipments important for safety have to be designed to really tolerate the extreme conditions that can exist in a nuclear power plant. Experience has shown that extreme voltage/frequency disturbances can happen in NPPs. Generally it is more simple and reliable to design the equipments to tolerate these conditions than to try limit the transients with some complex class 1E qualified special devices. Like with safety functions, inherent safety features attainable by design shall be made use of in the first place.

The architecture of onsite power supply system must be as simple as possible without common elements (bottle necks) between the power systems in different defence lines. Normally the highest reliability is achieved with an AC-network -> rectifier -> battery -> consumer chain. Additional DC/AC (inverters) and AC/DC converters lower the reliability of the electrical distribution system chain, Figure 4 in section 3.4 "Power Supply Requirements for Protection and Control Systems" shows an example of a simplified DC system.

The architecture of an onsite supply system must be such, that a failed part of the system can be easily (manually or automatically) isolated as quick as needed to re-power system parts important to safety. The electrical power systems shall be provided with reliable protection devices that in transients and malfunctions selectively remove from service only the failed component and not the entire bus. The protection of electrical system shall also be designed so, that in case of its failure, the protection settles it in a state preferable from the plant safety point of view.

The design of normal power supply systems shall ensure that the disturbance or failure of a non-safety power supply system does not endanger the designed operation of a safety power system; e.g. battery charging devices shall be designed to reliably prevent the passing of disturbances from alternating current power systems to a direct current system via them.

The on-site electrical power supply system serving the safety functions shall be capable of carrying out its functions during anticipated operational transients and postulated accidents. Therefore it is desirable to have 3 trains of 100% ECCS capacity as a minimum to accommodate maintenance in one train and single failure in another train.

Safety systems which back up each other as well as parallel parts of safety systems shall be physically separated and electrically isolated from each other so that their failure due to an external common cause failure is unlikely (separation principle). This separation must also be used when the essential auxiliary systems of the onsite power source are designed. Any possible interdependence between different onsite power supply systems shall not affect safety.

In principle cross-connections between redundant subsystems shall be allowed only for emergency operations. Their design shall reliably prevent unintentional cross-connections and make human errors unlikely during their planned taking into service and operation. The propagation of malfunctions from one subsystem to another via cross-connections shall be reliably prevented. Cross-connections between systems of different nuclear power plant units are undesirable except for emergencies.

For the purpose of electrical failure monitoring and management, appropriate measuring and monitoring instrumentation shall be designed for the plant by which the operating personnel quickly obtains sufficient data for event assessment and for the planning and implementing of countermeasures.

Diversity

In ensuring the most important safety functions, supply systems based on diverse technology shall be considered (diversity principle).

Diversity shall be utilised for assurance of safety, particularly when the sufficient reliability of a system or component carrying out a safety function cannot be verified by testing. This is important especially when software based components are used, e.g. it is not possible to use the same digital protection relay in electrical supply systems that are in different defence in depth lines.

Alternate (SBO) AC power supply

The possibility of the alternating current on-site and off-site power supply systems being simultaneously lost shall be considered. As provision against such a situation, the plant shall have a diverse (SBO) power supply available which is independent of the electrical power supply units designed for the plant specific design bases. It must be possible to introduce this power supply unit into operation quickly enough and its capability shall be sufficient to remove reactor decay heat, to ensure primary circuit integrity and to maintain reactor sub-criticality.

By design the SBO supply unit shall remain disconnected from the operating power supplies to prevent propagation of any electrical fault. Design should consider earth-quakes, hurricanes and other similar external events. The SBO supply unit should be lined up only manually.

It shall be possible to reliably take the emergency power supply systems into service preferably from the main control room and/or from local control centres. Control room start up is not necessary for the SBO-system, if there is enough time to start it locally. The necessary manual back up controls of the electrical systems shall be implemented using technology as simple and reliable as possible.

Remote shutdown capabilities

The power supplies for the remote shut down station outside the main control room shall be separated from those feeding the systems in the main control room. A total destruction of one fire compartment shall not damage both power feeds to an extent that it can prevent the fulfilment of safety functions.

Ageing management

The service life of the electrical components and their ageing shall be assessed using sufficient safety margins. Furthermore, provision shall be made for the surveillance of their ageing and, if necessary, their replacement or repair.

3.5.3 Qualification

All onsite power systems and components shall be so designed that they perform their tasks reliably under plant specific design bases. The operability of a system or component in the designed situations shall be demonstrated firstly by the necessary tests or by analyses when testing is impractical. Testing/ analyses ensure there are no unintentional functions in the system or its components that could be detrimental for safety.

Equipment utilising solid state components must be proven to be able to sustain all possible voltage variations or transients in the power systems. This shall be particularly observed when modernising existing design.

Subsystems and auxiliary systems of an onsite power supply system (e.g. auxiliary voltage, cooling, fuel, lubrication and compressed air) shall be designed according to the same principles as the main system.

3.5.4 Software based systems

Equipment and controls using microprocessors running embedded software can offer operating flexibility and diagnostics unobtainable with hardwired systems. As with any type of device which is utilised in numerous applications within a nuclear power plant, the possibility and consequences of common cause failure (CCF) within redundant functional elements must be considered. Minimising the impact of CCFs is difficult because such failure modes are normally latent; it is impossible to know what to correct. Latent CCFs are activated by some triggering event. Software based systems, like the relay-based logic they often replace, can be so complex that they are difficult to verify as being 100% error-free in commonly used testing or verification processes. Part of this is related to not always fully recognising all the possible triggering events. Thus, 100% error-free functionality of microprocessor based devices is not possible to prove by testing alone.

The key elements used to demonstrate the reliability of a microprocessor-based system are: a high-standard design processes of the platform and the application, the competence of the personnel participating in the design and implementation, as well as the use of standards applicable to software production. Various independent inspections and assessments of compliance with the requirements, as well as applicable tools, are essential parts of a high-standard software design process. But all these procedures cannot exclude the existence of a latent CCF.

Digital, software based technology needs new ways of thinking. Understanding of new failure mechanisms is essential. The “old world” hardware based technology had its drawbacks. However, dominant failure mechanisms were controllable by statistical methods. Adapting programmable technology presents a new set of failure mechanisms, which are mostly related to inadequate functional design and software specification. And design faults are systematic by nature, and classical statistical methods have basically limited capabilities to handle them. PRA models are not mature enough to analyse the risk of same software based system or component used in multiple defence lines.

For preventing CCF, strict diversity and separation rules are needed in all design levels. The effects of software errors can spread fast using unexpected ways.

3.5.5 Testability

The onsite power systems and components shall be reliable. Therefore, provisions are required to service, inspect and test the systems and components over their entire life-cycle.

Periodic inspections and tests shall be extensive enough to facilitate the prompt detection of deterioration in safety-classified electrical power systems and components prior to their failure to fulfil the acceptance limits. In addition, it shall be assured in particular that equipment and components having to do with stand-by power supply, which are not in use during normal plant operation, are always ready for operation.

3.5.6 Maintenance

The plant design should provide for operational actions, periodic inspection, maintenance, testing and repair of electrical power systems and components.

To avoid maintenance errors, attention shall be paid to the physical work environment and component accessibility. A clear marking system shall be planned to identify components. Safety-related operator and maintenance staff operations shall be task-analysed to plan the necessary actions to avoid or reliably detect human error.

A testability provision shall be designed to safely isolate the concerned components of the onsite power system from the other parts of the plant's electrical system for functional testing, maintenance, and repair.

The service life of electrical components shall be considered when the maintenance programs are planned. Special attention shall be taken to components of known short operation life e.g. electrolytic capacitors or small memory back up batteries.

3.6 Desirable fail safe conditions

3.6.1 Introduction

The conventional design principles limit failure mode analysis to single failures and therefore loss of two trains of the four battery backed AC instrument bus trains was not considered into the design bases of Forsmark nuclear stations. During the event, two UPSs and the respective instrument buses were de-energised. The logic system reverted to the failure mode (due to the disabled process control system) and commanded a relief valve to go open along with two other safety relief valves. This failure mode was undesirable by reducing the rate of reactor coolant system recovery while the emergency core cooling system from the two operational trains were injecting water to cool down the reactor core. The level recovery was significantly increased when the remaining two trains were recovered in 22 minutes following the event.

3.6.2 Scope and limitations

The design basis generally considers single failure as a requirement in safety-related systems. In addition to single failure, common cause failures such as losses of electrical buses are to be considered in order to ensure that the failure does not introduce any undesirable challenges to nuclear safety. The following discussion will address the details of design precautions and techniques to avoid undesirable failure modes. The discussion and the diagrams are based on two-out-of-three logic for simplification.

3.6.3 General principle

In order to achieve defence in depth for electrical systems, the concept of 'fail-safe' is generally accepted as the design principle for critical applications where safety is the primary objective. However, the level of analysis for ensuring the fail-safe condition varies. A component level analysis, followed by combinations of components that have interdependent failures or consequences, followed by a system level analysis would be the recommended approach to confirm the adequacy of reliable electrical power system performance.

3.6.4 System level analysis

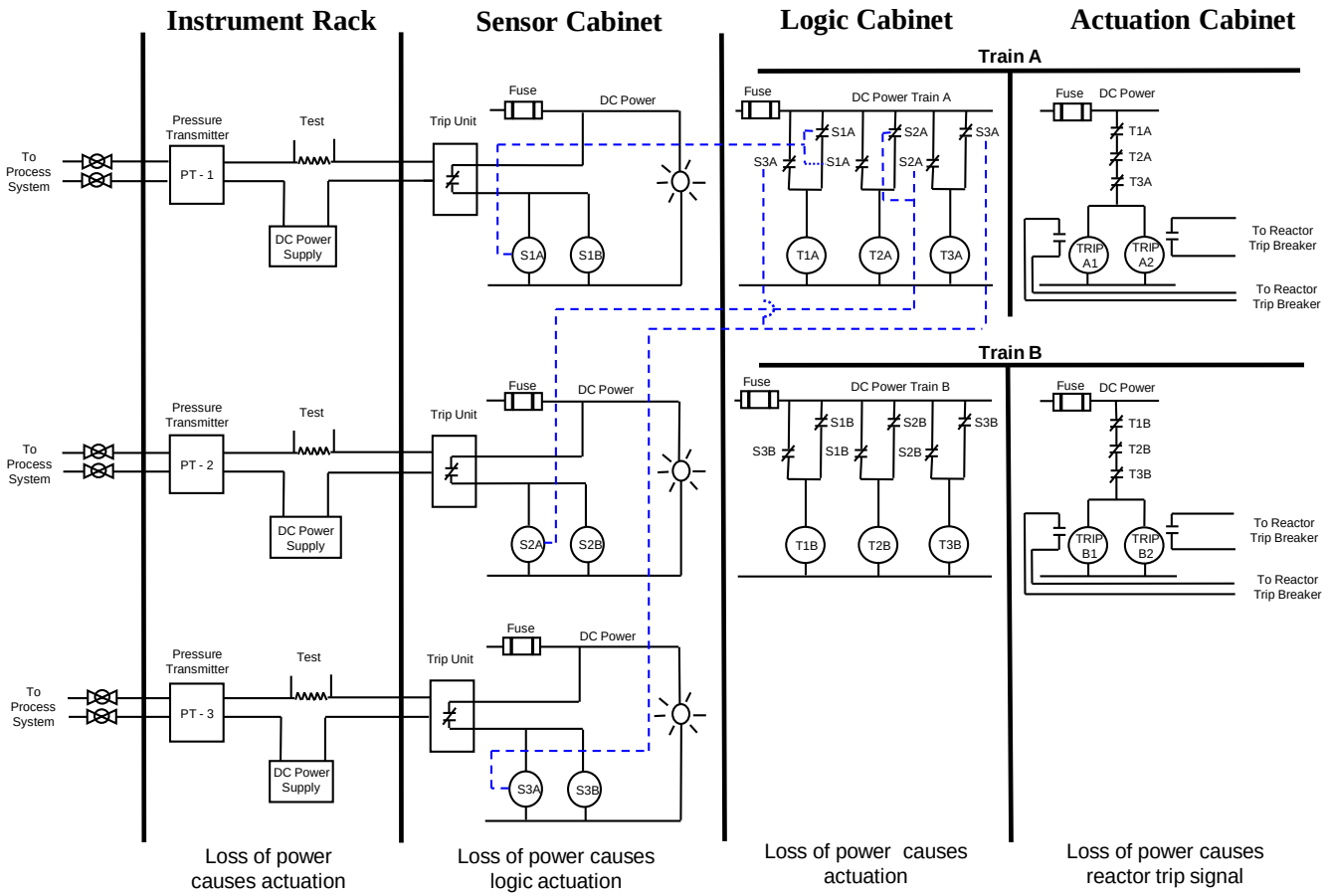
In the nuclear industry, reactor trip systems are generally designed to be fail-safe. The concept extends to all the supporting systems that are essential for operating the reactor at power. The critical support systems are DC power, Vital AC power, essential air pressure or hydraulic pressure for equipment operation. The design should consider loss of any of these critical support systems to constitute a condition to trip the reactor. In order to avoid spurious reactor trip challenges from isolated instrument failures and malfunctions, the validity of any trip condition is processed through a logic system that considers two-out-of-three, two-out-of-four, or other suitable logic to validate actual trip condition. Such selection logic should be designed with provisions to avoid any common mode failures that could fail to initiate a reactor trip on a valid demand.

In the early 80s maintenance related problems identified a common mode failure with reactor trip breakers that resulted in failure to trip a reactor on a valid demand. This concern was resolved by providing diverse methods for control rod insertion for events such as Anticipated Transients Without Scram (ATWS).

Fail-Safe Logic For Reactor Trip System

The industry experience has revealed that a design focused on a ‘fail-safe approach has certain weaknesses. Loss of power (voltage, air or hydraulic pressure etc.) is considered a fail safe condition but a degraded motive power could render the system into in an unknown condition when the response of the control system cannot be predicted. One solution to this vulnerability is to design a monitoring system that actuates a loss of motive power condition when these system parameters are outside the operating band. Such a supervisory control is essential for all major support systems to prevent operation in the unknown region. The simplified diagram (Fig. 3.6.4-1) for reactor trip system is an example of a fail-safe logic that causes a plant trip signal for loss of power.

Figure 3.6.4-1: Simplified fail-safe reactor trip system with a two-out-of-three logic



Core cooling logic system

The failure modes for emergency core cooling system (ECCS) need to follow a modified approach for ensuring the operational readiness. The spurious actuation of a cooling system may be acceptable if the flow path is through a check valve and the check valve is remaining closed by the higher pressure on the primary side during normal operating conditions. The operator can intervene to terminate this actuation after verifying the relevant parameters and its validity for the actuation. An example of this kind would be the ECCS that injects water into the secondary of a pressurised water reactor (PWR) through a check valve.

The ECCS actuation also involves modulating power operated relief valves for PWRs. A spurious actuation of these valves would create a Loss of Coolant Accident (LOCA). Therefore, the desirable failure mode for such condition would be to fail-as-is and generate an alarm condition to draw prompt attention to an incipient failure that has disabled a safety function. The alarm would need a separate DC power supply, preferably a supply with back up sources, so that a loss of power in logic power cabinet would not fail the alarm. Inoperative or bypassed status indication for safety systems was addressed as design guidance in USNRC Regulatory Guide 1.47 “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”.

The design illustrated in the Core Cooling System diagram (Fig. 3.6.4-2) could withstand a single failure of the source signal, actuation relays in the sensor, logic and actuation cabinets. The sensor cabinet relays stay energised, so that a loss of power or trip unit actuation closes the contacts in logic cabinet. The relays in logic cabinet energise on two-out-of-three logic and open the contacts in actuation cabinet to produce an output. Two types of outputs are shown in the actuation cabinet. The first case indicates the absence of an output on loss of power but causes an alarm. This signal would be desirable in case of power operated relief valves that should not open when control power is lost. If a spurious actuation of a pump start or a valve movement during a loss of power can be an acceptable failure mode, the second example of automatic output can be utilised.

Figure 3.6.4-2: Simplified core cooling system with a two-out-of-three logic

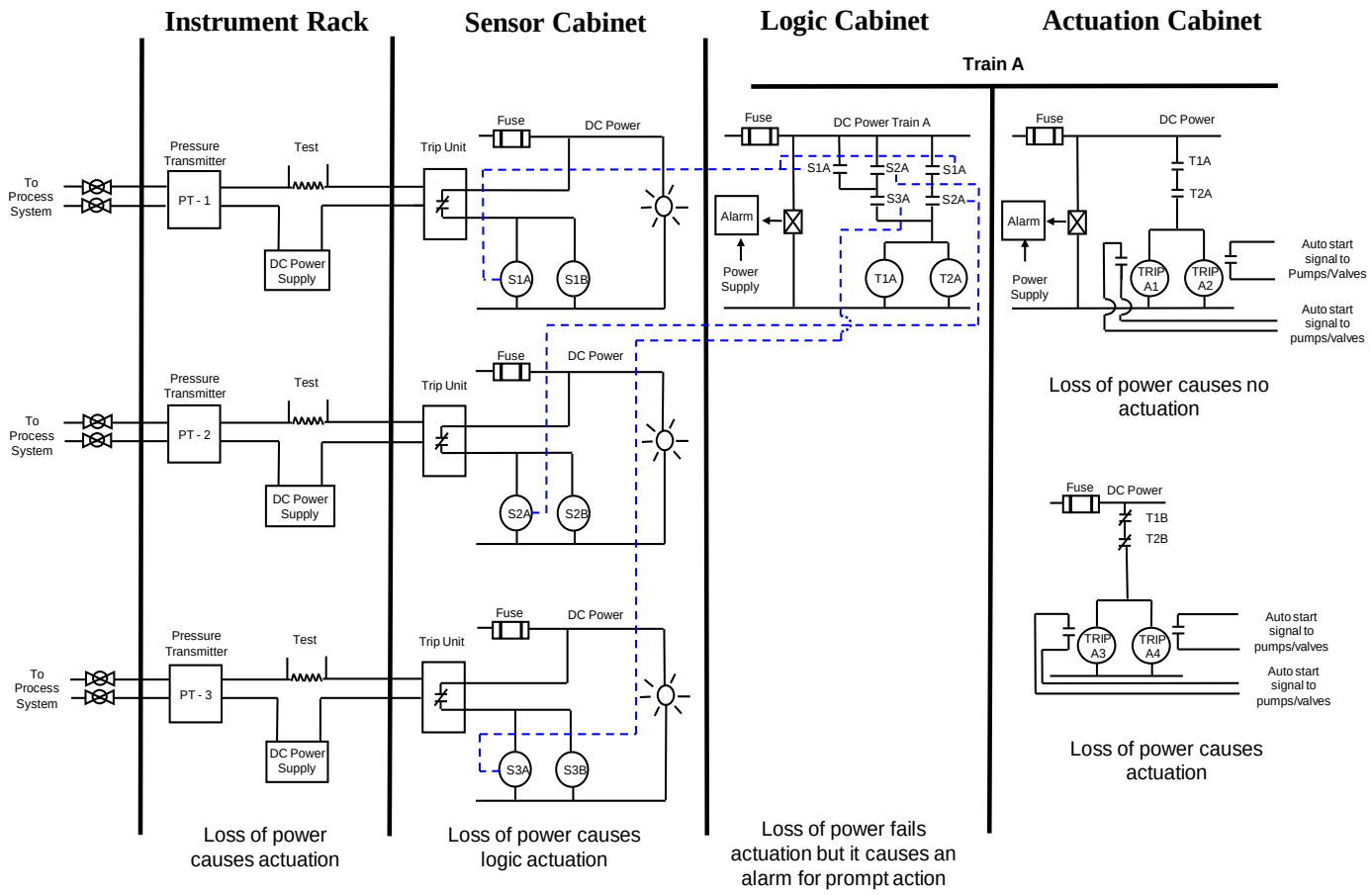
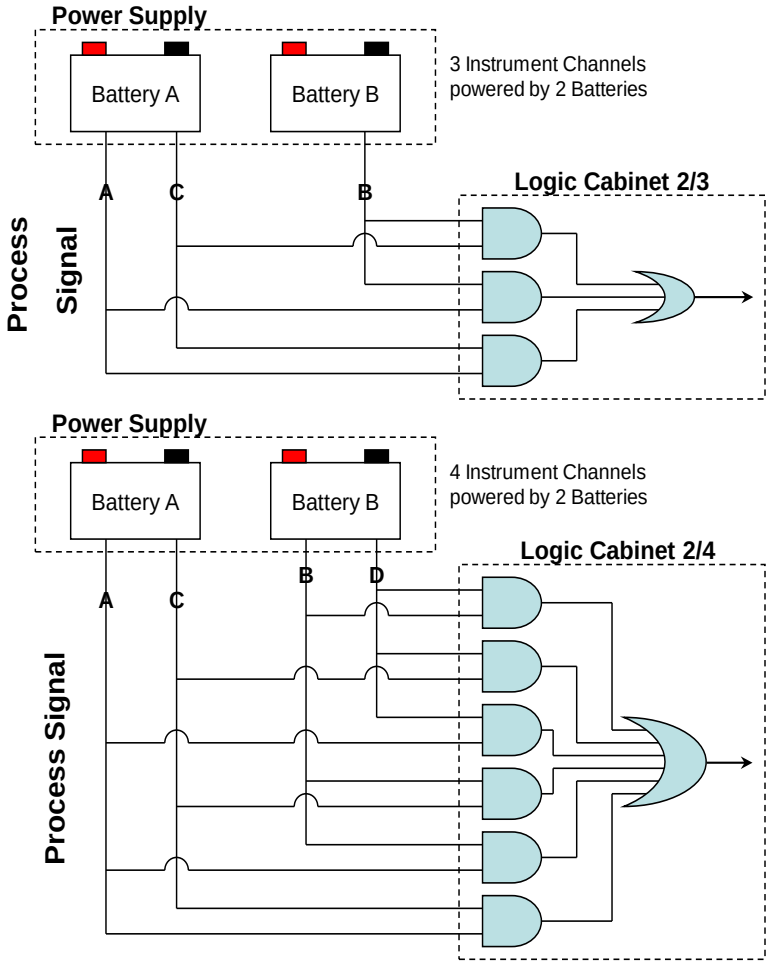


Figure 3.6.4-3: Two train DC systems with 2/3 and 2/4 logic



Source Power:

UPS – Susceptible for common-mode failures from over voltage or under voltage

DC – Comparatively more reliable

Two train DC System with 2/3 logic has the following vulnerability

• When Battery Bus A is lost the logic could create a false output or prevent logic from any output

Solutions:

(1) Fail-Safe Logic

(2) Logic Reverts to 1/1 logic when Bus A fails

Two train DC System with 2/4 logic has the following vulnerability

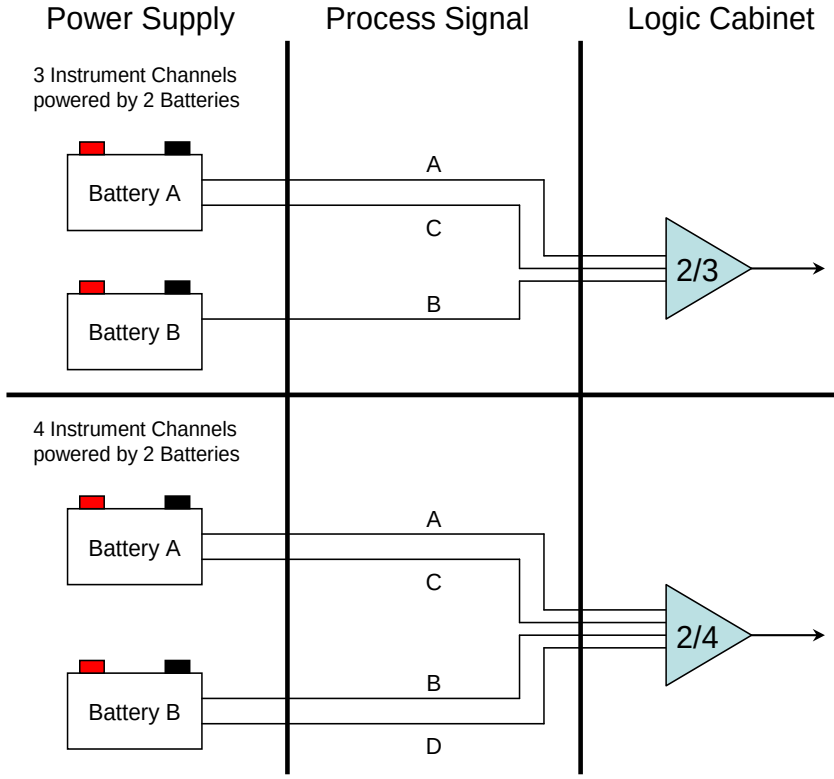
• Loss of Bus A or B can cause a false output

Solutions:

(1) Fail-Safe Logic

(2) Logic Reverts to 2/2 logic with the available pair of signals

Figure 3.6.4-4: Simplified two train DC systems with 2/3 and 2/4 logic



Source Power:

UPS – Susceptible for common-mode failures from over voltage or under voltage

DC – Comparatively more reliable

Two train DC System with 2/3 logic has the following vulnerability

-When Battery Bus A is lost the logic could create a false output or prevent logic from any output

Solutions:

(1) Fail-Safe Logic

(2) Logic Reverts to 1/1 logic when Bus A fails

Two train DC System with 2/4 logic has the following vulnerability

-Loss of Bus A or B can cause a false output

Solutions:

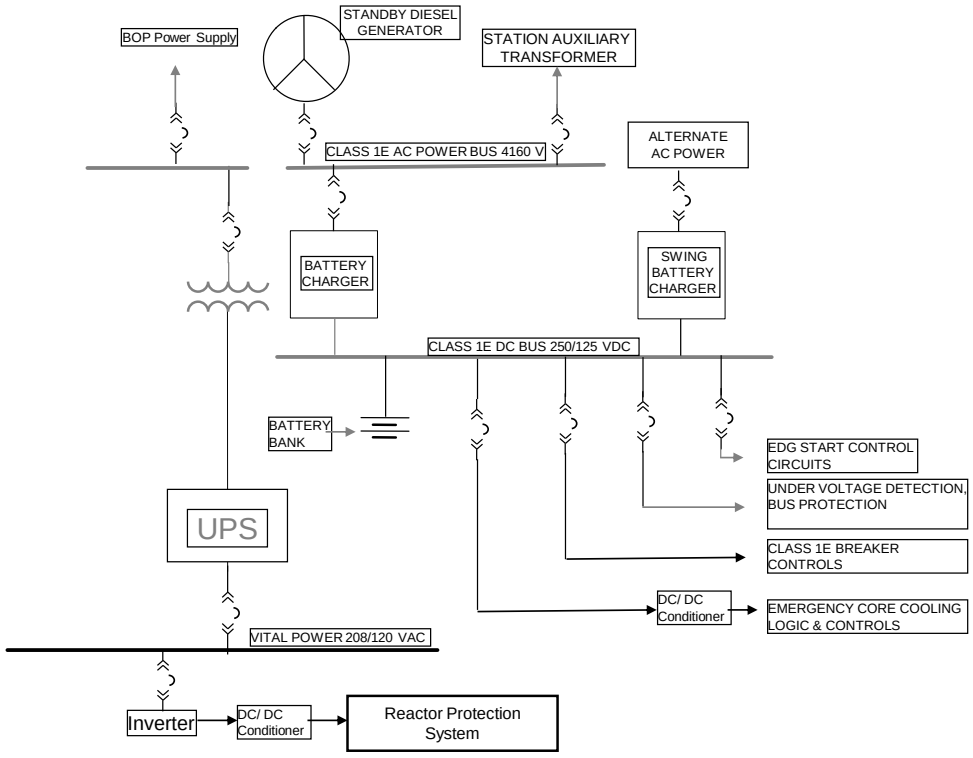
(1) Fail-Safe Logic

(2) Logic Reverts to 2/2 logic with the available pair of signals

3.6.5 Design provisions to limit the impact of power supply failures

Certain design provisions can be considered to limit the loss of power impact on emergency core cooling systems. If the core cooling system can be powered with DC power supply, the potential failure of a battery charger can be compensated through a second battery charger energised by an alternate AC source. The DC bus could provide for the starting of the emergency diesel generator and provide the AC source to power the large pumps in the emergency core cooling system. This approach could avoid dependence on UPS units and preserve independent onsite power capability for accident mitigation without dependence on the grid.

Figure 3.6.5-1: Improved Class 1E DC power system design



The DC/Dc power conditioners can be daisy chained to provide for additional reliability for the control system. If the use of UPS is necessary, the following design provisions need to be considered (using reasonable design margins) for satisfactory performance:

- The UPS should be able to withstand the worst case voltage, frequency and environmental conditions for the plant specific application (Consider grid transients and switching surges)
- Voltage surge protection to protect against the maximum generator voltage with the exciter and the voltage regulator failing to cause the maximum output voltage. A voltage clipping circuit that is always in service would be a desirable approach to overvoltage conditions
- Symmetrical and Asymmetrical fault in the zone of influence
- Capability to monitor rate of change in input voltage for equipment protection

- A withstand voltage coordinated with the protection capability to detect and clear the overvoltage condition
- Under voltage protection to ensure performance of all the connected componenets and systems
- Specification on the quality of sine wave (THD, etc.,)
- Performance requirements of the power conditioners
- Capacity of the battery with adequate provision to recover alternate power sources

3.6.6 Conclusions and recommendations

Review the current control systems for reactor trip systems and ECCS to verify if each of these have desirable fail safe conditions in response to degradation or loss of voltage, air, or hydraulic pressure systems as applicable.

While safety systems in all OECD member countries are required to meet the single failure criterion, there are no current regulations that explicitly require evaluation of failure modes of reactor control systems or accident mitigation systems beyond consideration of the single failure. The following documents have addressed the subject areas.

USNRC IE bulletin 79-07

The operating experience revealed certain weaknesses in the design of control systems. The USNRC addressed such evolving issue through mandated actions and generic communication. The earliest communication was issued in 1979 as IE Bulletin 79-07 "Loss of Non-1E Instrumentation and Control Power System Bus During Operation". This bulletin was in response to an inverter failure followed by a failure of power supply transfer to the instrument bus. The bulletin required the licensees to "identify the instrument and control system loads connected to the bus and evaluate the effects of loss of power to these loads including the ability to achieve a cold shutdown condition."

USNRC generic letter 89-018

During the resolution of Unresolved Safety Issues on "Systems Interactions in Nuclear Power Plants", Generic Letter 89-018 communicated that I&C power loss can cause significant transients and can simultaneously affect the operators' ability to proceed with the recovery by disabling portions of the indications and the equipment needed for recovery. It pointed out the incorrect reliance on fail-safe design principles and cautioned the industry regarding the automated safety-related actions with no preferred failure mode. The need for an added precaution to avoid (a) failure to actuate when necessary and (b) a failure that actuate the system when not required.

ANSI/IEEE Std. 352-1987

The Institute of Electrical & Electronics Engineers (IEEE) published "IEEE Guide For General Principles of Reliability Analysis of Nuclear Power generating Station Safety Systems". This standard was not endorsed by any regulatory organisations.

The following purposes are stated for conducting a failure mode and effects analysis in the design phase:

A. Purposes for FMEA:

1) To assist in selecting design alternatives with high reliability and high safety potential during early design phases

2) To ensure that all conceivable failure modes and their effects on the operational success of the system have been considered

3) To list potential failures and identify the magnitude of their effects

4) To develop early criteria for test planning and the design of test and checkout systems

5) To provide a basis for quantitative reliability and availability analyses

6) To provide historical documentation for future references to aid in the analysis of field failures and consideration of design changes

7) To provide input data for trade-off studies

8) To provide a basis for establishing corrective action priorities

9) To assist in the objective evaluation of design requirements related to redundancy, failure detection systems, fail-safe characteristics, and automatic and manual override.

The FMEA may be performed with limited design information because it is not primarily concerned with rate of occurrence or frequency of failure. The basic questions to be answered by an FMEA are as follows:

1) How can each part conceivably fail?

2) What mechanisms might produce these modes of failure?

3) What could the effects be if the failures did occur?

4) Is the failure in the safe or unsafe direction?

5) How is the failure detected?

6) What inherent provisions are provided in the design to compensate for the failure?

The recommendation in this area is first to revise the above IEEE standard[23] using the guidance in this section and address the failure modes of the new digital systems. This standard could be codified through a regulatory action as a permanent solution to address this problem.

23. The Nuclear Power Engineering Committee of IEEE that is responsible for all the nuclear standards entertained a presentation from a representative of DIDELSYS Task Group and committed to revise IEEE Std. 352 "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems" to address the desirable failure modes of the RPS and ECCS control systems.

3.6.7 References

1. IE Bulletin 79-07 “Loss of Non-1E Instrumentation and Control Power System Bus During Operation”.
2. USNRC Regulatory Guide 1.47 “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”
3. ANSI/IEEE Std. 352-1987 “IEEE Guide For General Principles of Reliability Analysis of Nuclear Power generating Station Safety Systems”.
4. Generic Letter 89-018, “Systems Interactions in Nuclear Power Plants”.

3.7 Challenges in FMEA and diversity

3.7.1 Introduction

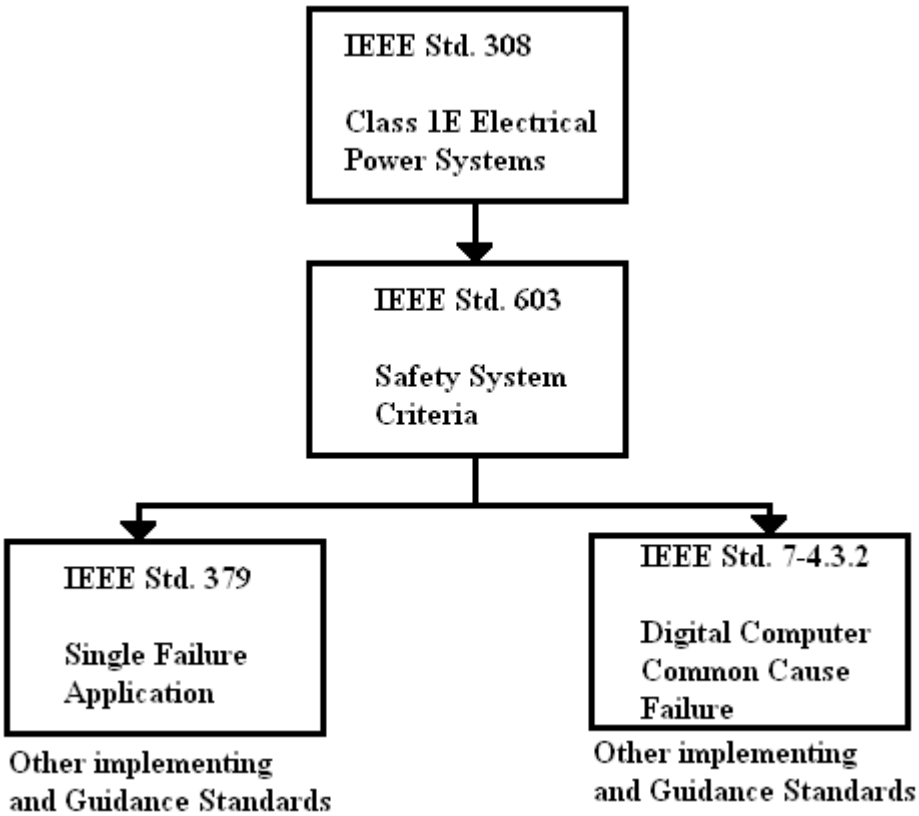
Events (such as the 2006 Forsmark event) have revealed after-the-fact a number of design weaknesses that in theory should have been prevented by existing industrial standards. The following questions arise:

- Are there weaknesses in the industrial standards used to design electric power systems that allowed designs with such Single Failure vulnerabilities?
- Perhaps the standards for considering and addressing Single Failures are sufficient – but is the implementation into specific design practices by designers flawed?
- Are the tools used to support electrical system Single Failure analysis sufficient?

3.7.2 Hierarchy of requirements related to class 1E power systems

Within the IEEE Standards framework the following hierarchy exists (Fig. 3.7.2-1) which describes the industry design requirements for nuclear power plant electrical systems. The supporting standards are further described in the subsequent text.

Figure 3.7.2-1: Hierarchy of requirements related to Class 1E power systems



IEEE Std. 308 (IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations) provides general criteria such that: "….no design basis event causes the following: *A loss of electric power to a number of engineered safety features, surveillance devices, or protection system devices so that a required safety function cannot be performed. *A loss of electric

power to equipment that could result in a reactor transient capable of causing significant damage to the fuel cladding or to the reactor coolant pressure boundary." The standard contains the following specific guidance in Section 8.1 on what must be considered and documented:

> The following information and studies should be included, as a minimum, in the documentation supporting design of the Class 1E power systems:
>
> a) Steady-state load and voltage profile studies that show the voltages throughout the power system for various modes of plant operation, including design basis events, at the time of normal and degraded voltage conditions.
> b) Transient load and voltage studies that show the profile of the loads that are sequentially applied to the preferred and standby power supplies during various modes of plant operation, including design basis events.
> c) An instrument and control power system study that examines loading and voltages in the alternating current and direct current systems for postulated design basis conditions.
> d) Protective device coordination and equipment protection studies that show proper setpoint selection in all of the protective schemes.
> e) A bus transfer study that analyzes the impact of voltage, phase angle, and frequency on buses and motors before, during, and immediately after automatic bus transfers.
> f) Short-circuit studies to determine the maximum fault currents throughout the power system for various modes of plant operation, including design basis events, to be used to analyze the withstand and fault clearing capability of the electrical equipment.
> g) Equipment sizing to ensure that the electrical equipment has been properly applied.

In addition to the above criteria given in Section 8.1 of IEEE Std 308, design basis should consider consequences of electrical transients triggered by various single failures that could impact voltage/frequency profile. Because these transients can be propagated to the class 1E systems that are electrical coupled.

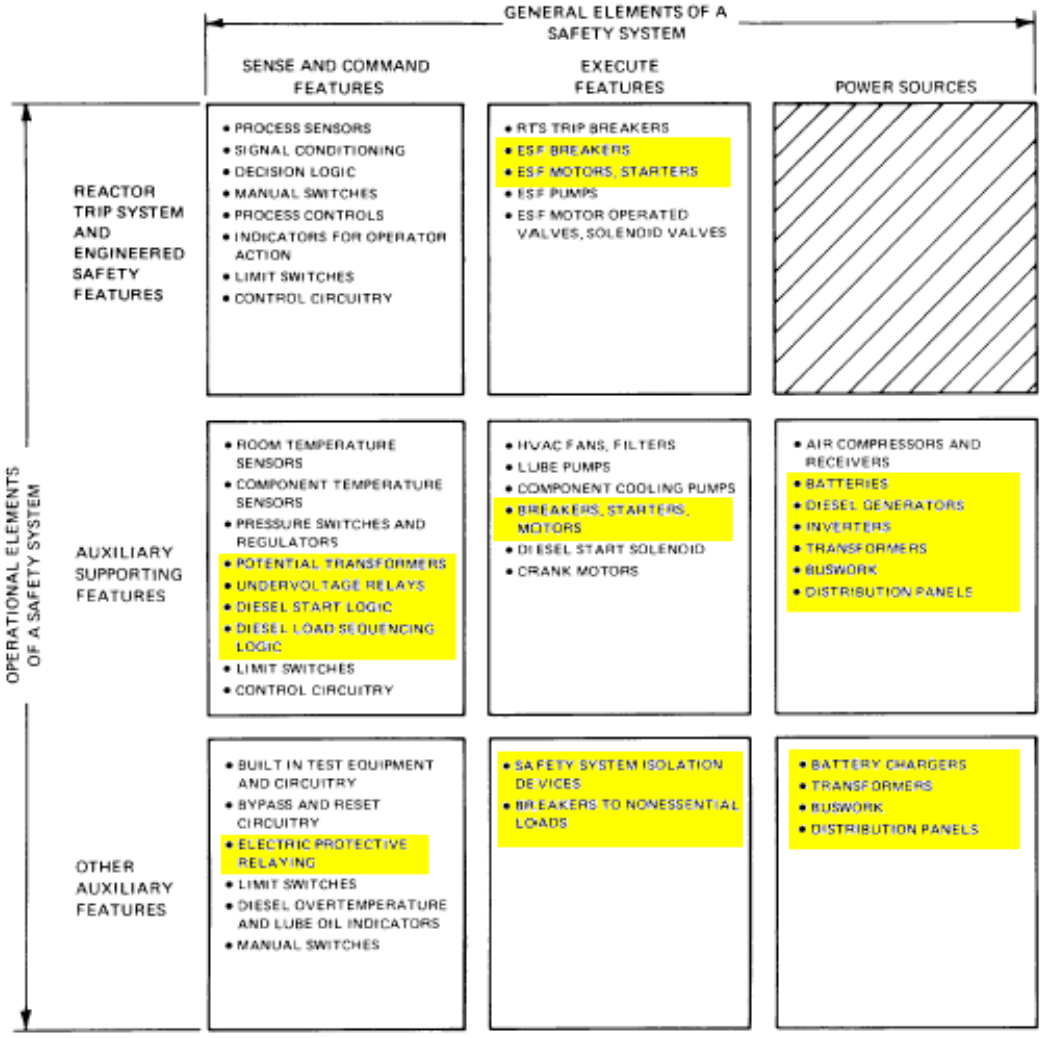
Diversity should be understood as having a different system to avoid common vulnerabilities or deficiencies.

The standard refers to IEEE Std. 603 for definition on how to implement specific features (actuation logic, bypasses, bypass indication, etc.) The need to postulate scenarios involving over-voltage and under-voltage would need to be considered and documented as a part of the design analysis of the power system. This would also include protective device coordination and the effects of maximum fault currents. Thus the basic requirements exist and one must now look at the implementation of the requirements.

IEEE Std. 603 (IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations) provides general criteria for design of all Class 1E safety systems (including the electric power systems). IEEE Std. 603 references: (i) IEEE Std. 379 as the standard practice for single failure criteria application, and (ii) IEEE Std. 7-4.3.2 for issues associated with digital computer common cause failure treatment.

The following Figure, taken from IEEE Std. 603, shows the systems and components scope:

Figure 3.7.2-2: IEEE Std. 603 systems and components scope



From this figure the essential elements of Class 1E electric power systems within the scope of this effort are highlighted.

3.7.3 Identification of single failure modes

IEEE Std. 603 Section 4.g requires the following design bases be documented:

> g) The range of transient and steady-state conditions of both motive and control power and the environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, vibration, and electromagnetic interference[9]) during normal, abnormal, and accident conditions throughout which the safety system shall perform.

The standard provides the following single failure requirements in Section 5.1:

The safety systems shall perform all safety functions required for a design basis event in the presence of

a) Any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures.
b) All failures caused by the single failure.
c) All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

Section 5.1 notes that probabilistic risk assessment considerations can be utilised to "screen out" certain events from consideration as single failures – but *not in lieu of the single failure criteria itself*.

The performance of a probabilistic assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.

In addition to the credibility assessment based on the frequency of occurrence, the operating experience has to be considered.

One possible reason for not considering under-voltage, over-voltage, and under-frequency events would be if they had been screened out from consideration as a result of probabilistic risk assessments. Given actual operating experience with such events, going back several decades, it would not be possible to screen such events out from consideration. The table below shows specific under-voltage, over-voltage, and under-frequency events identified from reactor operating experience reviews. Thus IEEE Std. 603 would require postulation of scenarios involving under-voltage, over-voltage, and under-frequency events.

Under-voltage	Over-voltage	Under-frequency
July 5, 1976 Millstone 2 under-voltage event July 20, 1976 Millstone 2 under-voltage event	March 1, 1993 Sequoyah excitation system failure causes 120% over-voltage event	Sept. 12, 1985 Palo Verde 1 under-frequency during load rejection test
July 11, 1989 Virgil C. Summer reactor/turbine trip causes under-voltage on grid	April 16, 1993 North Anna excitation system failure causes 120% over-voltage event	Sept. 11, 1986 Palo Verde 2 under-frequency during reactor/turbine trip test
August 12, 1999 Callaway 1 offsite grid under-voltage event	May 30, 2008 Olkiluoto 1 generator excitation failure causes 150% over-voltage event	May 27, 2008 Sizewell B trips on under-frequency and grid degrades to 48.6Hz
March 14, 2005 San Onofre under-voltage setting found inadequate		

IEEE Std. 379 (Standard Application of the Single Failure Criterion to Nuclear Power Generating Stations Safety Systems) provides further guidance in application to the criteria stated in IEEE Std. 603. In particular, where and how to consider: cascaded single failures and common cause failures. Section 5.3 would require:

> Whenever the design is such that additional failures could be expected from the occurrence of a single failure from any source (e.g., mechanical, electrical, and environmental), these cascaded failures, collectively, shall be considered to be a single failure.

The wording of this requirement implies that scenarios involving under-voltage or over-voltage events would be considered as a cascaded failure. The standard further describes treatment of common cause failures as follows:

> Common-cause failures not subject to single-failure analysis include those that can result from external environmental effects (e.g., voltage, frequency, radiation, temperature, humidity, pressure, vibration, and electromagnetic interference), design deficiencies, manufacturing errors, maintenance errors, and operator errors. Design qualification and quality assurance programs are intended to afford protection from external environmental effects, design deficiencies, and manufacturing errors.

Propagation of common cause failure events not subject to single failure analysis are thus assumed to be precluded by Design Qualification and Quality Assurance Programs.

> Additionally, provisions should be made to address common-cause failures. Examples of techniques are detailed defense-in-depth studies, failure mode and effects analysis, and analyses of abnormal conditions or events. Design techniques, such as diversity and defense-in-depth, can be used to address common-cause failures.

IEEE Std. 379 provides detailed guidance in the process of conducting and documenting a single failure analysis, including the identification of safety function, protective actions, safety groups, and how independence of the safety groups was established. In the specific case of an onsite electrical system in which portions of the equipment are interconnected (via transformers) during normal operation, the following additional guidance is provided in Section 6.1:

> Those actuators designed to apply power when protective action is required shall be analyzed to assure that no single open circuit, short circuit, or loss of power can cause loss of a safety function.

It is at this level we first recognise that the scope of the single failure analyses is limited to single open circuits, short circuits, or loss of power – but no mention is made of situations where there is a circuit connection but voltage levels are outside of ranges that would allow proper device operation.

IEEE Std. 352 (Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems) is referenced in IEEE Std. 308, 603, and 379 as a source of information ("informative guidance") on conducting and documenting a Failure Modes and Effects Analysis of the type which are frequently submitted in Safety Analysis Reports. IEEE Std. 352 dates from the mid-1970's (was revised in 1987) and covers FMEAs, fault trees, and estimation of reliability data from operating experience data. The stated purposes of an FMEA in Section 4.1 are:

4.1.1 Purposes of Failure Mode and Effects Analysis [23]. The purposes of an FMEA are as follows:

(1) To assist in selecting design alternatives with high reliability and high safety potential during early design phases

(2) To ensure that all conceivable failure modes and their effects on the operational success of the system have been considered

(3) To list potential failures and identify the magnitude of their effects

(4) To develop early criteria for test planning and the design of test and checkout systems

(5) To provide a basis for quantitative reliability and availability analyses

(6) To provide historical documentation for future references to aid in the analysis of field failures and consideration of design changes

(7) To provide input data for tradeoff studies

(8) To provide a basis for establishing corrective action priorities

(9) To assist in the objective evaluation of design requirements related to redundancy, failure detection systems, fail-safe characteristics, and automatic and manual override

Thus, a weakness of the existing industry standards guidance is: that one could perform a detailed FMEA assessment as described in the current standard and it gives the impression that by covering faults such as: open circuits, fails to open, fails to close that in fact all conceivable failure modes and their effects on operational success have been considered and thus all possible single failures considered. Obviously the need to postulate a much wider spectrum of events is needed, possibly as a future update to this standard.

3.7.4 Identification of effects of specific failure modes

An additional area of weakness in application of traditional FMEA is in the difficulty in projecting the effects of specific failure modes within electrical systems. Simple failure modes such as: open circuits do not require further analysis to demonstrate they result in de-energising of circuits. Similarly, failing to close a switch or breaker does not require further analysis to demonstrate it results in a circuit remaining de-energised.

In the area of electrical faults such as delayed trip of a breaker, the extent to which an electrical fault propagates clearly requires further analysis (in some cases) supported by system simulation tools to understand the extent of effects on the overall electrical system. Other examples include:

- A failure of the main generator excitation system. How high of a voltage could be generated and impressed back to Class 1E buses through the station auxiliary transformer? Is it likely to be coincident with a turbine-generator overspeed, which would further increase the peak voltage surge?
- A short duration switching transient generates an inductive load pulse. How high of a voltage surge pulse is transmitted back to other phases through the station auxiliary transformer?

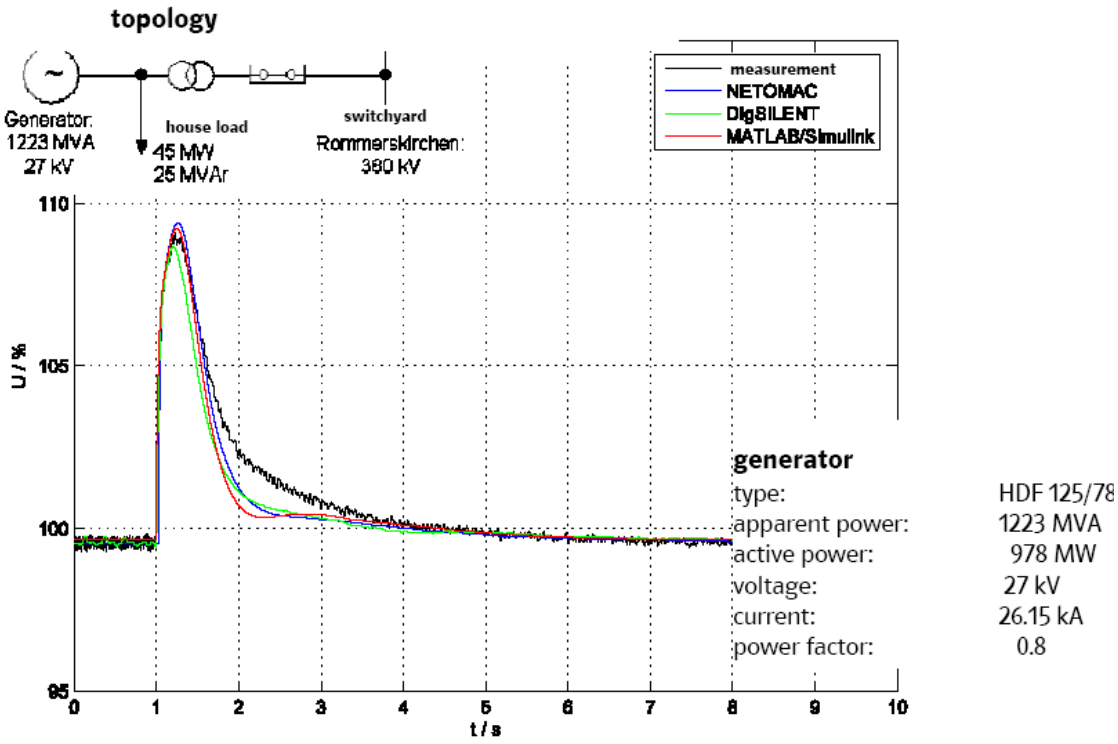
Are events such as these sufficient to exceed the normal design rating of the connected Class 1E loads – such as: inverters, battery chargers, and local control system power supplies? These are the specific types of questions that should be pursued in order to perform the “effects analysis” portion of an FMEA.

Comprehensively answering these questions requires use of verified and validated simulation tools which can be used with the same level of confidence as reactor LOCA analysis simulation codes. For the same reasons that one would perform a LOCA break spectrum analysis using a LOCA analysis simulation code to verify the adequacy of existing ECCS systems, a strong case can be made that the equivalent should be done to evaluate various types of electrical transients on the onsite electric

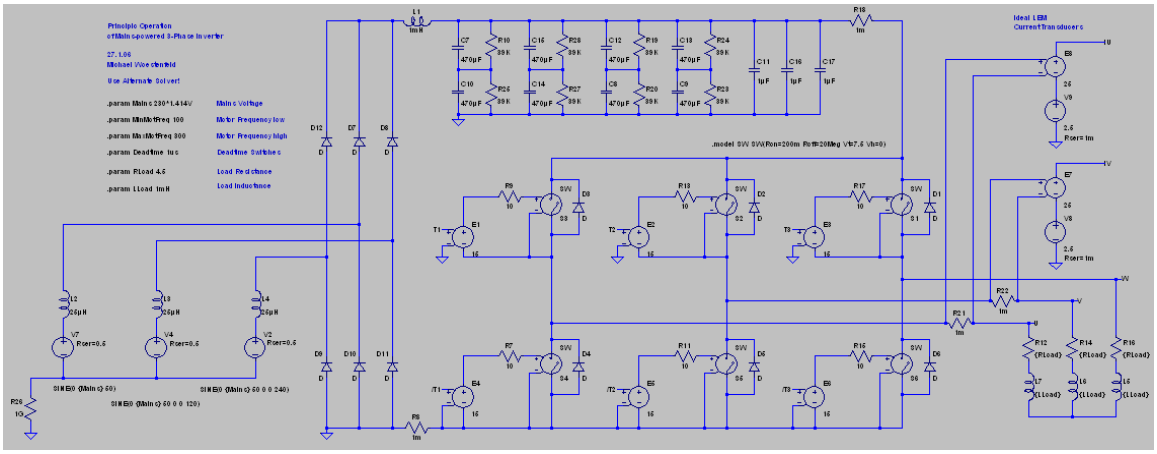
systems. The simulation codes needed to do such analysis do not need to be developed – they already exist. What is missing is the standard process of verifying and validating such codes for use in nuclear power plant safety analyses.

Analogous to a reactor systems code such as RELAP5 or ATHLET, for predicting peak cladding temperature during a design bases LOCA, there are electrical power system simulation codes that can be used to predict onsite AC power system voltage and frequency response to various types of electrical fault conditions. An example of this type is shown in the figure below (based upon work supported by the German Nuclear Operators Organisation, VGB).

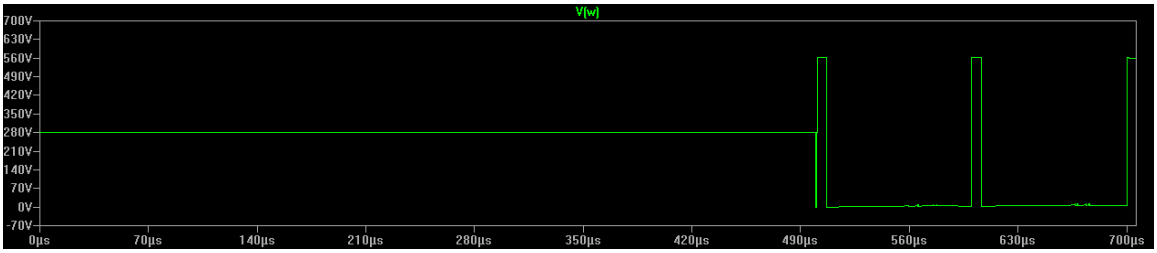
Figure 3.7.4-1: Validation of simulation tools



Analogous to detailed nuclear fuel rod transient codes such as FRAP-CON, it is also useful to be able to perform detailed analyses of the impacts of various types of voltage/frequency transients on local devices such as inverters, battery chargers, starter circuits, and local control system power supplies. Again, tools to do this type of simulation tool have long existed in electronics design industry via computer codes such as: SPICE. Manufacturers of rectifiers, thyristors, and various integrated solid state devices routinely provide and update their specific component's SPICE models to allow designers to understand their exact static and dynamic properties. The figure below is an example of the Graphical User Interface (GUI) for a spice simulation of a 600V 3-phase Pulse Width Modulated Inverter.



The figure below shows a simulation of the A-phase start-up transient of such a device.



SPICE models are capable of injecting specific voltage/current waveforms, modelling non-linear component properties, and time dependent response. Additionally such models can be used to determine heat dissipation and other performance parameters needed to assure products operate within acceptable design tolerances. In order to be able to use such tools for nuclear safety applications, however, it would be necessary to subject such models to a standard verification and validation process. This should not prove difficult as the tools are currently used extensively in the telecommunications, and electronic circuit design process.

3.7.5 Conclusions and recommendations

Failure Modes and Effects Analysis (FMEA) is an important design and safety demonstration tool. We observe that current FMEA has not systematically postulated *all observed failure modes* and has not identified the possible effects of these observed failure modes from actual operating experience.

Existing standards such as IEEE Std. 379 currently suggest one to consider single failures such as: single open circuits, short circuits, or loss of power. This obviously does not preclude the need to consider other types of single failures which have been observed in actual plant operating experience since the last major upgrade cycle of the standards.

We recommend augmenting the types of single failures considered in FMEA to include the following types of failure modes when designing or justifying the design of offsite/onsite AC power systems:

- Degraded voltage on offsite/onsite AC supplies at all levels above those precluded by existing under-voltage protection setpoints.
- Degraded frequency on offsite/onsite AC power supplies above those precluded by existing protection setpoints.

- Voltage surges on onsite AC power supplies below those physically limited by existing surge and lightning protection features.
- Short duration switching surges (pulses) of durations shorter than breaker opening times and below those of existing surge and lightning protection features.

Recognising that the effects analysis of specific failure modes in offsite/onsite AC power systems involves complex, non-linear, and frequency dependent response characteristics it becomes difficult to apply engineering judgment to project the actual outcome of specific faults.

We recommend augmenting the tools available for comprehensively assessing the outcome of specific electrical faults by use of systems simulation tools such as (but not exclusively limited to) MATLAB/Simulink[24] for onsite power systems and SPICE for evaluation of local component effects. To do this of course requires qualifying and benchmarking these types of simulation tools to a pedigree required of tools utilised to support nuclear safety analysis in areas such as reactor thermal hydraulics and structural mechanics.

3.7.6 Summary discussion on FMEA/single failure challenges

After reviewing the hierarchy of IEEE standards that are used to guide designers on addressing single failure in electrical systems, it is apparent that:

- The higher level standards and requirements appear appropriate – but the lower level implementation guidance on scope of an acceptable FMEA needs revision.
- The postulation of scenarios involving over-voltage and under-voltage events would need to be considered and documented as a part of the single failure analysis in the design of the electrical power system, per the requirements of IEEE Std. 308, IEEE Std. 603, and IEEE Std. 379.
- IEEE Std. 379 would allow excluding over-voltage and under-voltage events from the single failure analysis if and only if one can credit Design Qualification and Quality Assurance Programs. The intent of Quality Assurance Programs although not referencing a specific ANSI standard would clearly be related to conformance at least to 10 CFR Part 50 Appendix B criteria. The term Design Qualification, however, is not defined in the standard, and specific attributes of an acceptable Design Qualification program are not addressed in this standard, nor is reference made to another standard.
- IEEE Std. 352 (an "informative document") is very limited in the types of faults which are suggested to be considered in a standard FMEA. It does not mention faults such as over-voltage and under-voltage events – yet gives the impression it is intended to produce all conceivable failures – which is clearly a gross overstatement.

24. Researchers in Sweden have noted the inability of "off the shelf" MATLAB/Simulink (Power System Toolbox) to accurately reproduce asymmetric faults in non-effectively grounded 3-phase systems.

3.8 Conflicts between protection and reliability

3.8.1 Introduction

Class 1E onsite electric systems are the essential support systems for numerous safety functions such as reactor makeup, decay heat removal, and containment sprays, etc. These safety features rely on medium voltage power to run large AC pump motors. Should there be an electrical fault in a motor it is essential that the fault be isolated to prevent the loss of power to other motors powered by the same bus. Should there be a fault in one of the high voltage buses or transformers supplying numerous connected motors, it is essential that the fault be isolated to prevent fire or fault propagation back to higher voltage buses. Another consideration is the role of protective relaying in protecting equipment so that it may be relied upon once a fault is cleared and power restored to the bus. The need for automatic fault detection and breaker trip logic is thus obvious.

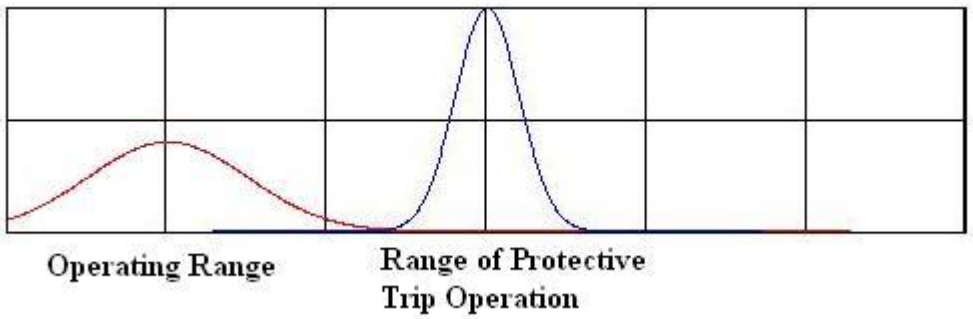
3.8.2 Reliability of power supply

When addressing reliability of supplying power to safety loads, the possible spurious operation of protective logic becomes one source of possible failure to start or run a safety related pump. A quick look[25] at estimates (NUREG/CR-4550) of which types of faults inherently have the highest failure rates indicates the following:

- 4.16kV Electrical Bus Faults: 1x10-8/hr - 4x10-6/hr
- High Voltage Transformer Shorts/Faults: 2x10-6/hr
- Protective Relay Spurious Operation: 1x10-6/hr

Faults would appear to be a more likely source of losing a bus credited for supporting a safety related motor. If one directly uses such data and presumes that all protective relay devices have sufficient operating margins to the point of actuation – one could have double or triple the number of protective relay devices before they would become a source of concern that spurious tripping would dominate the unavailability of power supplies to safety related motors. On the other hand if one envisions a situation where the upper range of operation is close to the range where protective action could occur, the spurious trip rate is obviously higher.

Figure 3.8.2-1: Relationship between upper operating range and protective trip range

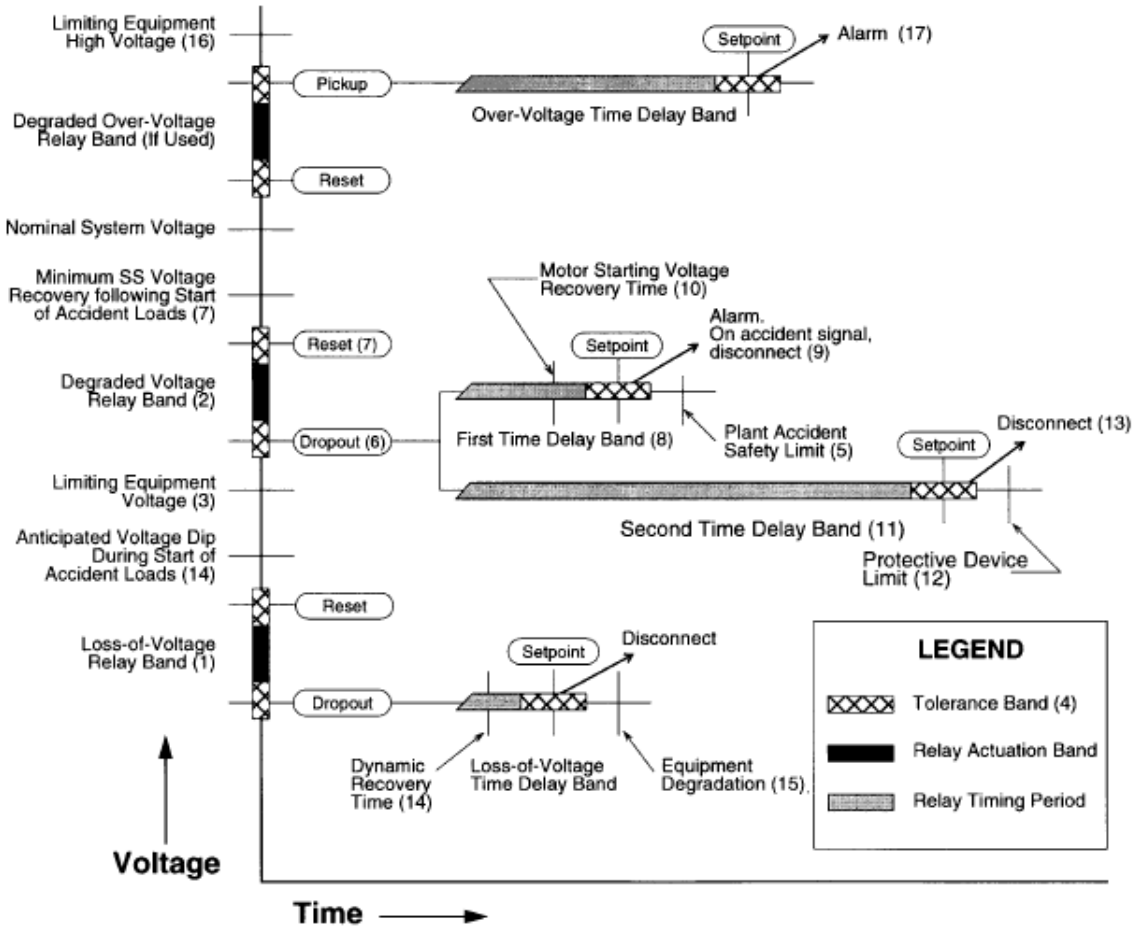


25. These estimates are based upon total numbers of observed faults and estimates of population sizes (number of components and run times). One item not clear from such raw data on protective relaying is the operating margin between normal operating ranges and the point of trip operation.

3.8.3 Role of standards in maintaining margins

IEEE Std. 741 (Standard Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations) provides current guidance in the arrangement of bus protection requirements including determination of the relative levels where equipment protective actions should be initiated relative nominal operating voltages and limiting equipment voltages. Fig. 3.8.3-1 below is taken from IEEE Std. 741. Note that IEEE Std. 741 provides redundant, and differently staged timed disconnects for undervoltage, but *only suggests a time-delayed alarm function as suggested protection practice.*[26]

Figure 3.8.3-1: Protection of Class 1E power systems and equipment



In the USA, the Nuclear Regulatory Commission (NRC) standard review plan NUREG-0800, Branch Technical Position BTP 8-6 Rev03 entitled "Adequacy of Station Electric Distribution System Voltages" recommends use of redundant coincidence logic to determine when a degraded voltage condition exists and requires in Section 1.c.iii:

- "The under-voltage protection should include coincidence logic on a per bus basis to preclude spurious trips of the offsite power source."

26. The need to upgrade IEEE Std. 741 to address overvoltage protection that could damage electrical equipment is further discussed in Appendix B as an essential required upgrade to the standard.

The use of redundancy to reduce the likelihood of a spurious actuation of voltage protection logic is a reasonable way to address electrical bus protection vs. reliability concerns.

3.8.4 Conclusions and recommendations

Assuring appropriate design margins per the use of IEEE Std. 741 and use of redundant voltage protection logic both contribute to assuring high likelihood of providing required protection while minimising the possibility of spurious operation.

We recommend that in order to assure high probability of detection in time to prevent equipment damage that:

- A systematic analysis of equipment voltage requirements be performed to determine ranges of voltage where specific Class 1E equipment can be operated using offsite AC power.
- Points should be determined where protective action must be initiated to separate the bus from offsite power, start onsite diesel generators, and reenergising local buses using the onsite power sources. Such operating points should have appropriate margins to assure avoidance of spurious operation.
- Redundant high reliability voltage detection circuitry should be provided to initiate the protective action with coincidence logic to assure no single voltage detection circuit failure will initiate spurious protections.

3.9 Level of protection of safety buses

3.9.1 Introduction

The Forsmark incident was initiated by a short circuit in a switchyard outside the plant which resulted in an electrical transient. Due to improper protection devices in the responsibility of the grid operator as well as faults and shortcomings in the installations of the normal and emergency power supply of Forsmark 1 the transient resulted in the loss of two of four divisions of the emergency power system (EPS). The transient actually occurred was not expected in the design of the protection devices of the EPS.

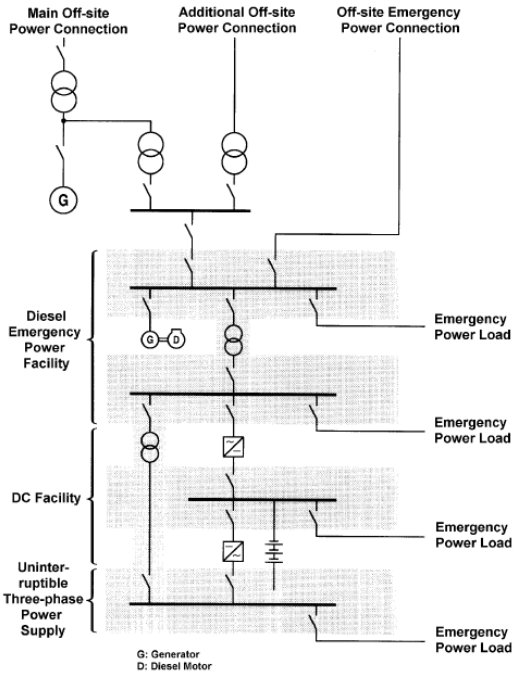
3.9.2 Scope

Scope of this section is a review of the requirements on the protection devices for buses of the emergency distribution system (EDS). Not within the scope of this section are the monitoring and protection devices for the diesel generator safety buses which are used for the detection of loss of offsite power.

3.9.3 Emergency power supply (EPS)

The safety systems in the NPPs require electrical power to perform their safety functions. Thus, the electrical power has to be provided in operational states, under design basis accident conditions and in the event of certain severe accidents. The systems important to safety (safety and safety related loads) are connected to the EPS. Hence, the purpose of the EPS is to provide the necessary power in all relevant conditions within the design basis. So, the EPS serves as a support feature for safety systems. Figure 3.9-1 shows a schematic representation of the different parts of the plant power supply.

Figure 3.9-1: Schematic representation of one division of a German plant power supply (KTA 3705)[27]



Following IAEA Safety Guide NS-G-1.8, the boundaries of the EPSs are at the input terminals of the circuit breakers used to connect the EPSs to the normal and the alternative power supplies and at the input terminals for the emergency power loads. The EPS includes buses of the electrical distribution system as well as the following components: transformers of the EPS, emergency diesel generators (EDG), rectifiers/inverters, rotary converters, batteries.

Usually, the components (loads) are equipped with protection features to prevent damages from the components (component protection). These protection features are within the boundary of the respective component, i.e. the component inverter includes the overload protection logic of the inverter.

Protection devices designed to prevent the propagation of damages due to electrical faults like short circuits and overcurrents are installed at the safety buses. Additionally, a monitoring and control system (not within the scope of this section) is installed at the EDG buses[28] to detect a degradation of the normal power supply and to actuate the start of the EDGs.

27. KTA-Geschaeftsstell, Switchyards, Transformers and Distribution Networks for the Electrical Power Supply of the Safety System in Nuclear Power Plants, Safety Standard KTA 3705 (06/1999).

28. Refer to Appendix B.2 discussion of German standard KTA 3702. The setpoints for protection of the safety system follows in principle the philosophy for non-safety systems. A diesel generator differential protection can be set to actuate at 5% of rated current. Such a setting increases the risk of spurious operation. With a setting of 50% of rated current, the risk of spurious operation is reduced, but also the sensitivity. A recommendation or guide on how to establish an optimum setpoint would be beneficial.

3.9.4 Requirements for protection devices of safety buses

The distribution system of the EPS is necessary to provide power to safety system loads, and other safety related loads under all required operating conditions of the EPS. Hence, the operating conditions cover a wide range of voltage and current values. In particular, the load sequencing program of EDGs results in voltage and current transients on the AC safety buses. A spurious operation from operational transients should be prevented. Thus, reliable detection and isolation of electrical faults is required.

To meet these goals - selectivity and reliability - the threshold levels of protection devices of safety buses have to be set in a manner that ensures both, the prevention of spurious actuations even under worst operating conditions and reliable detection and isolation of electrical faults.

3.9.4.1 Design of emergency power systems for nuclear power plants NS-G-1.8

The general requirement for protection devices of safety buses is to prevent the propagation of the effects of electrical faults. Therefore, the defective safety bus must be isolated from the electrical fault (e. g. short circuits). Hence, selectivity is required for protection devices of safety buses as stipulated, for instance, in NS-G-1.8:

- "4.34. All main and branch circuits of the EPSs should be protected against overloads, ground faults and short circuits by the use of protective devices, which should be located in enclosures and structures designed to protect the EPSs from the effects of postulated initiating events. The protective devices should be part of the safety system and should be qualified for service for protection against overloads and short circuits."
- "4.35. The protective devices against overloads and short circuits should be properly sized, calibrated and co-ordinated so that the EPSs perform as designed and protect the equipment, buses and cables of the main and branch circuits from damage in overload and fault conditions. The co-ordination of the protective devices should be such that only the faulty part of the EPSs is isolated and the remaining intact circuit is unaffected."

3.9.4.2 German nuclear safety standards

In this section the situation in German NPPs is described as one example of the state of the art. Other countries use different nuclear standards or apply their respective industrial standards, but the requirements may be similar.

In Germany, detailed requirements for NPPs are stipulated in the nuclear safety standards. Furthermore, industrial standards (e.g. the German Occupational Accident Prevention Regulations, DIN Standards and VDE Regulations) are applied to nuclear facilities. The nuclear standards presume that the conventional requirements and standards are met unless other requirements are specified in the nuclear standards and regulations.

The respective requirements for the EPS are stipulated in the safety standards KTA 3701, 3702, 3703, 3704 and 3705.

Requirements for protection devices of safety buses, transformers and motors

The basic requirements regarding protection and selectivity protective devices are stipulated in the paragraph protection and selectivity of the safety standard KTA 3705:

- "3.2 (1) The layout of the circuits, the design of the electric components and the selection and adjustment setting of the protective features shall assure that faults within

the switchyards, transformers, distribution networks and power loads are detected and the necessary disconnections carried out. …"

- "3.2 (2) The protective features shall be designed such that faults are reliably registered, that the required shutdowns are performed and that erroneous actuations are prevented."
- "3.2 (4) In the case of a failure of a short-circuit protective feature, the affected component shall be disconnected by the closest upstream protective feature. … A non-tripping of safety fuses (melt fuses) need not be postulated."

Additional requirements are stipulated for the short-circuit protection of transformers and the short-circuit and overload protection of motors:

- "3.2 (7) The short-circuit protection on the high voltage side of a transformer shall meet the following conditions …:

  a) The immediate short-circuit trip on the high voltage side of the transformer should be adjusted to such values that it will not cause any disconnection of the transformer due to the sudden inrush current of the transformer or due to a short circuit in power load feeder branches on the low voltage side.

  Note:

  This requirement can be met if, e.g., the immediate short circuit trip is set to a value greater than or equal to 1.2 times the maximum short-circuit current of the low voltage side with respect to the high voltage side, and greater than or equal to 1.2 times the sudden inrush current of the transformer.

  (b) The overcurrent trip on the high voltage side of the transformer shall be adjusted to such values that the minimum short-circuit current on the bus being fed by the low voltage side will cause the transformer to be disconnected.

  Note:

  This requirement can be met if, e.g., the overcurrent trip is set to a value smaller then or equal to 0.8 times the minimum short-circuit current of the low voltage side with respect to the high voltage side."

- "3.2 (8) the short-circuit and overload protection of motors shall meet the following conditions …:

  (a) Immediate short-circuit trips shall be adjusted to such values that inrush current peaks will not cause a disconnection of the motor.

  (b) Overload protective features for motors of machines shall be adjusted to such values that the number of successive starting cycles required with respect to process engineering will not cause any disconnection of the motor. As far as the design and adjustment setting of the protective features of continuous duty successive starting cycles required with respect to process engineering will not cause any disconnection of the motor. As far as the design and adjustment setting of the protective features of continuous duty motors are concerned, at least two successive startup operations from the cold state or one startup operation with the motor at operating temperature shall be postulated in specifying the minimum startup voltage. Overload protective features shall not cause disconnection of the motor when the motor is operated at the lowest specified static terminal voltage for the specified period of time.

  Note:

  The startup cycles to be applied to the thermal design of motors are specified in KTA 3504, Sec. 7.2, para. 3. (c) Winding temperature protective features should be

> provided for the overload protection of control drives. If current dependent overload protective features are used these shall be adjusted to such values that they will not cause any disconnection of the motor in the specified operating mode (in the case of control drives, at least one CLOSE - OPEN – CLOSE operating sequence)."

Requirements for protection devices of components

Requirements and boundary conditions concerning the calculation of short-circuit currents are also given in the safety standard KTA 3705.

Component specific requirements are stipulated in the safety standards KTA 3702 for EDGs (not within the scope of this section), in the safety standard KTA 3703 for AC/DC converters and batteries and in the safety standard KTA 3704 for DC/AC inverters. Therein requirements for component protection devices are given.

In the safety standard KTA 3703 a protective disconnection for rectifiers is required for:

- input voltage (AC-side of the rectifier) HIGH
- output voltage (DC-side of the rectifier) HIGH
- short-circuit
- voltage band out of range
- actuation of thyristor/control circuit fuses

A protective disconnection of the battery units is not required according to the nuclear safety standards.

For inverters a disconnection by the component protective devices is stipulated for:

- input voltage (DC-side of the converter) LOW
- output voltage (AC-side of the converter) HIGH
- overcurrent protection (motor and generator) HIGH
- rotary speed/frequency HIGH and LOW in the safety standard KTA 3704.

The requirements for static inverters given in the safety standard KTA 3704 differ from the required protection equipment for rotary converters:

- input voltage (DC-side of the converter) LOW
- output voltage (AC-side of the converter) HIGH
- short circuit protection

3.9.4.3 Review of German NPPs due to Forsmark

The German nuclear non-mandatory rules have been updated. The draft version of the current update has been specified due to the Forsmark incident. Now, the requirement of the draft regarding protective devices reads:

> "Protective installations on equipment units and auxiliary installations are designed such that if an equipment unit is challenged by the instrumentation and control installations of the safety system, the protective installations will as a rule not become operative un-less the possible consequential damage will put the safety of the plant more at risk than the failure of the equipment unit".

The protective installations as a rule are designed such that the priority of the instrumentation and control functions of Category A (RPS and ESFAS, A.N.) over the protective installations is ensured.

If priority over the instrumentation and control functions of Category A (RPS and ESFAS) is necessary in a protective installation, this protective installation is required to fulfill the requirements of Category A (RPS and ESFAS, A.N.).

The requirements of Category A for the protective installations will not be required if it can be demonstrated that failures of protective installations are so unlikely that inadvertent actuations that would be caused by such failures can be excluded.

3.9.4.4 Further activities of German licensees

This paragraph gives an overview on the actions taken by the German licensees after the Forsmark incident. The licensees initiated a review program due to the Forsmark incident and the recommendations of GRS, as published in the information notice. The goal of the review is to demonstrate the robustness of the electrical power supply against electrical transients and to identify necessary improvements.

The review is done in two steps. The first step comprises generic issues concerning all plants. For instance, the identification of an enveloping electrical transient at the 27 kV level (outlet of the main generator) is identified in the first step. Therefore, electrical transients as caused by switching operations, grid disturbances, lightning strikes, starting currents, short circuits and earth faults are considered. The frequency spectrum of the transients varies from 0.1 Hz up to 15 MHz. Additionally, the operating experience is taken into account. For instance, a voltage transient up to 136% of nominal voltage at the generator terminals occurred due to a failure of the oscillation damping device. Thus, a single enveloping transient covering the whole frequency spectrum cannot be defined. Another issue of the first step is to create models for the propagation of electrical transients within the NPP.

The second step includes the assessment of the impacts of the electrical transients to the specific plants. Consequently, improvements for the specific plants will be derived. Therefore the results of the first step are used[13].

3.9.5 Conclusion and recommendations

3.9.5.1 Recommendations for reviewing the EPS

External or internal electrical transients shall not result in an unacceptable impairment of safety related loads. Thus, a robust EPS is required. To improve the robustness of the EPS a detailed knowledge of the installed equipment and its protection devices is necessary. Hence, the existing EPS and the connected loads should be analysed and documented. The following issues should be considered:

- operating range of the loads
- protection devices of the loads, limit values in voltage and current and tripping behaviour
- protection devices of the safety buses, limit values in voltage and current and tripping behaviour

In the next step, enveloping electrical transients should be identified.

Finally, the robustness of the EPS against these enveloping electrical transients should be verified by models and simulations. The simulations should cover conditions such as voltage excursions, switching transients, filtering harmonics, load driven variations, lightning storms:

- different operational states
- several initiating events

- failures of operational or protection devices
- a sensitivity analysis

Because of the sensitivity of the solid state equipment, the power systems should demonstrate the voltage spikes and its period that could be let through within the constraints of the protection system.

3.9.5.2 Recommendations for refitting the EPS

An EPS may be robust against electrical transients, but over the life time of the plant the robustness can be unintentionally impaired by plant modifications, design changes and modernisation. The new susceptibility could be caused by the installation of modern, e.g. digital, control systems which are less robust (more sensitive) against electrical transients, or produce unexpected performance or interaction with the old equipment and the EPS. Thus, it is good practice to:

- verify the specifications given by the technical data sheets by tests;
- identify implemented protection devices of the unit and verify whether they are adequate, remove or disable undesired features and co-ordinate their settings with the existing protection devices of the EPS;
- reassess the limit values in voltage and current of the protection devices of safety buses along with a system modification. Consider an equipment specific test programme to validate its protection capability for the sensitive downstream equipment;
- implement the new loads step by step, e.g. one division per outage, to gain operating experience and identify hidden flaws.

3.9.6 References

1. Safety Standard KTA 3701: General Requirements for the Electrical Power Supply in Nuclear Power Plants, KTA-Geschaeftsstelle. June 1999
2. Safety Standard KTA 3702: Emergency Power Generating Facilities with Diesel-Generators Units in Nuclear Power Plants, KTA-Geschaeftsstelle, June 2000
3. Safety Standard KTA 3703: Emergency Power Facilities with Batteries and AC/DC Converters in Nuclear Power Plants, KTA-Geschaeftsstelle, June 1999
4. Safety Standard KTA 3704: Emergency Power Facilities with DC/AC Converters in Nuclear Power Plants, KTA-Geschaeftsstelle, June 1999
5. Safety Standard KTA 3705: Switchyards, Transformers and Distribution Networks for the Electrical Power Supply of the Safety System in Nuclear Power Plants, KTA-Geschaeftsstelle, June 1999
6. Safety Standards Series No. NS-G-1.8: Design of emergency power systems for nuclear power plants, International Atomic Energy Agency, Vienna 2004
7. Information Notice regarding the Forsmark-1 incident 2006, Gesellschaft für Anlagen- und Reaktorsicherheit mbH, WLN 2006/07
8. VGB Powertech, Untersuchungsprogramm zum Einfluss von Spannungstransienten auf das Notstromsystem, 24.10.2007

3.10 Digital protective relays

3.10.1 Introduction

Protective relays are essential parts of electrical systems and play a very important role in ensuring and adequate protection of the electrical busbars and equipments. The safety related systems should provide for the adequate protective actuation in case of an electrical failure while preventing unintended spurious actuations that could result in loss of power to essential systems.

Digital protective relays are replacing the old generation of electro-mechanical relays and the electronic relays due to obsolescence and to realise the benefits of higher performance.

3.10.2 Scope

As digital protective relays are used more frequently, this section examines the potential weaknesses of these relays in case of electrical transients, based mainly on operating experience.

3.10.3 Digital protective relays

Digital protective relays are generally used in existing NPP to replace obsolete electromechanical or electronic devices. They present many advantages as replacement parts due to their versatility, self-diagnostic capability, and the ease to adjust the settings. However, they may cause unanticipated features that were not present in the previous relay types. Both types of protective relays are susceptible to common cause failure if the basic functional design requirements were inadequate or were based upon an incorrect understanding of protection requirements.

3.10.4 Operating experience

3.10.4.1 In Belgium

As mentioned earlier, digital protective relays were used to replace obsolete electromechanical relays in a Belgian NPP. The relay modernisation was completed with verification of the relay specifications and appropriate changes to the setpoints. The digital relays were fully tested before startup and no problems were identified until an electrical short circuit occurred on a 6 kV pump motor. The protective relay did not actuate the switchgear as expected and the fault was finally eliminated by the backup protective relays at the busbar level, resulting in the complete loss of all the 6 kV users of the electrical board. The problem was investigated and the root cause was identified as a failure from high intensity current produced by the short circuit. The protection circuit installed on the input of the relay was not designed or rated to withstand very high currents. This kind of failure[29] could not be identified by on-site testing because the testing system was set to *simulate the lowest value of short circuit current and verify relay actuation*. It should be noted this specific failure mode was related to inadequate specification of functional requirements and could have also occurred with older relay devices.

Other failures of digital protective relays were observed with software errors (errors in algorithms) not detected by the testing program.

29. More information on this event is available in IRS Event #7682.

3.10.5 Discussion

Digital protective relays are less sensitive than electronic or electromechanical devices to environmental conditions. They present a number of advantages against the old types of protective relays, e.g. intermesh of flexibility and ability to improve the protection of electrical components for more complicated scenarios requiring protective actions, such as: parameter rate of change.

However, the capability to accommodate more complicated scenarios requiring protective actions can introduce greater levels of complexity, which requires consideration of new types of failure modes not found on older electromechanical relays that operated based upon simpler functional requirements that in some cases were easier to verify. This is in particular the case with transients that were not necessarily anticipated in the design stages.

Experience shows that the compatibility between old and new devices has to be carefully looked at to prevent either spurious actuation or miss actuation of the relay. The testing console often does not detect this kind of potential failures.

3.10.6 Conclusions and recommendations

The design and testing should address the software lock up, computer operating system, software and hardware lock up, the impact of rebooting on actuated devices and systems during rebooting and at the end of rebooting on nuclear safety systems. The preoperational tests should consider simulated conditions of failure modes from all connected systems and actuated components.

See further considerations on software based systems in Section 3.5.4

The post modification testing for digital devices should include a verification of all applicable safety functions.

3.11 Power supply requirements for nuclear power plant operator information systems

3.11.1 Introduction

The operators in nuclear power plants have to rely on information available to them to operate the plant without intimate knowledge of design details. Different type of information is generally provided to NPPs operators:

- Modern control rooms are equipped with modern integrated displays with systems status, displays, recorders, annunciators
- Status lights: e.g. indicating that an equipment is running or not, or that a valve is open or closed
- Indicators: giving the value of a given parameter (temperature, pressure, flow rate, etc.)
- Recorders: in addition to provide for the value of a parameter, they provide for information on trends
- Alarms: provide for audible and/or visible signals when parameters (or their trend) deviate from specified limits/setpoints.

In addition, computers can provide for complementary information on the history in log files. Modern digital technology can further provide for information better "formatted" (coloured displays, graphical parameter display, etc.) to assist the operators in monitoring the plant parameters.

All these systems need to be powered by reliable electrical power supplies. Recent experiences showed that this information could be partially or even totally lost by failure of their respective power supply. The failsafe design may be acceptable a safety channel in the actuation system, however, the loss of all annunciators in channel/train may cause undesirable challenges for the operators during plant events/emergency conditions.

3.11.2 Scope

This section discusses electrical power supplies to the NPP operator information system.

Several regulations, norms and standards are mentioned as examples. It is not the intent to cover all existing regulations in this area.

3.11.3 Information systems

3.11.3.1 Norms and standards

According to the country, different norms and standards are used. A number of countries use IEEE standard or norms which are very close to the requirements found in the IEC's.

As far as electrical power supplies are concerned, the following top level IEEE standards apply:

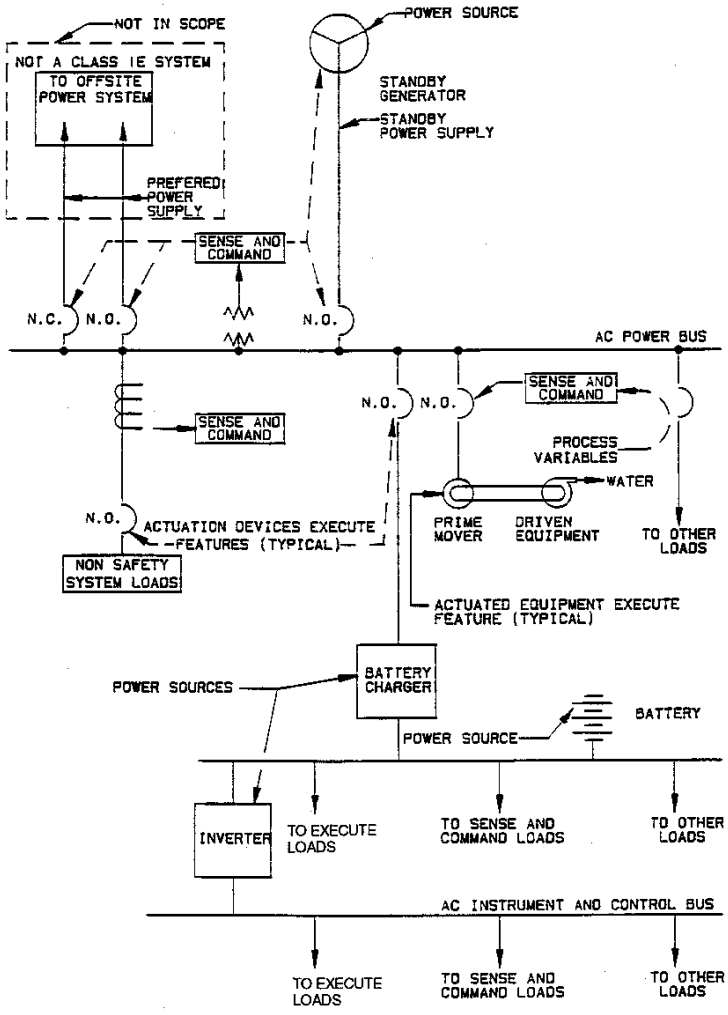
- IEEE Std. 308-2001: Criteria for Class1E power systems
- IEEE Std. 379-2000: Single failure criteria for nuclear power generation stations
- IEEE Std. 603-1991: Standard criteria for safety systems for nuclear power generating stations
- IEEE Std. 741-2007: Standard criteria for the protection of Class 1E power systems and equipment in nuclear power generating stations
- Regulatory Guide 1.97: Criteria For Accident Monitoring Instrumentation For Nuclear Power Plants Rev, 4

The main requirements in matter of electrical power supplies can be summarised as following:

- Redundancy: there must be several divisions available to cope with a single failure.
- Independence and physical separation: the concept of single failure assumes that a given failure in one division would not propagate to the others. This requires that the divisions should be separated from each other and independent.
- Quality of equipment: in order to grant credibility to the single failure criteria, reliability of the components must be assured and this can be translated in general terms of quality.
- Qualification: safety related equipment must be capable to operate under adverse conditions such as earthquake or high temperature and pressure and the ability to operate under such conditions must be demonstrated by adequate qualification programs.
- Capability: the power supplies to class 1E systems should be capable to provide for the needed power under the most severe environmental conditions.
- Surveillance: systems should be in place in order to monitor essential parameters of the power supply.
- Testing: periodic testing is required in order to demonstrate that the essential features of the systems including the protection systems are maintained.

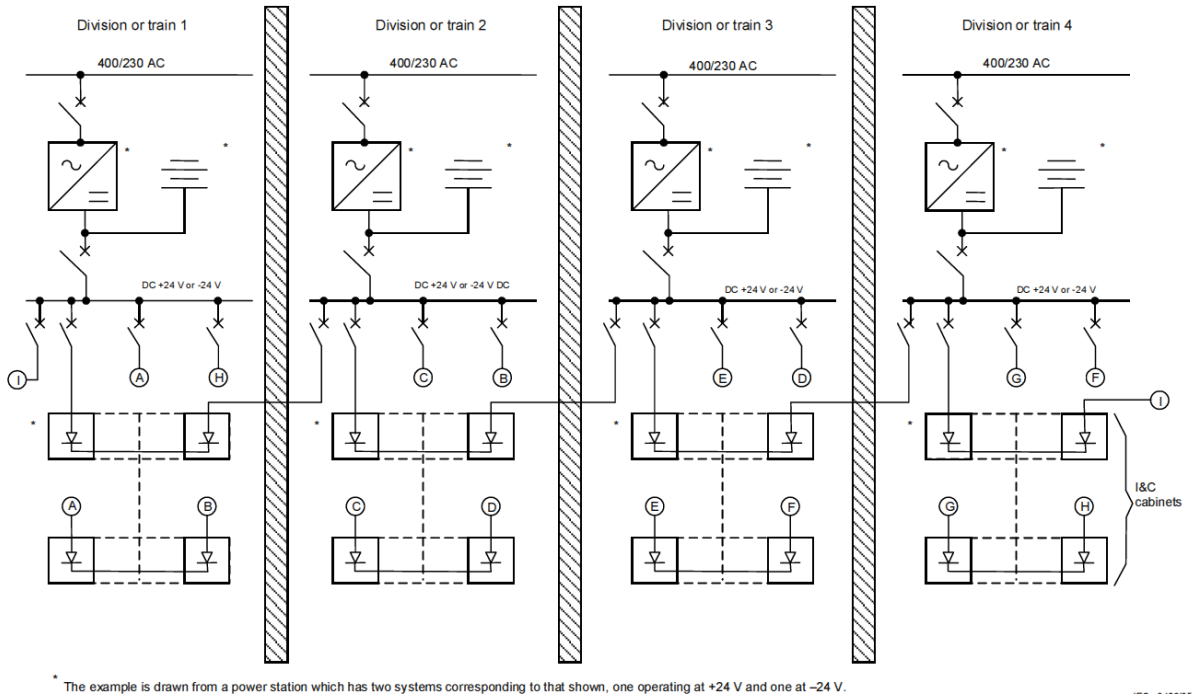
Figure 3.11.3-1 reproduces a typical power supply system as defined by IEEE standards.

Figure 3.11.3-1: Typical one-line diagram as defined in IEEE Std. 308-2002



The IEC 61225 (2005) "Instrumentation and control systems important to safety – Requirements for power supplies" addresses specifically the needed power supplies. The general requirements are very close to the IEEE standards (and IEC is referring to IAEA safety guide NS-G-1.3). It foresees redundant power supplies for systems important to safety without actually requiring for redundancy ("The redundancy of an I&C power supply system covered by this standard shall be determined by the plant design criteria which apply to the I&C systems."). A typical electrical distribution system according to IEC, with redundant power supply for each division, is showed in Fig. 3.11.3-2.

Figure 3.11.3-2: Typical electrical distribution system for I&C important to safety with redundant power supplies (IEC 61225)



3.11.3.2 Regulatory requirements

The USNRC has issued a number of regulatory guides describing acceptable approaches to the design of safety related electrical power systems. These are:

- RG 1.32 (power systems) endorses IEEE Std. 308 with no sharing of DC power systems on multi-unit sites
- RG 1.53 (SFC) endorses IEEE Std. 379
- RG 1.153 (safety systems) endorses IEEE Std. 603
- They generally endorse corresponding IEEE standards with some exceptions.

In other countries, such as Finland, YVL guides (YVL 5.2) provide similar requirements to those set up by the USNRC, but with some additional demands:

- The single failure criteria must be fulfilled taking into account that another division could be unavailable for maintenance, test or repair.
- The house load operation is required as a potential electrical power supply source.

The KTA guides from Germany (KTA 3701/3703/3704) have requirements similar to YVL. However, for DC electrical power supply system, redundancy as showed on Fig. 3.11.3-3 is required. As AC electrical power supply systems are concerned, a "plain" uninterruptible power supply is considered to be acceptable (see Fig. 3.11.3-4).

Figure 3.11.3-3: Typical one-line diagram for DC electrical power supply as by KTA 3703

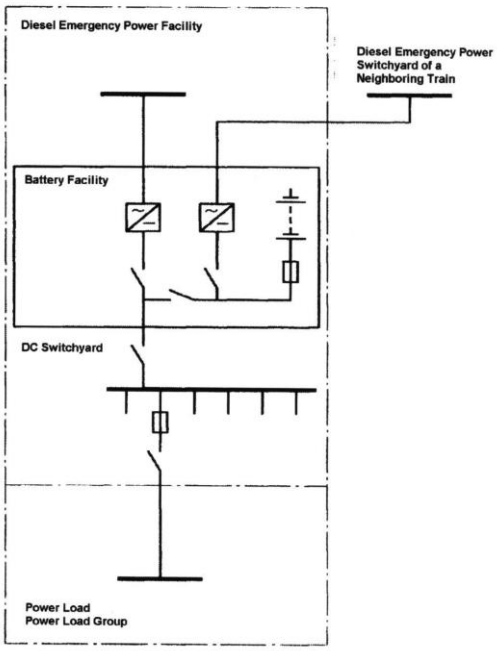
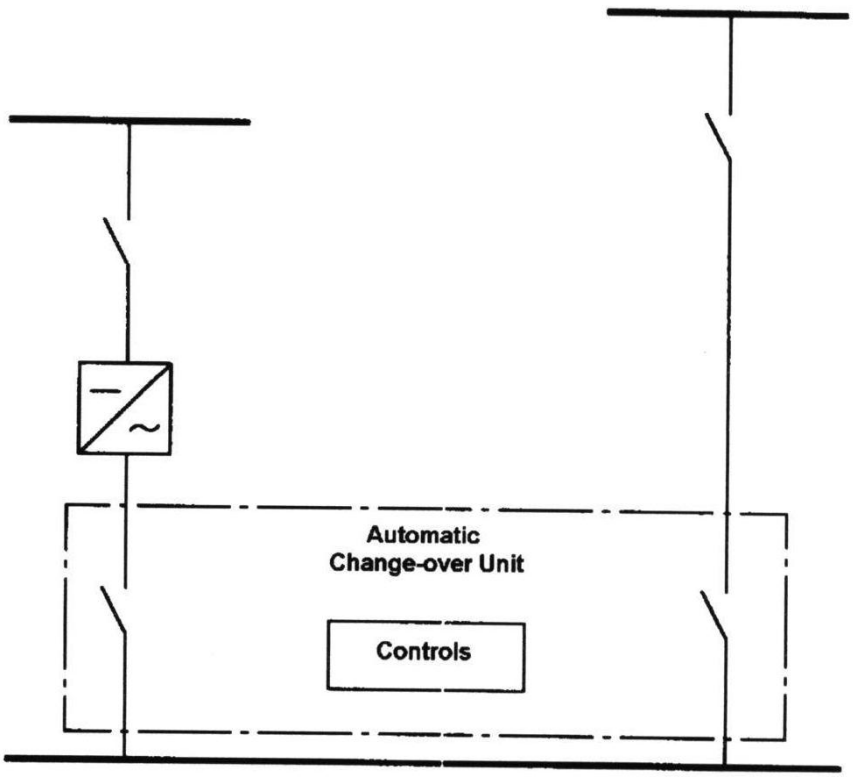


Figure 3.11.3-4: Typical one-line diagram for AC electrical power supply as by KTA



In order to facilitate accident management critical information such as control rod bottom lights, reactor coolant system integrity, relief valve open status, etc., there should be diverse power sources to provide uninterrupted information for the operators.

3.11.3.3 Plant contingencies

The so-called "combined" loss of onsite power supply can be defined as a loss of one or more Class 1E UPS with no back-up provided by the transformer. Another possible combined loss of power supply would be the loss of more than one division of DC power supplies.

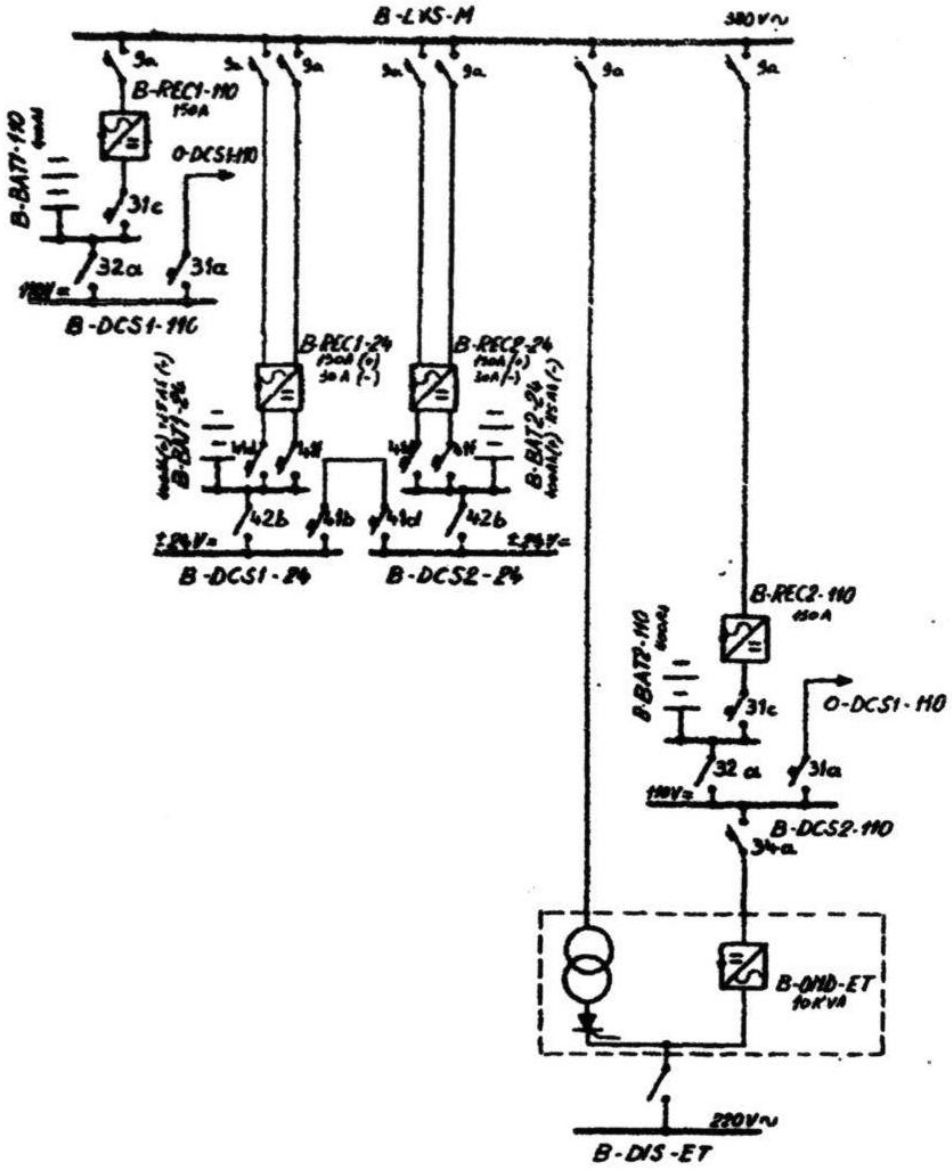
All these failures were generally considered as not being credible and no design provisions, procedures or investigations were performed to address these cases. Experience shows that these occurrences could happen and that the operators have significant difficulties to recover from the condition, without appropriate guidance.

Recent investigations in a Belgian NPP showed that the loss of two out of three Class 1E regulated 220 V AC is difficult to manage and that a specific procedure had to be written in order to provide for adequate guidance to the operators.

3.11.3.4 Existing and future designs

As for existing design, the electrical power supply system for display systems in control room is generally not redundant. Each division has a separate class 1E or equivalent electrical power supply and the loss of one division leads to losing the information supplied by this division (see example in Fig. 3.11.3-5).

Figure 3.11.3-5: Existing NPP - Class 1E AC electrical power supply



New designs such as the US-EPR or ESBWR provide for redundant electrical power supplies for each division as shown on the one-line diagram in Fig. 3.11.3-6 and Fig. 3.11.3-7.

Figure 3.11.3-6: US EPR – Class 1E DC electrical power supply

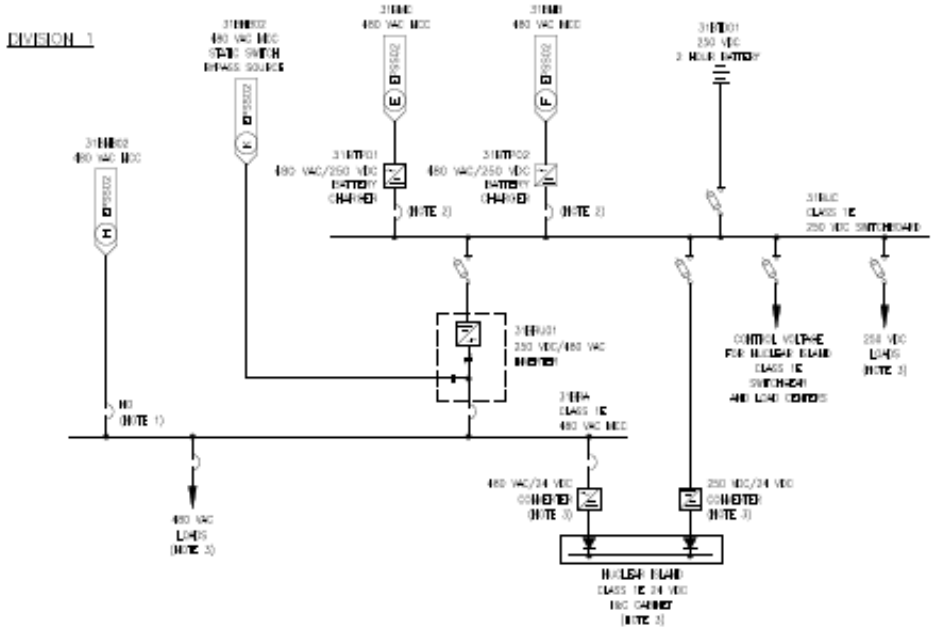
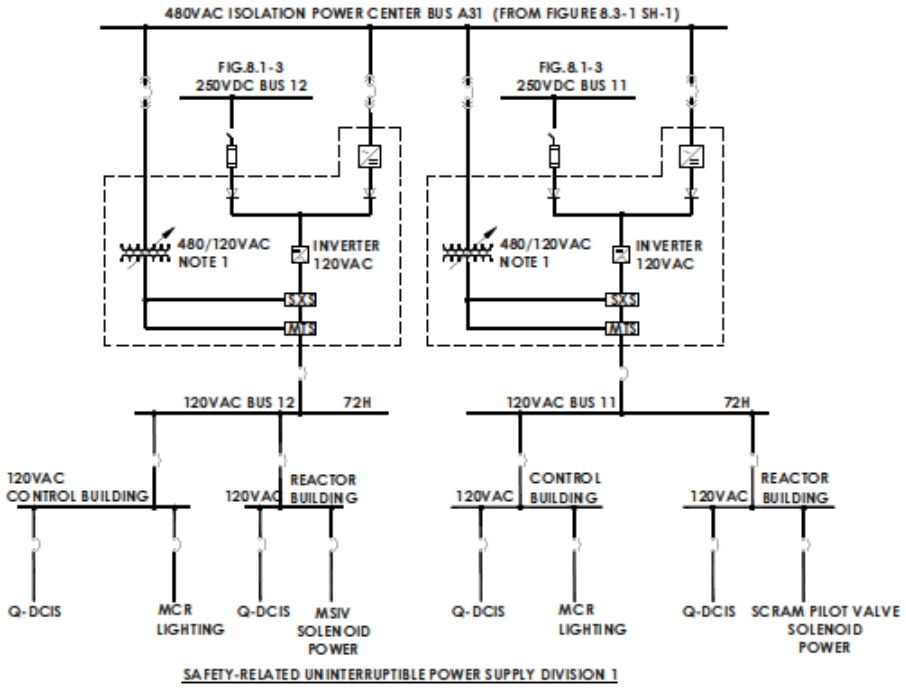


Figure 3.11.3-7: ESBWR AC Class 1E electrical power supply – 480/120V transformer is not Class 1E

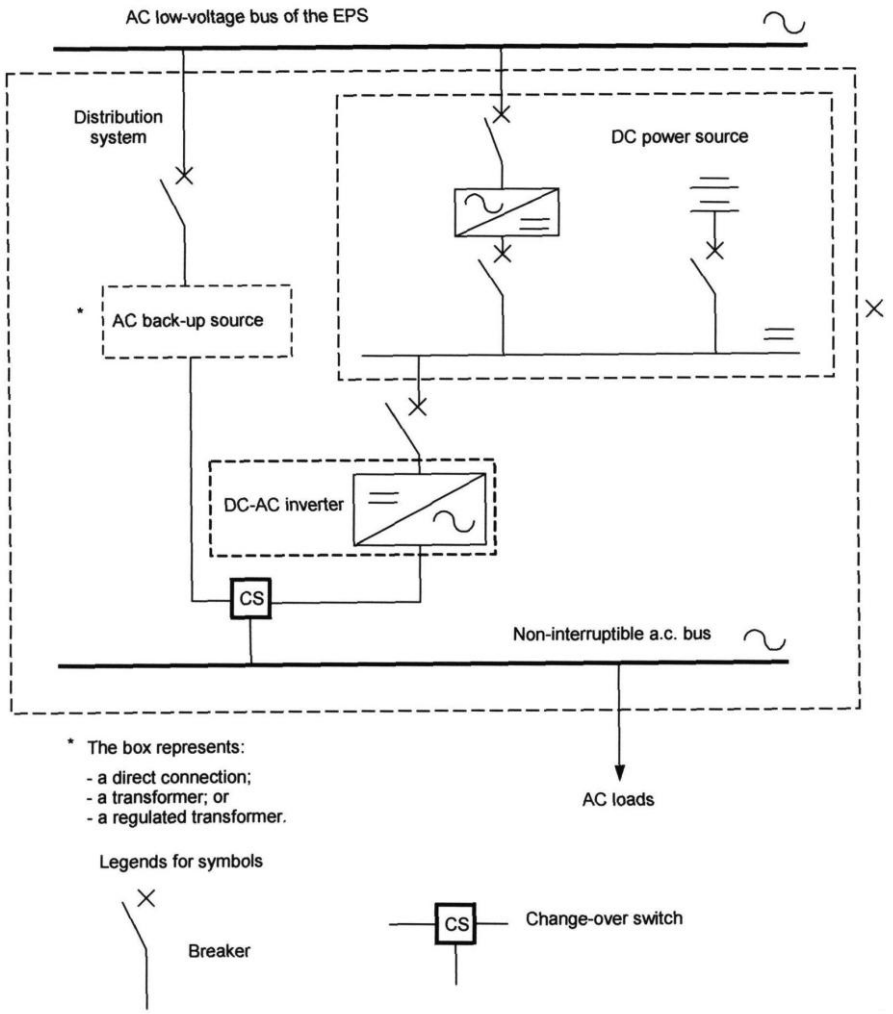


The coupling of adjacent power supplies through diodes may have some inherit benefits, however it is acceptable for over current and over-voltage incidents that could fail the diodes on the conduction and bring down all the interconnected trains. Addition of two swing UPSs, capable of connecting to either pairs of the train at a time would be a desirable solution.

3.11.4 Conclusions and recommendations

As mentioned in the introduction, electrical power supply to control room display systems is important in order to allow the operators to monitor and control the NPP. The existing requirements, standards and guidance generally do not provide for redundant power supply for information systems in a given division. The single failure criterion is assumed to be met if the other divisions are still powered. In case of AC power supply, the use of UPS is assumed to provide reliable and redundant power supply. In this case, the redundancy is considered to be fulfilled by either providing power from the batteries in case of failure of the rectifier (or its power supply) or by the by-pass transformer in case of failure of the inverter (assuming that the power supply to the input of the transformer is ensured). The single failure analysis seems not to consider the failure of the static commutation switch and associated control logic that ensures no-break transfer from the inverter to the transformer (see Fig. 3.11.4-1). Moreover, in some designs, the by-pass transformer is not considered to be a Class 1E component and thus cannot be relied upon to compensate for a failure of the inverter. Experience shows that, in some UPS designs, even if the switchover to the by-pass transformer works as designed and the input of the transformer is powered, depending on the failure of the inverter, the system could not ensure appropriate power supply to the Class1E loads.

Figure 3.11.4-1: UPS typical arrangement (from IEC 61225)



These observations mean that one should possibly investigate the design and operation of UPS systems in order to verify their robustness and eventually a need to provide for redundant (and diverse?) UPS systems inside each safety related division.

Operating experience with UPS could also be investigated and it might be worthwhile to add this kind of systems in the list of OECD ICDE project.

In order to accommodate CCF and single failures, the design should have adequate diversity to provide uninterrupted display of critical reactor parameters and successful operation of ECCS.

The control room should have guidance in place to implement remedial actions to accommodate power system failures affecting more than one division.

3.12 Nuclear power plant operators response to electrical events

3.12.1 Introduction

Before considering operator response to events such as a loss of electrical power on a given busbar or electrical board, it seemed useful to investigate a little about the requirements linked to the electrical power supplies.

In order to maintain adequate electrical power supply to the class 1E systems and components, several sources can be used from the external grid to internal diesel generators, up to and including specific diverse SBO diesel generators.

Operating procedures are needed to be able to respond promptly and correctly to loss of electrical power events. Experience indicates that the loss of some safety related busbars and electrical boards can be very confusing for operators. It may difficult and complex to restore the situation because of spurious actions and signals that can be generated.

Procedures are also needed to provide guidance to operators while having contacts with the grid operator.

3.12.2 Scope

This section deals with the expected operator response to electrical events such as the loss of electrical power supply and the potential accompanying voltage transients.

3.12.3 Preferred power supply (PPS)

3.12.3.1 Norms and standards

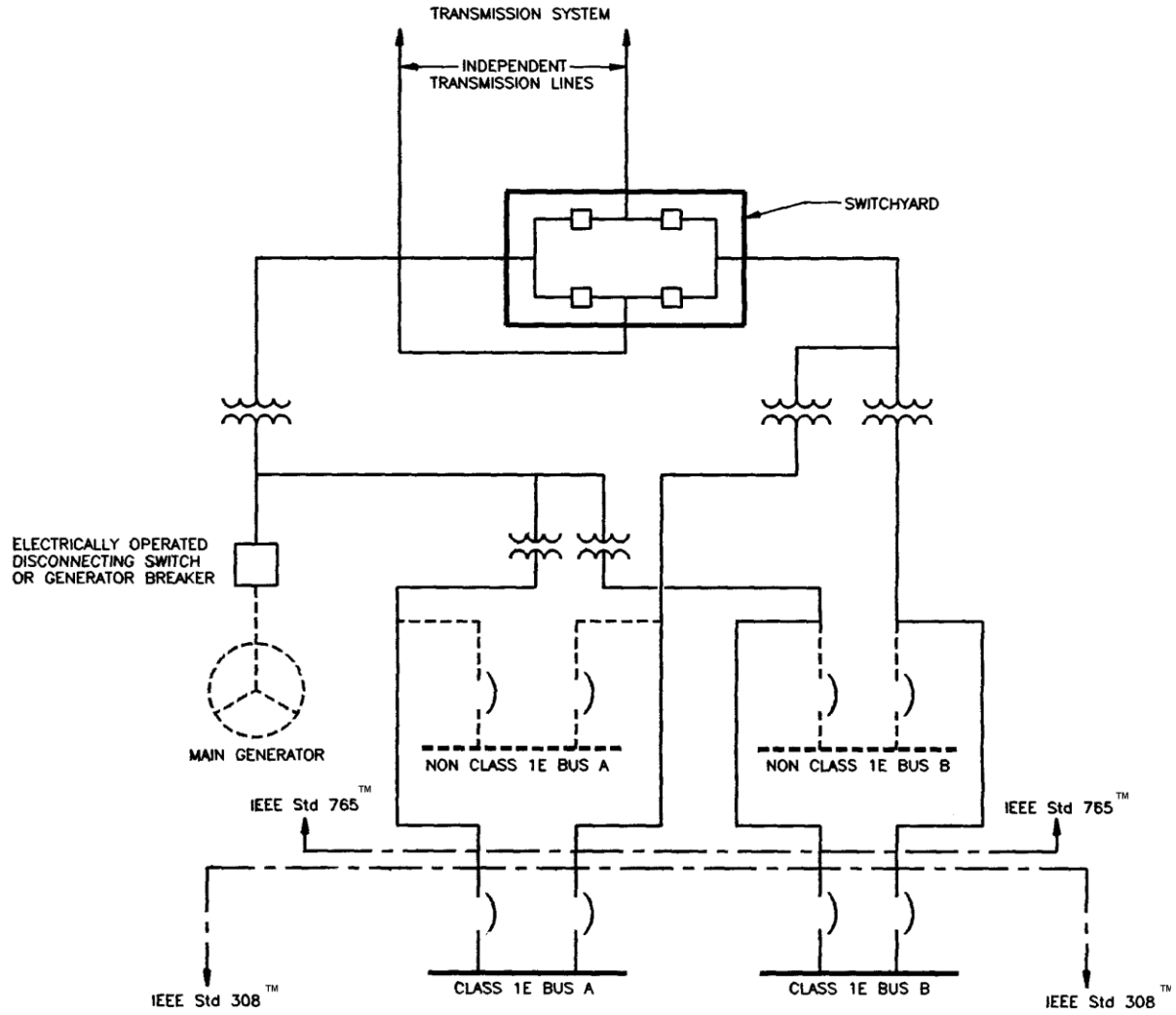
Taken as an example, the IEEE 765-2006 provides requirements related to the electrical power supply. This standard also provides some guidance in establishing relationships between the NPP operator and the different organisations involved in the external power supply such as:

- The Independent System Operator (ISO)
- The Transmission System Operator (TSO)
- Other organisations (e.g. grid regulator)

The IEEE defines the preferred power supply as being two separate, independent transmission lines supplying the local switchyard close to the NPP (see Fig. 3.12.3-1). Note that this design configuration does not have the capability of house load operation. Other configurations, with additional switchgears or transformers, can provide for this capability and can have more flexibility. An example of enhanced preferred power supply is available in the IEEE standard.

Transmission and net stability studies have to be performed to demonstrate the reliability of these electrical power supplies. These studies can result in specific grid configurations that have to be adopted in order to maintain sufficient independence between the two supplies, for example.

Figure 3.12.3-1: Preferred power supply defined in IEEE 765-2006



3.12.3.2 Regulatory requirements

USNRC regulatory requirements and guidance are provided in RG 1.32 and RG 1.155. RG 1.32 is endorsing IEEE Std. 308-2001 (with some exceptions). IEEE Std. 765 is not explicitly mentioned in this RG but is referred to in the IEEE Std. 308. RG 1.155 considers mitigation of Station AC Blackout (SBO) and the capability to restore electrical power supply as required by 10 CFR 50.63.

The Finnish YVL guides provide requirements which are very similar to the US ones. However, more stringent conditions are set for the PPS, requiring that two independent rights of ways shall be used and that the design shall be capable of house load operation.

The KTA 3701 guide provides requirements similar to the Finnish ones.

3.12.3.3 Operating procedures

As the electrical power supply and its loss are concerned, different areas can be considered:

- Relationship with the grid operator
- Loss of offsite power supply
- Loss of onsite power supply including the SBO
- "Combined" loss of onsite power supply

Relationship with the grid operator

Procedures to provide guidance to operator in their relationship with the grid operator generally exist. However, the experience shows that this area could be improved by better communication between the NPP operator and the grid operator. This interface, which was naturally covered in a regulated environment, suffers from the regulatory requirements on independence and strict separation between the two actors that is required in a deregulated environment to promote competition.

As well as for normal operation, information exchange has to be effective between the NPP and the grid on incidents, failures or potential weakness in their respective electrical systems.

Information exchange on (scheduled) maintenance activities should also occur between grid operator and NPP. This exchange should not be limited to the information only. In some cases, bilateral collaboration should take place in order to schedule activities that could impair or weaken the reliability of the electrical power supply when it is the most appropriate as regard to the nuclear safety.

Further guidance in this area can be found in the USNRC GL 2006-2. The IEEE 765-2006 also provides in appendix A to this standard guidance on the agreement between grid operator and the NPP; appendix B provides guidance on transmission system studies to ensure voltage adequacy of the PPS.

Loss of offsite power supply

Procedures do exist to provide guidance to NPP operators in case of loss of external power supply. However some complicated situations with (multiple) voltage losses and/or degradations that could be encountered according to the experience feedback are generally not covered.

As related to the reliability of the grid some additional improvements could possibly be made to provide for provisional arrangements in order to prevent potential grid failures. In some other cases, when it is virtually impossible to ensure grid reliability, other actions could be taken, e.g. by reinforcing the reliability of onsite power supplies in case of potential threats to the offsite power supply such as:

- Adverse weather conditions
- Risky maintenance activity on the grid
- Loss of onsite power supply (SBO included)

Loss of onsite power supply (SBO included)

Procedures to cope with the loss of onsite power supply are available. In addition to procedures related to the loss of medium voltage busbars (e.g. 6-10 kV), some specific procedures are foreseen to handle the loss of low voltage AC class 1E electrical boards supplied with UPS. In the same way, procedures are provided to restore the situation in case of loss of DC power supply.

All these procedures generally assume the loss of a single board or division, except for the station blackout. In this latter case, neither the additional loss of UPS supplied systems nor is the loss of DC supplied systems is generally taken into consideration. Improvements in this area could be worthwhile to provide better guidance to the NPP operators. Another line of thinking could be to

improve these power supplies in order to increase their reliability (e.g. redundant power supplies for each division).

"Combined" loss of onsite power supply

The so-called "combined" loss of onsite power supply can be defined as a loss of one or more Class 1E UPS with no back-up provided by the transformer. Another possible combined loss of power supply would be the loss of more than one division of DC power supplies.

All these failures were generally considered as not being credible and no procedures or investigations were performed to cover these cases. Experience shows that these occurrences could happen and that the operators have difficulties to recover the situation, without appropriate guidance.

Recent investigations in a Belgian NPP showed that the loss of two out of three Class 1E regulated 220 V AC is difficult to manage and that a specific procedure had to be written in order to provide for adequate guidance to the operators.

3.12.4 Conclusions and recommendations

As mentioned above, operator response to voltage transients or grid degradations could be improved by providing additional guidance. The relationship between the grid operator and the NPP operator plays an important role in this area.

It is recommended to investigate and reconsider the following topics:

- Agreements and arrangements between grid operator and NPP operator
- Availability of operating procedures to handle power supply losses and/or degradations, even in complicated operating conditions
- Improving the reliability of power supplies needed to provide plant information to the operator.

4. CONCLUSIONS AND RECOMMENDATIONS

4.1 Conclusions

Current[30] nuclear power plant safety relies on the availability of preferred power sources for operation of emergency core cooling and decay heat removal systems. The defence in depth of nuclear power plant electrical systems can be viewed as a combination of the following design and operational practices:

- Preventing electrical grid and plant generated electrical faults which are capable of interrupting the preferred source of power to decay heat removal systems,
- Robustness of nuclear power plant electric power systems to cope with electrical grid and internal plant generated electrical faults without further fault propagation or degradations to safety related equipment,
- Continuously improving nuclear power plant and external transmission system operator training, procedures, and information capabilities to deal with possible degraded electrical systems,
- Coping capability of nuclear power plants to deal with severe electrical grid and internal plant generated electrical faults, and:
- Ability to recover offsite electric power by co-ordinated actions of the nuclear power plant and transmission system operator.

Recent international operating experience has indicated that generally accepted design practices and standards which have been relied upon for decades to assure defence in depth have not kept pace with ongoing changes in technology and in changes in the organisation of electrical suppliers. These ongoing changes, if not commensurately addressed by improved practices and design standards could eventually result in events with serious nuclear safety implications. The sequence of events observed at Forsmark in 2006 and Olkiluoto in 2008 are such accident precursors.

Examples of major technology changes include: replacements of robust, but maintenance-intensive, motor-generator sets with less robust solid state UPS units for supplying vital control and instrument power, and replacement of older hardwired relay-based control and protection devices with microprocessor-based devices which can be more sensitive to degraded input power supplies.

Examples of changes in the organisation of electrical suppliers include the reorganisation of electrical industries into separate generating companies, transmission system operators, and local electrical distribution companies who may have competing market interests on where power is needed.

The DIDELSYS Task Group recognises that for nuclear power plants operating throughout the world to maintain their current safety levels while these external changes are going on, efforts must be initiated to commensurately upgrade older design practices and standards.

30. Advance light water reactor designs in the future will rely upon passive safety features to assure emergency core cooling and decay heat removal. These designs will still rely on safety related electrical power sources to power operator controls and displays.

4.2 Recommendations

The DIDELSYS Task Group performed: a review of recent operating experience related to nuclear power plant electrical system failure events, held fact-finding discussions with representatives of several European utilities, directly involved members on the working group who are active in the IEEE, IEC, and KTA standards setting bodies, and reviewed current good safety practices originating from regulatory bodies and WANO.

The group observed that practices implemented in one country to address their specific operating experience were not necessarily being communicated or adopted in counterpart organisations in other countries, or to international design standards bodies such as IEEE or IEC. The process of changing accepted electrical design standards is recognised as being a 3 – 5 year long process from the time of creating a working group to the time the standard is adopted and published for use. It must also be noted that creation of a new standard does not necessarily imply its adoption or use in upgrading nuclear safety related equipment unless the national regulator makes the new standard obligatory.

The DIDELSYS Task Group was not chartered to carry out new electrical systems analyses or define specific numerical values for qualifying safety related electrical equipment. This is the proper responsibility of design and operating organisations. The task group did make substantive observations where specific practices had "gaps" and where design standards need to be upgraded. These are summarised in the following subsections.

4.2.1 Recommendations related to preventing electrical grid and plant generated electrical faults

The task group recognises that WANO SOER 99-1 and their 2004 Addendum offers a number of practical approaches to reduce electrical grid challenges and these should be addressed by nuclear power plant operating organisation. These include, but are not limited to:

- Establishment of Binding Agreements between nuclear power plant operators and transmission system operators for communication and coordination of planned activities such as major upgrades.
- Jointly planning and coordinating electrical circuit test and maintenance activities,
- Requiring transmission system operators to provide nuclear power plant operators with early warning of any on-going electrical grid problems that may become more severe. Examples would include degradation in voltage or frequency, sudden loss of major production units, or problems that might require de-energising a critical circuit or substation.
- Requiring nuclear power plant operators to provide transmission system operators with early warning of any operational limitations that might impact nuclear power plant output. Examples would include: technical specification limitations that might require a power reduction or controlled shutdown.
- Assuring that transmission system operator procedures recognise that nuclear power plants are priority load centers that must be avoided when load shedding is necessary and which need priority during restoration activities given blackout.

While the WANO SOER 99-1 and 2004 Addendum recommendations are recognised as being very important, it was recognised that WANO is a voluntary organisation, and that not every OECD member country was in conformance with these recommendations.

4.2.2 Recommendations related to robustness of nuclear power plant electric power systems

The DIDELSYS Task Group review found that many critical nuclear power plant safety systems are directly connected to the preferred power source (offsite power transmitted to plant safety systems via a transformer connection). A large rapid surge can propagate to these systems in some cases faster than alarms or active protective devices can respond. This presents the possibility for a common cause failure such as has been observed in the 2006 Forsmark event. Nominally a value of 120% voltage is assumed as an upper limit and used as the basis for qualifying many safety related electrical systems. The task group found this 120% value commonly used in IEEE, IEC, and German KTA standards. As examples: IEEE Std. 944 (1986) in Section 5.7.1 (4) only requires qualification testing of UPS units to 120% rated voltage. Additionally IEEE Std. 741 (1997) in Annex A states:

> "In an overvoltage condition, an alarm is generally adequate, without automatic tripping, because such a condition would be expected to only cause gradual component loss of component life."

Other standards contain similar limitations not based upon an assessment of actual hazard levels. Recognising this, the task group performed a review of selected IEEE, IEC, and KTA standards utilised in the design of nuclear power plant electrical systems. This review is documented in tables with specific suggested action items in Appendix B to this report.

The DIDELSYS task group thus recommends that nuclear power plants need to:

- Conduct a Hazard Review to determine the plant-specific range of possible voltage surge transients (considering: voltage and frequency content, rate of change, and duration) including: anticipated lightning surges, symmetric and asymmetric faults, switching faults, generator excitation system malfunctions and develop a design specification to be used as a basis to qualify existing or replacement equipment. Such a Hazard Review should consider the impact of such faults in conjunction with a single failed or delayed protective device operation. This is because operating experience indicates that recent events have been directly caused by initiating events not properly considered in plant electrical system design bases which were compounded by reliability issues associated with infrequently tested protection devices.
- Conduct a review of plant safety systems to confirm their capability to withstand the worst case power frequency overvoltage transients (including events such as: asymmetric or single phase faults, failure of the generator voltage regulator and excitation system with its maximum output). This is because operating experience has demonstrated that more serious current/voltage transients have occurred than were used as the design basis.
- Review the potential voltage degradations, their rate of change, and duration, and evaluate its impact on voltage sensitive devices such as local power supplies, MOVs, SOVs, contactors, etc.
- Review solid state device-based equipment such as: UPS, local power supplies, for their response (e.g. risk of tripping) to design basis voltage transients for an increasing and decreasing voltage in response to anticipated transients.
- Review the possible impact of voltage surge transients propagating through UPS, rectifiers, and other power supplies, causing detrimental effects on safety system loads.
- Consider the need for additional protection or equipment upgrade if the protective system response is not fast enough.

In making these recommendations to carry out further technical investigations it is recognised that the analytical tools such as Failure Modes and Effects Analyses are hindered by the lack of qualified

electrical system simulation models for evaluating issues such as voltage/current surges potential and the impacts on local components to voltage/current surges. It would be the equivalent of attempting to understand the magnitude of LOCA blowdown loads or fuel rod heatup during a LOCA without qualified system simulation codes. Clearly there is a need to select and qualify suitable electric power system simulation codes and benchmark these models against actual plant events.

4.2.3 Recommendations related to improving training, procedures, and information capabilities

The DIDELSYS Task Group recognised that the reason events such as the 2006 Forsmark event did not become more serious was because operators were well trained and followed procedures as best they could (given complicated nature of the event presented to them - and which was compounded by the unavailability of substantial portions of safety related displays). The DIDELSYS task group thus recommends that nuclear power plants:

- Review the existing reliability and diversity of power supplies needed to support Operator Information Systems important to safety.
- Given that the investigative processes recommended in Section 4.2.2 may require some time to fully implement, consider recovery procedures for events involving more than one safety related electrical supply until any corrective actions are completed.
- Review and confirm that WANO SOER 99-1 and 2004 Addendum recommendations related to electrical system recovery at the nuclear power plant have been carried out.

4.2.4 Recommendations related to coping capability of nuclear power plants

The DIDELSYS Task Group recognised the need to assure that while upgrades and improvements are being made to prevent electric power system common cause failures that events could occur that could fail one or more redundant trains of safety related equipment. The DIDELSYS task group thus recommends that nuclear power plants:

- Review RPS and ESFAS logic circuits for undesirable failure modes from loss of power, air, hydraulic pressure etc., (such as automatic depressurisation in BWRs, or actuation of automatic switchover to sump recirculation in PWRs) given loss of power to safety related electrical divisions or more than one train/channel of control and protection systems.
- Develop procedures and/or design modifications to address concerns arising from such undesirable failure modes.

4.2.5 Recommendations related to electrical system recovery

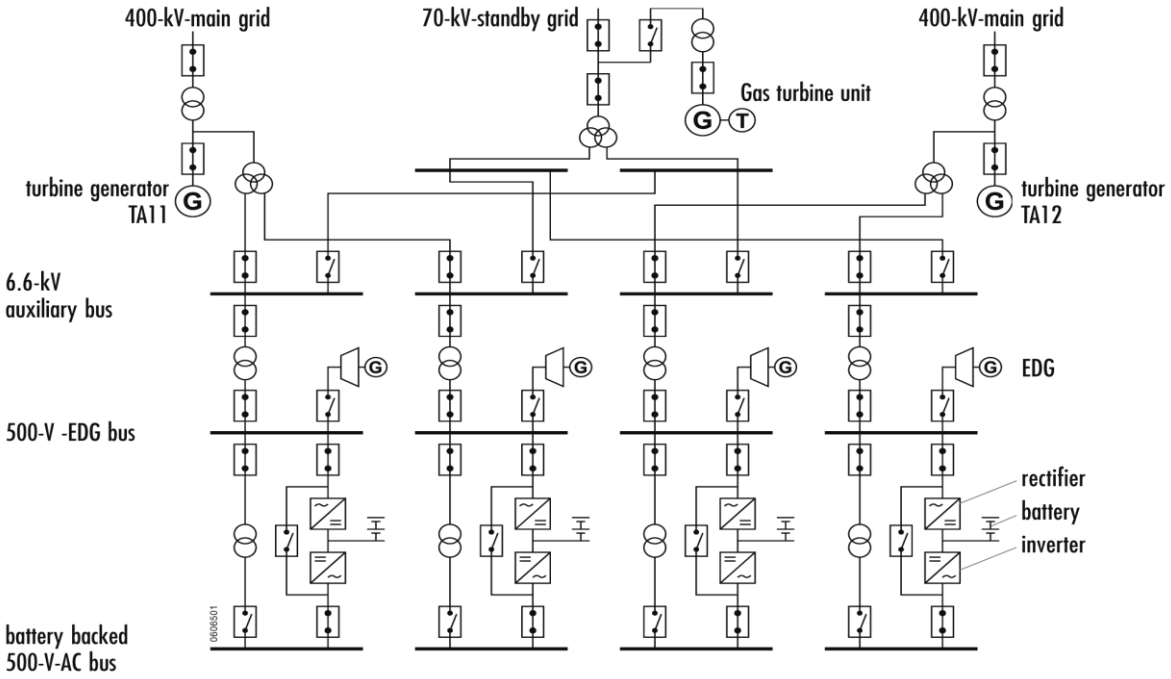
- For BWRs and PWRs that are designed with only electric power driven decay heat removal systems: evaluate a diverse means for promptly supplying power to core cooling systems (e.g., diesel driven pump, or fast starting gas turbine, etc.).
- Confirm existence of, or immediately develop a protocol for requiring offsite power to the nuclear station as a high priority and that transmission system operator procedures recognise that nuclear power plants are priority load centres which need priority during restoration activities given blackout.
- Review plans for grid recovery from brown and blackout events to assure adequate priority is given to NPPs and other essential high priority facilities.

Appendix A

DETAILED DESCRIPTION OF THE JULY 2006 FORSMARK-1 EVENT

The event at Forsmark Unit 1 involved a 1000 MWe BWR plant of ASEA Atom design and with twin turbines, commissioned in1980. Its principal safety design is 4 trains redundancy of 50% capacity Emergency Core Cooling Systems (ECCS), which in most transient situations corresponds to 4 times 100% capacity. The unit at the time of the July 25th 2006 event was operating in normal full power operation with its twin, Unit 2, connected to the same switch yard, down for maintenance. The third unit at the power station operates through a separate switch yard.

Figure A-1: Scheme of the power supply of Forsmark 1



The 25 July 2006 event was initiated by a short circuit in the 400 kV switchyard outside the plant caused by a maintenance error in the switch yard. Following the short circuit an electrical transient was fed back through the main transformers and the four divisions of the EPS (divisions A, B, C and D). Each of the four divisions of the EPS contains an uninterruptable power supply (UPS) system. The transient resulted in a failure of the UPS systems in the divisions A and B, by pure chance the UPS systems of the divisions C and D were not affected due to minor random variations in protective settings. The UPS system is intended to supply the low voltage AC systems without any interruptions. During normal operation, the batteries in each UPS system are charged from the normal AC system via rectifiers. In the event of loss of power supply, the batteries supply the safety

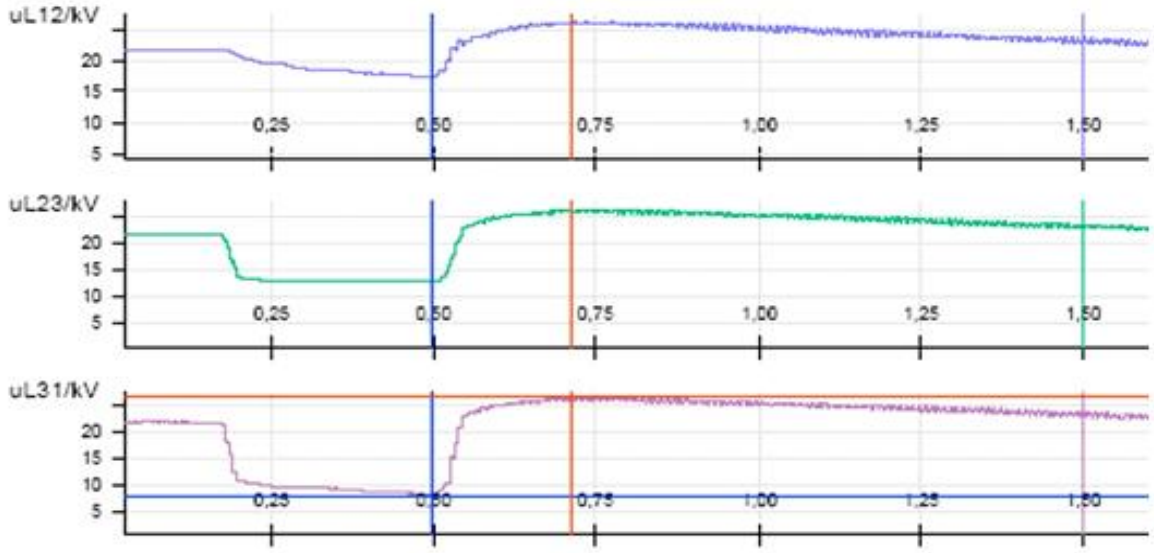
equipment powered from the system with low voltage AC via inverters. Both the rectifiers and the inverters incorporate various internal component protection features.

To the normal plant control systems the event initially appeared as a 50% load rejection. The reactor power was reduced by partial scram and the plant attempted house load operation, but only for a short period. The protection for under-frequency on the 1E busbars operated slower than the designed response time and allowed the frequency to drop below the acceptable range, during turbine coast-down, to a level that prevented fast transfer of plant safety related loads to the alternative (70kV) offsite supply. The 1E busbars were disconnected and diesel generator start was initiated on low voltage. The generator breakers opened when power no longer could be fed from the coasting-down generators. Restoration of auxiliary power was done through connection to the 70kV grid which includes a 2 second period of powerless busbars.

At the switch yard shorting, the generator busbar voltage dropped initially and was followed by an overshoot after tripping of the unit breakers. The over-voltage transient (See Fig. A-2) was to a large extent driven by the generator excitation controller trying to compensate the previous voltage drop. The transient was transmitted back into the station. The protective settings on the uninterruptible power supply (UPS) units, supplying battery backed-up power to AC 220V and underlying busbars were not properly co-ordinated with the battery chargers for protecting against a voltage surge transient.[31] Two (A and B) of the four redundant UPS-units tripped and left the underlying AC loads without power. The diesel generators started, but one function necessary for proper connection of diesel power to the busbar was dependent on control power from the UPS unit. Thus, train A and B diesel generators ran but did not connect and left the safety systems objects in these trains without power. After some moments, the situation was (roughly) that the 70kV was connected to the plant's non-safety busses, train C and D safety busses operated as intended on their diesel generators but train A and B were without power. The battery-backed DC busbars were powered as intended. The plant was at this stage left with two out of the four trains inoperable for, e.g., control rod electric insertion (hydraulic insertion had occurred at scram), auxiliary feed water injection, component cooling and main control room information systems.

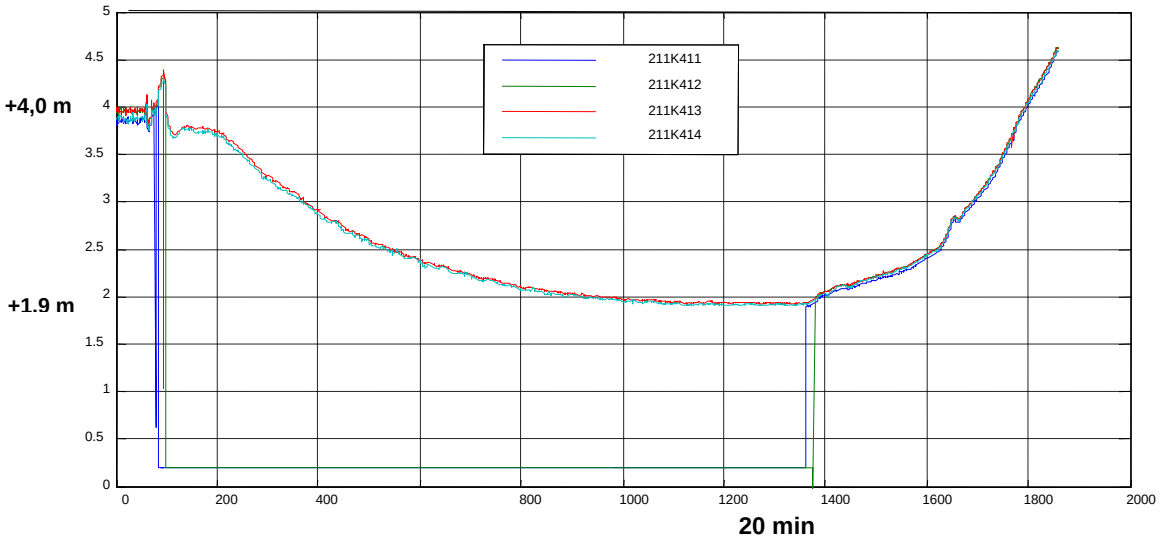
31. The protective settings on the UPS units were not properly co-ordinated with the voltage levels that would trip the incoming supply to the battery chargers. It was set to operate at voltage levels below where the battery chargers would trip. Had the supply from the battery chargers tripped first, the event would not have been as severe. Confirming the coordination of UPS vs Battery Charger protective settings was an insight developed from the Electricité d'France (EdF) and German Reactor Operators (VGB) review of the Forsmark event.

Figure A-2: Phase to phase generator busbar voltage recordings during the Forsmark event



The plant's Engineered Safety Features Actuation logic operates on 2 out of 4 coincidence logic. As transmitters were left powerless in train A and B, several signals in these trains failed to zero-output values and the Engineered Safety Features logic conditions were initiated, leading to trip of the protection channels. As the design of the protection system not in all cases correctly distinguished a "fail-safe" situation, this tripping of protection channels lead to the partial actuation of the "Forced Relief System" valves which resulted in a Blowdown of steam from the reactor. These valves functioned as designed but it was not optimal in this scenario. The total steam relief was in excess of the needs for decay heat removal and the system pressure gradually decreased. The system water inventory loss was at high pressure not fully compensated by the auxiliary feed water pumps in trains C and D and the water level was decreasing as is shown in Fig. A-3. At lower pressure, the high capacity ECCS system train C and D restored the level. The reactor water level turned around at 1.9 meter.

Figure A-3: Reactor pressure vessel water response



The operators quickly realised that the situation was very unusual. The information available to them in the main control room was substantially reduced due to the power disturbances. They handled the event very professionally in accordance with the emergency procedures. 22 minutes into the event they detected that the non-safety busbars were powered. They closed the breakers to the DG backed busbars in train A and B and thus restored power to the remaining safety functions. The pressure in the reactor vessel had blown down to a level allowing the low pressure injection system to inject. When power to A and B was reconnected and all water injection capacity was available again, the vessel inventory was quickly restored.

Detailed time-sequence of events

The following text gives a brief overview of the event:

Time: 13:20:20 A disconnector in the 400 kV switchyard opens, creating an arc and a two phase short circuit.

+ 0 sec: Both generator circuit breakers in Forsmark 1 trip on under-voltage, i.e. disconnecting the station from the 400 kV grid. Changeover to island operation.

+ 2 sec: Rectifiers in the UPS systems (divisions A and B) trip on a control fault, and the inverters in the same systems (divisions A and B) trip on over-voltage.

+ 5 sec: One turbine tripped (emergency stop) due to low governing oil pressure.

+ 18 sec: Changeover to direct supply of the battery backed AC network (division A) due to low voltage.

+ 24 sec: The normal supply circuit breakers to the 500 V diesel backed distribution systems open in division A and division C due to low frequency on the 500 V diesel generator buses.

+ 24 sec: Diesel start and connection in Division C. The connection of division A fails.

+ 33 sec: Emergency stop of the second turbine due to high pressure in the turbine condenser.

+ 35 sec: Changeover to direct supply of the division A network due to low voltage.

+ 36 sec: One generator circuit breaker trips on low power (less than 5 MW).

+ 36 sec: Changeover to 70 kV supply to divisions A and C due to low voltage in the 6 kV switchyard.

+ 37 sec: The normal supply circuit breakers to the 500 V diesel backed distribution systems open in division B and division D due to low frequency, i.e. less than 47 Hz for more than three seconds on the 500 V diesel generator buses. Diesel start and connection to division D successful. Connection of diesel generator to division B fails.

+ 43 sec: The second generator circuit breaker trips on low power.

+ 43 sec: Changeover to 70 kV supply via divisions B and D due to under-voltage in the 6 kV system.

+ 22 min: Manual restoration of power to the diesel backed 500 V division A and division B buses.

Root causes of the event

The event analysis indicated the following factors that contributed to the seriousness of the Forsmark incident:

- The initial event was due to the fact that work in the switchyard was not carried out with adequate controls.
- The short circuit in the switchyard resulted in a more severe disturbance because of the delay for the secondary protection device to actuate. The impact of this delay in clearing the fault on the main generators was not considered in the design basis.

- The under-frequency relay that was replaced did not undergo a verification following the installation for phase sequence that was important for the precise operation of the new model.
- The UPS replacement did not consider worst case voltage transients engineering analysis for choosing the set points for over-voltage and under-voltage.

Each of these issues is further discussed below.

The event was initiated by a faulty maintenance procedure manoeuvre during regular switch yard maintenance. The sequence of events that then followed has its cause largely in insufficient quality in plant modernisation, maintenance and testing. Replacement Exchange of under-frequency protection system that had taken place in 2005 did not notice that the new device was, in contrast to the one being replaced, dependent on correct phase order for proper function. At installation, the phase order was not electrically verified but only checked as marked up, which turned out to be incorrect. The delayed function of the protection disabled the possibility to a fast transfer to the 70kV grid powering the safety busbars.

During the initial years of plant operation, uninterruptible or vital instrument power UPS was supplied by a motor-generator (MG) set. Such a system is tolerant to momentary voltage transients. When replacement to a UPS based on solid state technology took place in 1993 the risk of malfunction due to exposure to voltage transients was not properly taken into account. The maintenance fault also had disabled the first level of the busbar protection which enhanced the duration of the short circuit and the transient amplitude. Thus, the UPS protection was not designed to respond to a voltage surge of this magnitude and therefore voltage settings did not properly cope with the event and, instead of isolating the underlying busbars from the transient, it shuts the UPS down leaving the underlying systems unpowered. This fault exposed all redundant UPS operated safety systems to a common cause hazard, which in this case resulted in failure of two of the four trains.

One of the conditions for connection of the diesel generator to its busbar is verified correct motor speed. The tachometer was powered from the UPS fed AC system, thus giving dependence between the connection of diesel power and an AC power downstream to the bus. Such dependencies reduce the robustness of the safety related power in that it exposes the system to common cause failures. In addition, the event highlighted several other aspects with safety relevance which needs to be discussed and optimised. One is the interaction between failing power systems and degradation of information to operators in the main control room. Another is the determination of “fail-safe” state in situations with actuation of safety logics in complex sequences.

The alternate AC source from the switchyard was unavailable during the event because the power supply for the control system had failed.

References

The Forsmark incident 25 July 2006, Bakground Vol. 20, Analysgruppen, Feb. 2004

Appendix B

INTERNATIONAL ELECTRICAL STANDARDS GOVERNING ONSITE ELECTRICAL SYSTEMS IN NUCLEAR POWER PLANTS

One of the activities carried out by the DIDELSYS Working Group was an evaluation of overall industrial design standards governing the essential features of nuclear power plant electrical systems. Within the member countries represented on the working group it was observed that IEEE, KTA, and IEC standards and/or combinations of these standards are frequently used in designing the key features, level of redundancies, design capacity requirements of electrical systems within operating nuclear power plants. These standards document the cumulative wisdom and good practices from past designs found to be necessary for assuring safe reliable operation. Design standards are not static. They are evolving to reflect: the application of new materials and technologies that alter what were thought to be design constraints or limitations, the insights from recent operating experience showing a need for either increased design safety margins, or the reasonability to allow relaxing design margins.

In the review of the IEEE, KTA, and IEC standards the review focused on the reasonability of existing design margins and specific requirements for coping with degraded voltage scenarios. In areas where the current standards lack specificity or incorporation of design margins, we have identified these areas for possible revisiting when the standards are in their next periodic revision cycle. An observation from this review is that a designer starting off to specify the design of electric power system components would only be considering a dynamic AC voltages in the range of Umin = 80% nominal to Umax = 120-125% nominal. The standards looked at, do not consider the possibility of equipment needing to perform or function for voltages outside of these ranges. Voltages below Umin are assumed to be precluded by protective features. Voltages above Umax are assumed to be prevented either by: lightning surge arrestors, staged lower voltage surge arrestors, or by built in voltage limiting protection features on local equipment.

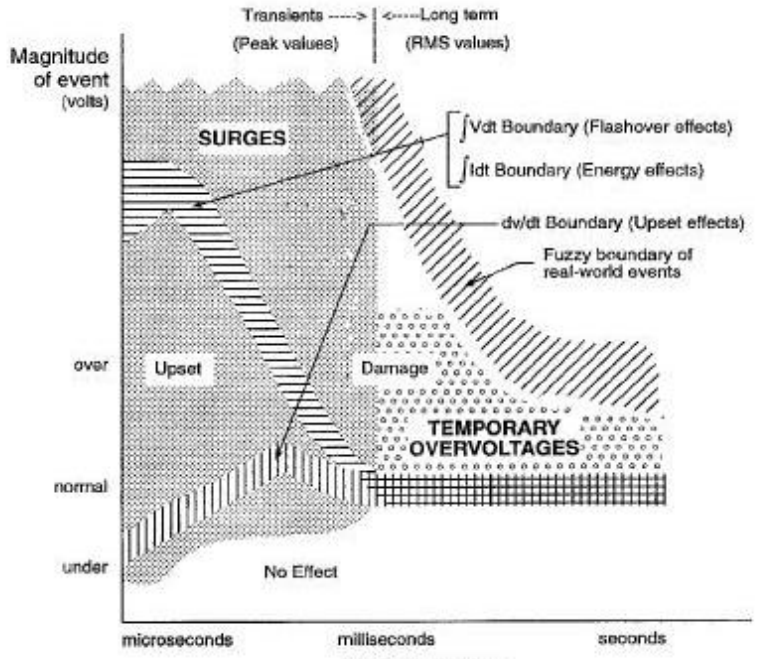
Each of the types of standards is discussed below.

B.1 IEEE standards for nuclear power plant electric power systems

Figures B-1 and B-2 are a hierarchy diagram showing the relationships between the very general top level design standards for the overall electric power system, general safety requirements for Class 1E systems, and the various technical issues such as: functional requirements, qualification, use of digital I&C components for control and protection features, design characteristics which address issues such as grounding and lightning protection, as well as design requirements for the various subsystems which make up the electric power system. These figures address only design related considerations and (for sake of brevity) omit testing and maintenance requirements which would make the diagrams unduly complicated. All of the major subsystems such as: batteries, switchgear, diesels, etc. - each have unique test and maintenance requirements which are also covered in industrial standards – and are not shown in these diagrams. Certain specific standards in the diagrams have been shaded to indicate the standard has design or safety margins requirements that impact the degraded voltage issue and may need to be upgraded in the next revision cycle to address the technical concerns of degraded voltage.

The main standard governing electric power system design (shown on the top of Figure B-2) is IEEE Std. 308. This standard references a number of other IEEE standards which provide further guidance and requirements on the design of subsystems and other specific requirements. IEEE Std. 308 invokes all of the general safety system criteria (e.g.: redundancy, testability, reliability, etc.) defined in IEEE Std. 603. The next tier of the diagram in Figure B-2 consists of specific major design issues and subsystem design requirements. The specific areas of: Digital I&C (Software) and Equipment Qualification involve many sub-tier standards and are respectively shown via links on Figure B-3. Table B-1 summarises how the various IEEE standards address safety issues associated with degraded voltage and possible changes which should be considered. The system of electrical design standards covered in the IEEE standards for nuclear power plant electrical systems assume the proper application of station grounding per: IEEE Std. 665, IEEE Std. 1050, and staged voltage surge protection as described in: IEEE Std. C62.2, IEEE Std. C62.23, IEEE Std. C62.41.2, and IEEE Std. C62.45. IEEE Std. C62.41.2 provides a graphical representation of the spectrum of voltage surges which need to be considered in providing protection. This figure is repeated below as Figure B-1. One of the acceptable methods of confirming component withstand capability is the performance of voltage surge tests according to IEC standard IEC 61000-4-5.

Figure B-1: Simplified relationships among voltage, duration, rate of change



NOTES

1—The graph shows the relative position of effects and the order of magnitude of the amplitude and duration. Do not attempt to read numerical values from this graph.

2—The scope of the guide is shown by the two dot-pattern areas. The fine pattern relates to surges, the prime scope of this guide. The coarse pattern relates to temporary overvoltages, the secondary scope of this guide. For surges, the upper limit for the duration is one half-cycle of the applicable power frequency. Swells—overvoltage events longer in duration than a surge but lasting only a few seconds—are considered to be a subset of temporary overvoltages.

3—The values or positions of the boundaries between "no effect" and "upset" and between "upset" and "damage" vary with the withstand characteristics of the equipment exposed to the surges.

4—The boundary between "upset" and "damage" in the microsecond range is shown as the integral of Vdt to reflect the upturn in the volt-time characteristic of sparkover. Equipment responses that do not involve a sparkover are more likely to be influenced by the simple magnitude of voltage V.

5—This figure shows only one measure of surge severity emphasizing voltage and time relationships. Other possible measures include current peak and duration, rise time, and energy transfer.

A key observation from this review of the IEEE standards is the use of a common 120% nominal upper voltage limitation which is found in the maximum voltage withstand qualification assumptions for relays, switchgear, and most importantly: for the assumed AC supplies to UPS units defined by IEEE Std. 944. Designers would view that the need to provide protection for surges above and beyond 120% was precluded by other considerations and thus beyond anything required by the standards and thus not necessary. The allowed "failure mode" for surges in this beyond design basis range could be anything from: component failure, operation of protective fusing, or operation of protective breakers.

Figure B-2: Hierarchy of IEEE Standards related to electric power system design

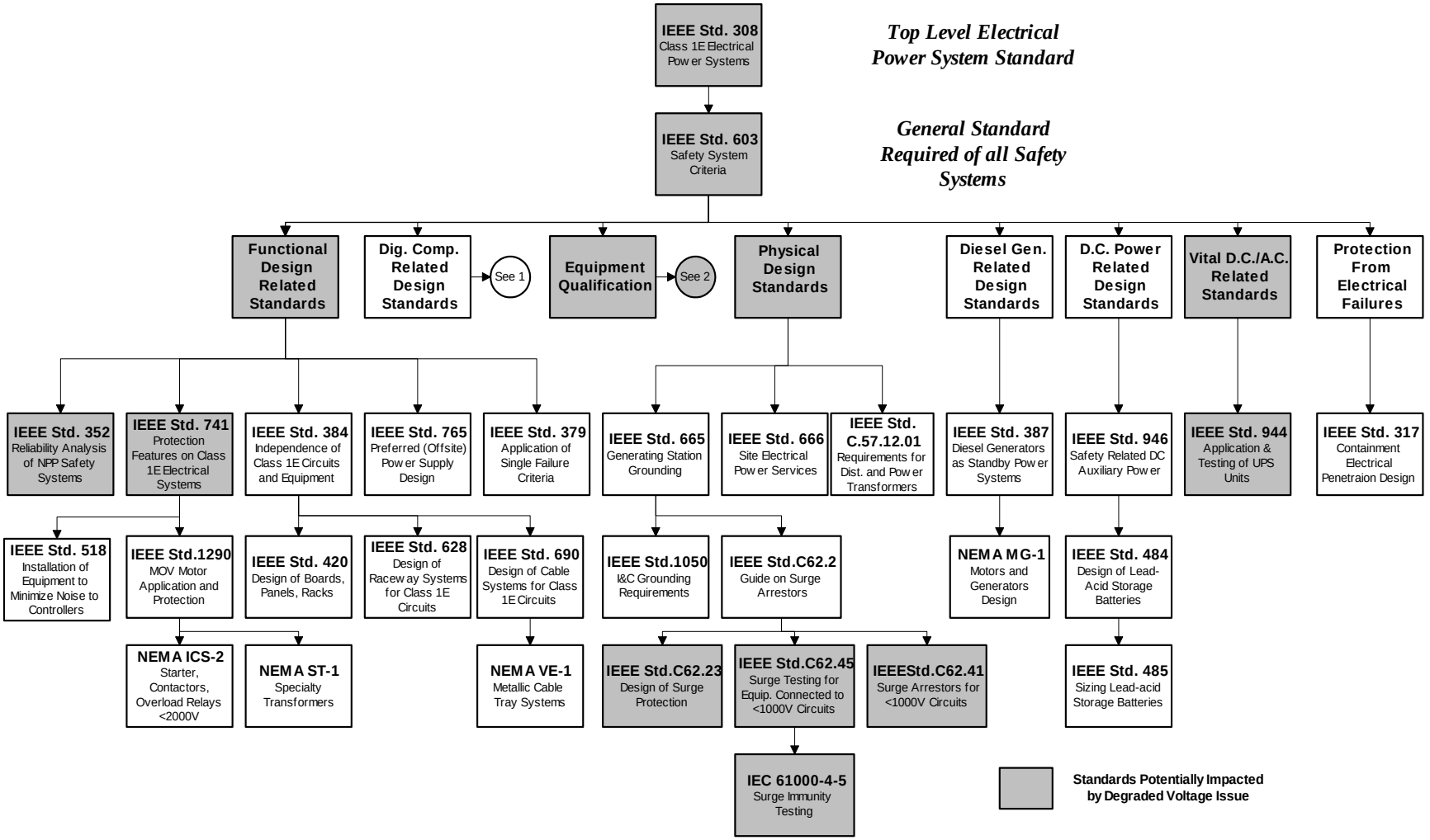


Figure B-3: Hierarchy of IEEE Standards related to electric power system design - continued

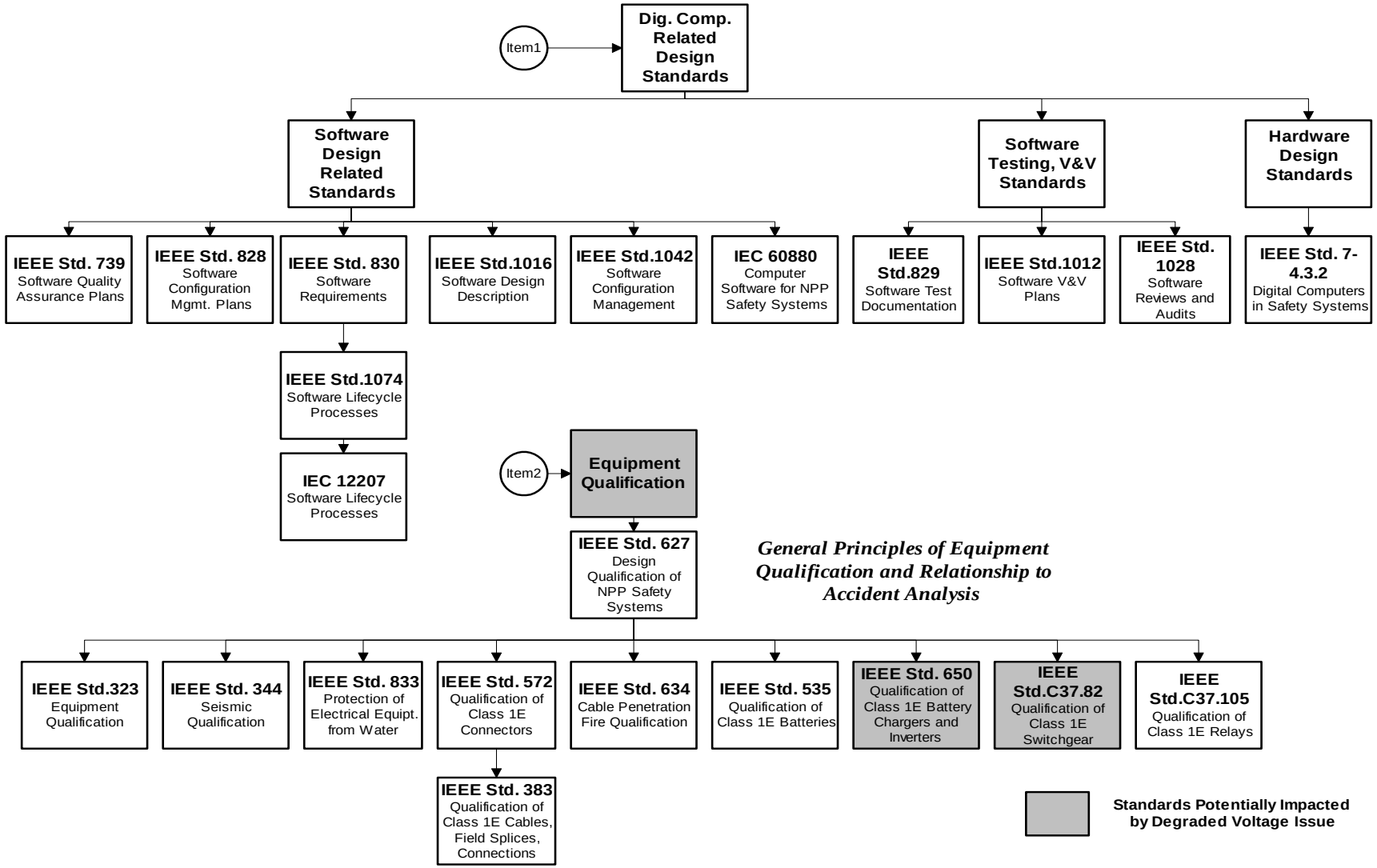


Table B-1: Observations from IEEE standards reviews

IEEE standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
IEEE Std. 308	2001	4.4 Design bases	Notes that Design Bases as minimum should consider *under-voltage,* but does not mention *overvoltage.*	Overvoltage should also be considered.
		8.1. Design documentation records	Requires documenting steady-state load and profile studies that show voltages throughout system (AC, DC, Vital AC) for various modes of operation, including design bases events, and degraded voltage conditions.	Faults during load rejections and other overvoltage scenarios need consideration.
IEEE Std. 603	1998	4. Safety system design bases	Requires documenting range of voltage, frequency…during normal and abnormal operation	Need to specifically address under-voltage and overvoltage scenarios should be considered.
		Annex B (informative)	References IEC 61000-4-5, -4-11 voltage surge testing to address dips and interruptions, but not voltage surges.	Need to specifically address overvoltage scenarios should be considered.
IEEE Std. 352	1987	4.1 Failure modes and effects analysis	FMEA analyses approach is focused on binary type scenarios (e.g. energised vs. de-energised) which do not require extensive analysis of degraded voltage within plant buses. To consider a wider range of possible failure modes would require simulation of voltage/current flows during failure scenarios.	Postulated fault scenarios in FMEAs need further evaluation considering voltage/current flows during failure scenarios.
IEEE Std. 741	1997 (R2002)	5.1.2 Bus voltage monitoring schemes	The standard was upgraded to address degraded voltages (which are clearly defied to be under-voltage and overvoltage) but primarily addresses remedies for under-voltage and loss of voltage alarming and protective actions.	Need to specifically address overvoltage scenarios should be considered.
		5.1.6 Surge protection	References IEEE Std.s C62.41 and C62.45 for surge definition and required protection.	None.

IEEE standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
IEEE Std. 741	1997 (R2002)	5.2 DC Power System	References IEEE Std. 446 for under-voltage and overvoltage alarms and trips	None.
		5.3 Instrumentation and Control Power	Requires under-voltage and overvoltage alarms and trips	None.
		Annex A (informative)	Describes setting of under-voltage and overvoltage alarms and trips, but predominance of discussion is focused on under-voltage. Overvoltage in section A-6 states that alarming (only) is all that is necessary because only implication is on gradual component degradation.	Include discussion of sources, implications of overvoltage on Class 1E Vital AC Circuits used for I&C power supply in Section A.6
IEEE Std. 944	1986	5.7.1 (4) AC Source	Presumes as design bases: *that overvoltage is limited to <120% nominal voltage and not lasting more than 30 seconds*.	Require local surge protection be provided on incoming AC power bus. (Otherwise, this section implies UPS failures would be expected at >120%)
IEEEStd.C62.23	1995	6.2.3 Internally Generated Surges	Describes possible surges requiring protection from capacitance switching, fault interruption, insulation breakdown, motor starting/stopping transients – *but does not mention main generator voltage regulator malfunctions* as events causing surges of the same magnitude that will propagate throughout in-plant lower voltage buses.	Majority of Section 6.2.3 focuses on justifications *not to provide protection* to large motors, transformers, etc.
		6.3.2.3 (Controls and Communication) Protection	Indicates surge suppressors may be used, but may not be practical at all locations of lower voltage control systems. Recommends against use of SCR "crowbar circuit" protection schemes in "critical facilities" as these would degrade reliability.	Section needs a clear recommendation of what protection would be best, possibly a local surge arrestor with low operating voltage?

IEEE standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
IEEE StdC62.41	2002	4. Summary of the Surge Environment	The standard currently focuses on surges caused by only 3 sources: lightning, switching surges, interactions between systems. This standard is used to specify the sources of the wave fronts used for surge testing which is then broken down into: 1) a pulse with a 5.0μs±0.15 μs rise and a 100kHz ringing frequency, and 2) a pulse with a 1.2±0.36 μs rise and duration of 50μs±10 μs	Consider adding a category of surge transients of longer duration (many milliseconds) and with voltage peaks reflective of main generator caused overvoltage transients that will be fed back to in-plant buses during upset conditions.
IEEE StdC62.41	2002	9.2 Standard Waveforms	The definitions of test waveforms for surge immunity tests come from IEEE StdC62.41.	Change this accordingly to changes in IEEE StdC62.41
IEC 6100-4-5 (Referenced in a number of IEEE Standards as an acceptable surge immunity test).	2001	3.1 Switching Transients	Uses pulse with a 1.2±0.36 μs rise and duration of 50μs±10 μs to simulate open circuit transients	Consider adding a category of surge transients of longer duration (many milliseconds) and with voltage peaks reflective of main generator caused overvoltage transients that will be fed back to in-plant buses during upset conditions.
IEEE Std. 650	1990	5.2.2.2.7 Surge Suppressors	Qualification tests defined in this standard focus primarily on thermal and other environmental factors. This includes aging simulation on Selenium surge suppressors.	Consider definition of voltage surge as design basis event requiring protection and thus qualification.

IEEE standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
IEEEStdC37.82	1987 (1993)	4.1.5	Notes that switching transients could result in voltage surges up to 200% but that lightning surges are not a required consideration for switchgear qualification. Key design bases events noted for switchgear are LOCAs and Seismic events only.	None.

B.2 KTA standards for nuclear power plant electric power systems

The German Nuclear Safety Standards Commission (KTA) maintains a series of nuclear safety standards used in Germany, and portions of these, deal with the design of electrical power systems. Figure B-4 shows a diagram for applications of the KTA standards related to the electrical power system design of NPPs and how they are interrelated. The main KTA standard governing the design of electric power systems is KTA 3701 – General Requirements for the Electric Power Supply in Nuclear Power Plants. As shown in Figure B-4, this standard references other KTA standards. In some cases, KTA standards reference industrial standards (e.g. DIN, or IEC standards) for aspects related to specific portions of the electric power system, such as design of: diesel generators, batteries, DC-AC inverter supplies, etc. Although not explicitly shown on this diagram, there is a Lightning Protection standard: KTA 2206 which is presumed as the underlying basis for grounding and lightning surge protection.

In addition to the nuclear safety standards, industrial standards (e.g. the German Occupationals Accident Prevention Regulations, DIN standards, and VDE Regulations) are applied to nuclear facilities. It is important to keep in mind that a presumption of the nuclear safety standards is the fulfilment of the conventional requirements and standards unless other requirements are specified in the nuclear safety standards and regulations.

Similar to the review of the IEEE standards, a review was also conducted of the KTA standards to evaluate how the issues of under-voltage/overvoltage were currently considered in the existing standards. This review was conducted using only the current English translations of the German KTA standards, and thus any revisions currently underway (and not yet translated to English) were beyond the scope of this review.

The KTA standards presume the proper operation of station grounding and staged lightning surge arrestors for protection against lightning-related voltage surges. Additionally these standards require consideration of possible dynamic voltage swings from a wide spectrum of possible power plant operation and specifically include the need to consider the unit separation from the grid (main and auxiliary grid) and runback to house loads powered only by the main generator. This mode is also known as the "islanding mode of operation". (See: KTA 3705 Section 3.4 (6) b). *What is not considered is the impact of a single failure while in, or transitioning to, this "islanding mode of operation"*.

Similar to the IEEE standards there is a presumption that maximum voltage withstand capability for plant equipment should be in the range of 110% -122% nominal. Some specific examples of how this range appears, includes:

- Permissible transient voltages to motor starters powered by batteries, diesels, and DC/AC converters: The ranges are: Umin = 80% nominal to Umax = 122% nominal (KTA 3504)
- Maximum assumed or allowed diesel generator voltage during transient operation: Umax = 120% nominal (KTA 3702)
- Maximum assumed dynamic AC supply voltages to Battery Charger rectifier units: Umin = 80% nominal to Umax = 115% nominal. When upper voltage limit Umax is reached, the charger unit is assumed to be shut off until less than Umax (KTA 3703)
- Maximum assumed ranges of motor-generator set or inverter operation are: Umin = 85% nominal to Umax = 120% nominal (KTA 3704)

- The requirements for design of transformers, switchgear, and distribution systems to consider the following range of overvoltages for short circuit currents: Umax = 105-110% nominal. (KTA 3705)

Another similarity to the IEEE standards is the method of confirming component withstand capability via the performance of voltage surge tests according to IEC standard IEC 61000-4-5.

Figure B-4: Application of KTA standards related to electric power system design

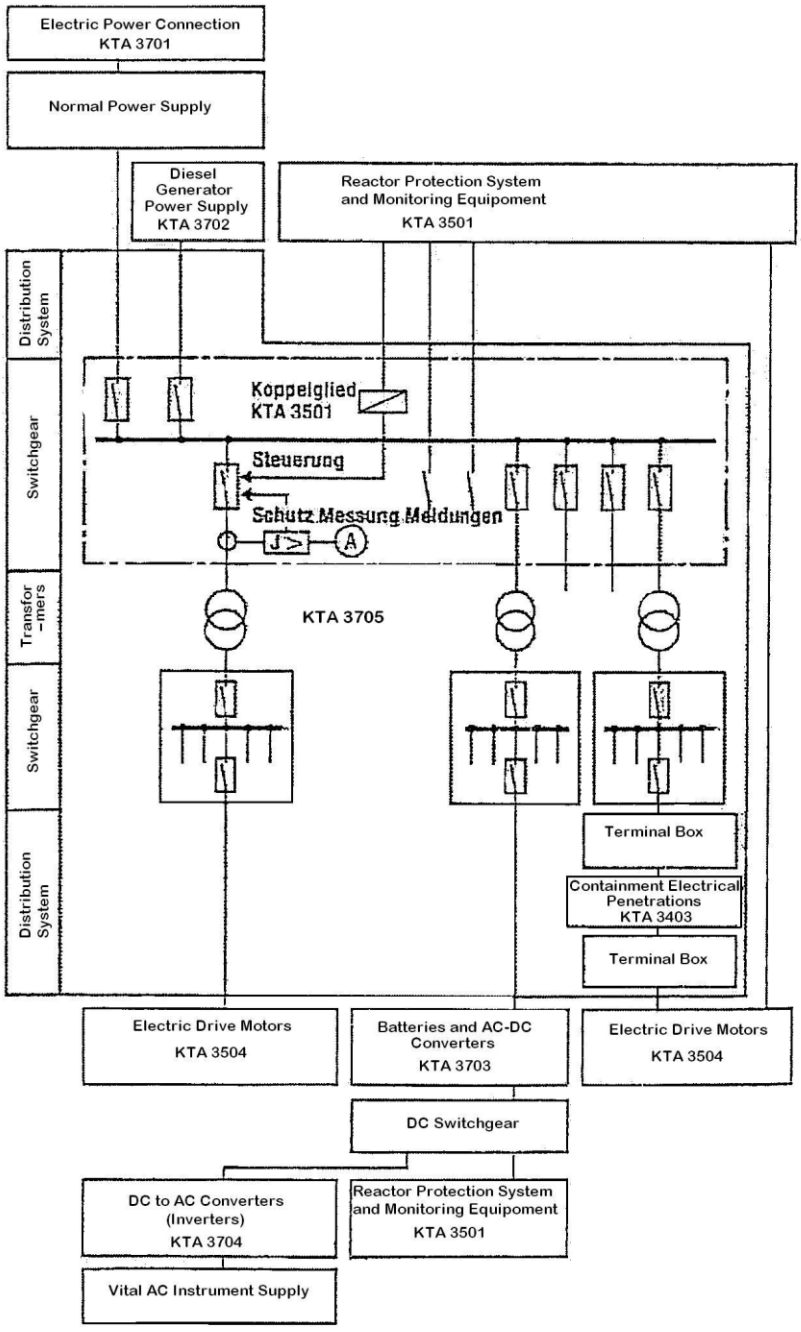


Table B-2: Observations from KTA standards reviews

KTA standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
KTA 3701 (Electric Power Connection)	6/1999	4.2 (4) Basic Requirements 5.2 (1) Basic Requirements	Notes a requirement that equipment must be designed for the allowed *tolerances* in voltage, current, or frequency both in static and dynamic ranges – but does not identify what these ranges are. Design values are presumed to be plant and design specific	Consider clarifying the presumed ranges of tolerances in voltage, current, frequency to match likely component operating limits.
		4.11. Initiation and Termination of Emergency Power Operation	Refers to standards KTA 3702 and KTA 3501 for initiation and termination criteria. The termination of emergency power operation depends on consideration of a specific situation. The standards deliberately give no recommended considerations and leave this up to specific plant operating organisations.	A review of both KTA 3702 and KTA 3501 does not find clear criteria for termination of emergency power operation. KTA 3701 should probably be amended to provide such values.
		C 1.2 (2) Connections between Station Service Facility or Offsite Power Supply and Emergency Power Supply	Requires that the design be such that scenarios involving overvoltage, or short-circuit to ground, etc. should not result in any common cause failure in the emergency power system. German KTA practice is to not provide specific implementation details. These details are typically provided in DIN, IEC, and VDE regulations such as: VDE 0100, 0101, 0432, 0446, and 0141.	Consider adding clearer identification of acceptable norms and standards that provide implementation details for overvoltage protection other than from lightning.

KTA standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
KTA 3702 (Diesel Generator Power Supply)	6/2000	3.11.2 (3)Initiation and Termination of Emergency Power Operation	Requires initiation when the electric power system voltage is less than allowed in plant design but no lower than 80%.	Clarify actions if a momentary or sustained overvoltage condition is present.
		3.11.2 (4)Initiation and Termination of Emergency Power Operation	Requires initiation when the electric power system frequency is less than allowed in plant design but no lower than 47.2Hz.	None.
		Table 3.2 Dynamic Tolerances	Item 3.1 uses 120% voltage limit for diesel generator transient operations. The presumption is that this value takes into consideration voltage drops across transformers.	Confirm this 120% voltage limitation assumption is consistent with onsite loads such as: UPS and inverter units.
			Item 3.2 uses 85% voltage limit for lower diesel generator transient limits	None.
KTA 3501 (Reactor Protection System and Monitoring Equipment)	6/1985	4.2.1 a) Failure-Inducing Events within the Reactor Protection Systems	Contains a general requirement that the RPS design consider external faults such as those caused by open circuits, shorts to ground, *changes in voltage*….	None.
		4.7 (6) Separation of the Reactor Protection System from Other Systems	Reactor Protection Systems is required to be decoupled from *over-voltages*. The decoupling elements shall be designed for an AC or DC voltage of 220V. Plant specific voltage tolerances shall be considered. This is accomplished via Zener diode clamping circuits and fusing. Protection against voltages >120% is provided by the inverters. KTA 3703, table 4-1 provides for inverters being shut down for conditions >115%	None.

KTA standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
KTA 3501 (Reactor Protection System and Monitoring Equipment)	6/1985	5.5.4 (3) Individual Drive Controls	Requires that coupling elements such as interposing relays – shall function *within the limits of the input and output voltages*. The individual coupling elements are not designed to be fail-safe. The requirement is to ensure the operation of the coupling elements and that the coupling elements are adapted to the operating voltage of the reactor protection system and its actuators.	None.
KTA 3503 (Type Testing of Electrical Modules)	11/2005	5.4 Electromagnetic Compatibility	Refers to IEC standard IEC 61000-6-2 for scope of EMC Qualification of radio frequency type emissions, and IEC 61000-6-4 for prevention of radio frequency emissions, but contains no clear requirements for voltage surge test qualifications. There are no specific requirements for voltage surge immunity except for "informative Appendix B" reference to IEC 61000-4-5 voltage surge testing.	Consider the need for voltage surge immunity tests, beyond those required by DIN EN 61000-6-2 (IEC 61000-6-2).
		5.7.4 d) Constant Humid Heat (Qualification Test)	Requires varying the power supply voltages between U_{min} and U_{max} after every 6 hours of testing. It is not within the scope of type testing to confirm the suitability of electrical modules for a specific application. The purpose of the type testing is to confirm whether electrical modules comply with the specification requirements.	There is a need somewhere to clarify requirements for U_{min} and U_{max} to be used in qualification tests.

KTA standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
KTA 3503 (Type Testing of Electrical Modules)	11/2005	5.7.6 c) Cyclic Dry Heat (Long-term Qualification Test)	Requires varying the power supply voltages between U_{min} and U_{max} after every 24 hours of testing. It is not within the scope of type testing to confirm the suitability of electrical modules for a specific application. The purpose of the type testing is to confirm whether electrical modules comply with the specification requirements.	There is a need somewhere to clarify requirements for U_{min} and U_{max} to be used in qualification tests.
KTA 3504 (Electrical Drive Mechanisms)	11/2006	3.2.1 Failure Initiating Events in Electric Drive Mechanisms of the Safety System	Contains a general requirement that the electrical drive mechanism design consider external faults such as those caused by short circuits, shorts to ground, voltage or frequency changes, *mechanical failures…*	None.
		5.6 Design of the Drive Motor	Contains a general requirement to be capable of starting a motor at lowest possible voltage U_{min}.	None.
		5.6 b) Reduction of motor torque during starting transients.	Contains a design assumption that the lowest voltage at motor starting should be U_{min} = 80% nominal, and U_{min} = 90% nominal if the power source is a DC/AC converter unit designed per KTA 3704.	None.
KTA 3504 (Electrical Drive Mechanisms)	11/2006	5.7 (1), (2) Electric Power Supply	Contains a general requirement that a motor starter be connected such that voltage drops to motor terminals will never be below: U_{min} The requirement reference KTA 3702 Section 3.11.2 for starting with diesel power sources.	None.

KTA standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
KTA 3504 (Electrical Drive Mechanisms)	11/2006	6.3 Electro-technical Design	Contains general requirements for long term values for U_{min} and U_{max}	None.
		6.3 (3) Impermissible Switching overvoltage provisions.	Contains general requirements to provide "circuitry measures" to limit switching over-voltages caused by devices such as solenoids de-energising.	None.
		6.4 Electric Power Supply	Contains a general requirement for the motor starter to be capable of starting a motor at the lowest possible voltage U_{min}.	None.
		6.7 (3) ak) Technical Documentation	Contains a general requirement to describe the protective circuitry for the limitation of over-voltages.	None.
		Table 6-1 Example Permissible Voltage Changes	Contains example ranges of permissible voltages to motor starters powered by batteries, diesels, and DC/AC converters. The ranges are: U_{min} = 80% nominal to U_{max} = 122% nominal, thus implying no need to consider impacts of voltages outside of this range except to presume inability to operate.	
		7.3 Electric Power Supply	Contains a general requirement for the motor starter to be capable of starting a motor at the lowest possible voltage U_{min}.	None.
		10.3.1(2) a), b) Physical Tests	Contains a general requirement to determine minimum start-up torque at U_{min} and maximum torque at U_{max}	None.
KTA 3504 (Electrical Drive Mechanisms)	11/2006	Table 10-1 LOCA Qualification tests for open-loop actuators	These are general requirements for LOCA Qualification Tests. They note usage of U_{min} = 80% nominal to U_{max} = 110% nominal, and a final test of the "coil" of U_{max} = 200% nominal	None.
		Table 11-1 LOCA Qualification tests for solenoid operated valves	These are general requirements for LOCA Qualification Tests. The ranges are: U_{min} = 80% nominal to U_{max} = 122% nominal, and a final test of U_{max} = 200% nominal.	None.

KTA standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
KTA 3703 (Batteries and AC-DC Converters)	6/1999	4.3 Circuit Design of Battery Facilities	Contains a requirement that the circuit design shall contain provisions for *overvoltage protection* - consistent with requirements of KTA 3701 Section 4.2 (4) to ensure electrical conditions of power loads are fulfilled even under unfavourable ambient conditions and accident related loading.	None.
		4.4.2 Determination of Current Requirements	Contains a requirement for considering (during transients) that a battery is loaded by power loads of connected train and neighbouring train.	None.
		4.4.5 b) c) Limit Values	Contains general requirements that upper dynamic limit values shall be specified as a function of the *short-time overvoltage permissible…* and that motor starting transient not cause rectifier shut-off, but that rectifier circuits may be temporarily shut-off to prevent over-voltages.	None.
KTA 3703 (Batteries and AC-DC Converters)	6/1999	Table 4-1 Limit Values for the Design of Rectifier Units	Contains requirements to consider a range of dynamic AC supply voltages of: U_{min} = 80% nominal to U_{max} = *115% nominal*. When upper voltage limit U_{max} is reached, the charger unit is shut off until less than U_{max}. The presumption is that this value takes into consideration voltage drops across transformers.	None.
		4.7.3 (5), (6) Protection Equipment	Contains requirements for overvoltage protection on the DC side of a rectifier circuits to prevent single failures from propagating.	None.

KTA standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
KTA 3704 (DC-AC Converters)	6/1999	4.5.2 (2) a)Design of Rotating Converter (e.g. Motor-Generator Set)	The nominal apparent power of the generator, its reactance and voltage control shall be specified such that even in the case of dynamic load changes the output voltage remains within the allowable dynamic limit values in accordance with item No. 2.1 of Table 4-1	None.
		Table 4-1 (item 2.1) Limiting Values for Design of the Converter Unit	Contains general requirements for converter operation. The ranges are: U_{min} = 85% nominal to U_{max} = 120% nominal	None.
KTA 3705 (Switchgear, Transformers and Distribution Networks)	11/2006	3.1 (1) a), c)General Requirements	Contains general requirements that static and dynamic limit voltage and frequencies of power loads shall not be exceeded and that protective devices shall be provided to maintain limits.	None.
		Table 3-1 Diesel Emergency Supply	Notes limiting value for isolated plant unit running on diesels: U_{min} = 70% nominal to U_{max} = 110% nominal	None.
		Table 3-2 Converting or Inverting Emergency Power Supply	Notes limiting value for running on Converting or Inverting Emergency Power Supply: U_{min} = 80% nominal to U_{max} = 110% nominal	None.
		3.2 Protection and Selectivity	Contains general requirements for location of short-circuit protection	None.
		3.4 (4), (5), (6) b) Voltage Drop, Voltage Dip, Voltage Increase	Contains general requirement to determine the maximum and minimum voltages during static and dynamic operating modes.	*Consider a single failure in main generator voltage regulation.*
		3.4 (8) Overvoltage protection	Contains general requirements for overvoltage protection due to over-voltages from lightning surges and switching transients.	*Consider a single failure in main generator voltage regulation.*
		4.2.1 d) Transformer Design Criteria	Contains requirements to consider the following range of over-voltages for short circuit currents: U_{max} = 105-110% nominal	*Re-evaluate if this range sufficient given experience.*

KTA standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
KTA 2206 (Lightning Protection)	6/2000	4.3.6 (1) Voltage Surge Protection Devices	Contains a general requirement that if I&C equipment supply voltage limit could be exceeded, the I&C equipment shall be equipped with surge protection devices such as: spark gaps, Zener Diodes, varistors, or a combination of such components. It also notes the possible necessity of installing a system of graduated voltage surge protection devices.	None.
		5.3 Testing of Permissible Voltages	References IEC 61000-4-5 as an acceptable means for conducting surge tests.	Evaluate if the ranges of surges produced in this standard test is sufficient given experience.

B.3 IEC standards for nuclear power plant electric power systems

The International Electro-technical Commission maintains a large body of internationally accepted standards which in many cases originated as national standards in individual member countries and have been converted over to IEC standards. Given the large volume of such standards, only three example IEC standards could be selected for evaluation with regards to requirements for voltage withstand capability. These are:

- IEC 60071-1 Insulation Co-ordination
- IEC 61000-4-5 Electromagnetic Compatibility - Voltage Surge Immunity Testing
- IEC 61225 Instrumentation and Controls Important to Safety Requirements for Electrical Supplies

IEC 60071-1 was utilised in the design of the Forsmark NPP and the upgrade with lead to the 2006 event. IEC 61000-4-5 is a voltage surge test which is referenced by IEEE, the German KTA, and other IEC standards as an acceptable method to confirm over voltage withstand capability. IEC 61225 provides guidance on the general design requirements for safety related I&C electrical supplies. While this list of standards is not comprehensive, it also identified roughly the same assumed normal operating range of Umin = 80% nominal to Umax = 125% nominal.

Table B-3: Observations from IEC standards reviews

IEC standard	Edition reviewed	Reference section	Under-voltage/over-voltage issues considered:	Recommendation
60071-1	12/1993		This is a general standard for coordinating the power withstand voltage of insulated cables and major components. It does not provide guidance for determining recommended maximum operating voltages for lower voltage equipment such as inverters, battery chargers, UPS units.	None.
61000-4-5	4/2001	5. Test Levels	Defines "test levels" as either: Level 1 = 0.5kV Level 2 = 1.0kV Level 3 = 2.0kV Level 4 = 4.0kV Level x = Special to be identified	None.
		6.1 Combination Wave Generator	Contains general requirements for a standard voltage surge for a 1.2 µsec rise time/ 50 µsec half-width pulse to represent an "open circuit" surge and an 8 µsec rise time/ 20 µsec half-width pulse to represent a "short circuit" surge. The choice of the specific pulse shapes and duration is identical to IEEE Std. C62.41.2	None.
61225	12/2005	Informative Annex A.2.2	Notes that Battery Chargers be designed to function for dynamic AC power input range from U_{min} = 80% nominal to U_{max} = 120% nominal	Consider higher overvoltage range based upon experience.
		Informative Annex A.3.1	Notes that DC/DC converters should be designed to function for dynamic DC power input range from U_{min} = 80% nominal to U_{max} = 125% nominal	Consider higher overvoltage range based upon experience.

Appendix C

OSKARSHAMN NPP CASE STUDY

The case study material is made available by OKG AB, the owner and operator of the Oskarshamn NPP. The profiles are **not approved as requirements and prerequisites for analyses**. Further analyses and reviews are planned and going on. It should be noted that the profiles are specific for the Oskarshamm units and their connection to the grid.

C.1 Disturbance profiles

Various events in the power system may cause transient disturbances. Based on power system operator statistics of disturbances in the power system possible events can be stated. Failure statistics of the devices gives a failure rate of various faults at the devices. One though has to consider the uncertainty when using operator and failure statistics. With the background of statistics and experience a number of events have been selected for simulations.

Simulations of events in the power system and the three units of Oskarshamn NPP show a similarity of the voltage profiles of the units. Hence the same transient profile can be used for all three units. The simulations treats a limited number of cases, in reality the possible number of transient profiles that the plant can experience are much higher. Instead a limited number of synthetic Disturbance Profiles have been determined with the background of simulations and calculations. The profiles are chosen so the most extreme and difficult profiles due to faults on the grid or failure to operate of one component in the fault clearing system are being covered. Hence profiles generated from faults in the NPP generator step-up protection are not covered. However, any specific susceptibility of each safety related equipment must be checked to be covered by the selected profiles. It should also be noted that faults originating from the generator side of the unit transformer are not included.

All Disturbance Profiles consists of a Voltage Profile and a Frequency Profile. In some cases the voltage or the frequency is almost constant and is not shown. Voltage Profile 1 to 9 represents voltage on the generator terminal while Voltage Profile 11 to 13 represents the voltage on the busbar in the NPP substation (the 400/130 kV substation Simpevarp where Oskarshamn 1, 2, and 3 are connected to 4 outgoing 400 kV transmission lines and 4 outgoing 130 kV sub transmission lines).

The power plant should, amongst others, be designed to withstand voltage and frequency variations originating from:

- Normal operation
- Load rejection
- Start of larger units (motors)
- Shunt faults in the power system with correct fault clearance
- Shunt faults in the power system with operation of breaker failure protection

- Busbar fault with failure of operation of busbar protection system
- Busbar fault in adjacent substation with failure of operation of busbar protection system
- Line fault near the remote substation with failure of teleprotection channel
- Wide area disturbances
- Power system restoration

These transients and variations are detailed below.

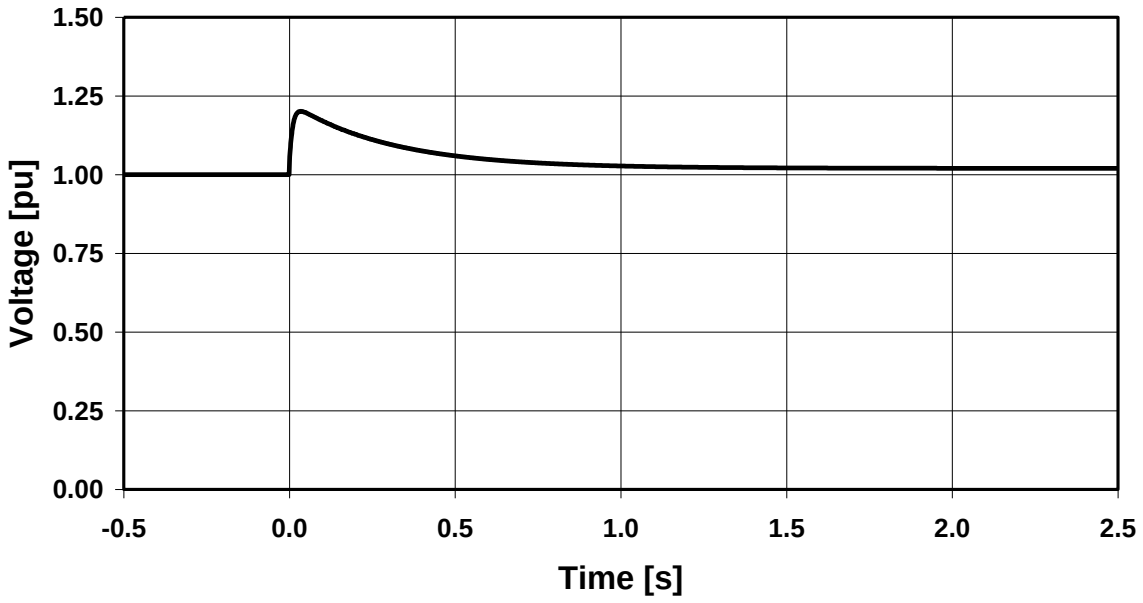
C.2 Load rejection

Load rejection occurs if the breaker disconnects the power plant from the transmission system. The inadvertent operation can be initiated from failures in the operating mechanism of the breaker or unwanted trip signal from the control system.

C.2.1 Disturbance Profile 1

Disturbance Profile 1 (see Fig. C-1) can be caused by an inadvertent breaker operation on the high voltage side of the generator step-up transformer during operation with full production in automatic voltage regulator (AVR) control mode. This event leads to an operation of the plant either in a successful house load operation (islanding) mode or a fast stop (scram). A scram implies tripping of the generator and field breaker after which the auxiliary power system voltage decays with a time constant of 5 to 10 seconds. Performed simulations show for Oskarshamn 1, 2 and 3 with static excitation systems, that the generator voltage does not exceed 120% of the rated voltage during house load operation with correct operation of the AVR. The decay back to normal operating voltage has been chosen with the background of recordings from the commissioning of the excitation system of Oskarshamn 1 and 2 and performed simulations.

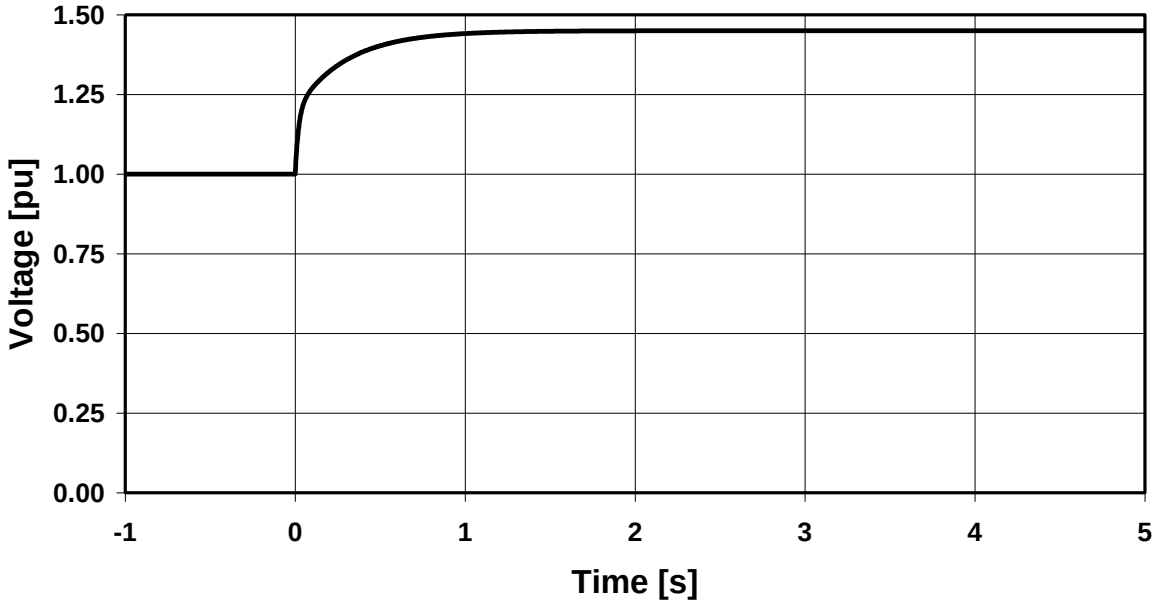
Figure C-1: Voltage Profile 1 (representing load rejection in AVR control mode)



C.2.2 Disturbance Profile 2

Disturbance Profile 2 can be caused by an inadvertent breaker operation at the high voltage side of the step-up transformer during operation with full production in field current regulator (FCR) control mode. During Geomagnetic Induced Currents (GIC) the control mode of the generator is switched from AVR to FCR according to the operating instruction of Oskarshamn 3. Some internal faults of the AVR cause an automatic transition to FCR mode. The voltage drop across the sub-transient reactance decreases to zero faster than a period. The no-load characteristic of turbo-generators is measured during workshop tests up to some 130% of rated voltage. The no-load characteristic has been extrapolated to full excitation current. The time constant depends on the ceiling factor of the excitation system and the setting of parameters in the FCR.

Figure C-2: Voltage Profile 2 (representing load rejection in FCR control mode)



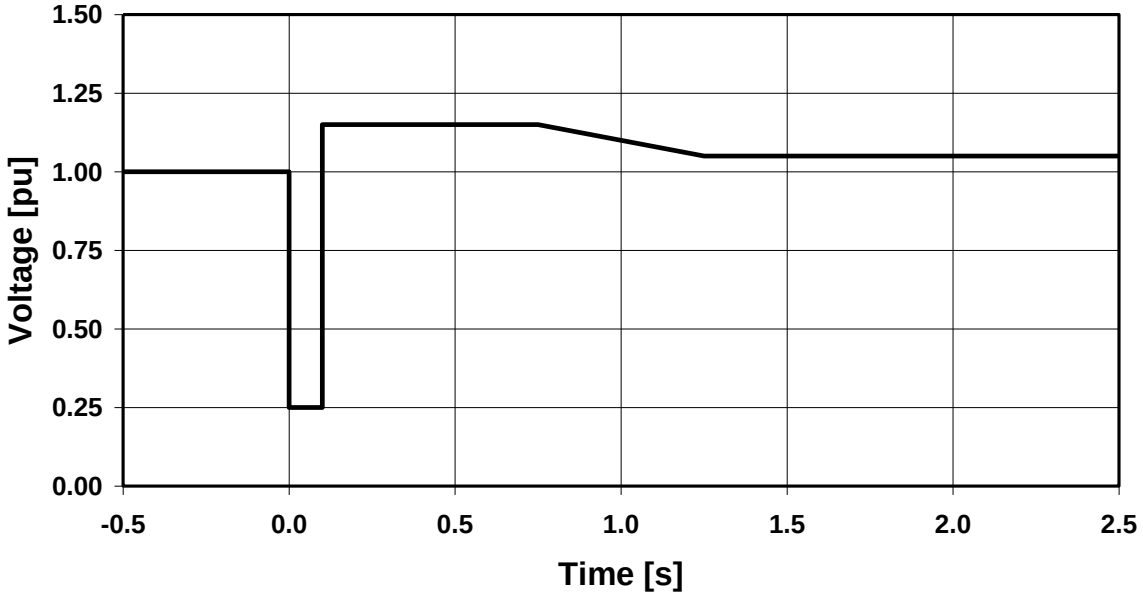
C.3 Shunt faults

A shunt fault is a short circuit between phase and earth or between phases. The most common cause of shunt faults in the transmission system (130-400 kV) is lightning strike at or close to a transmission line.

C.3.1 Disturbance Profile 3

A three-phase fault on the busbar in the NPP substation is cleared within 100 ms when the busbar protection and circuit breaker operates correctly. The voltage close to the fault location becomes zero and the currents normally increase and can be several times higher than the rated current. The voltage during the fault depends on the short-circuit reactance of the generator step-up transformer and the sub-transient reactance of the generator. Correct fault clearance operation has a fault clearance time of 100 milliseconds. This profile assumes a correct tripping to house load operation. The frequency is almost constant and equal to nominal system frequency (50 Hz).

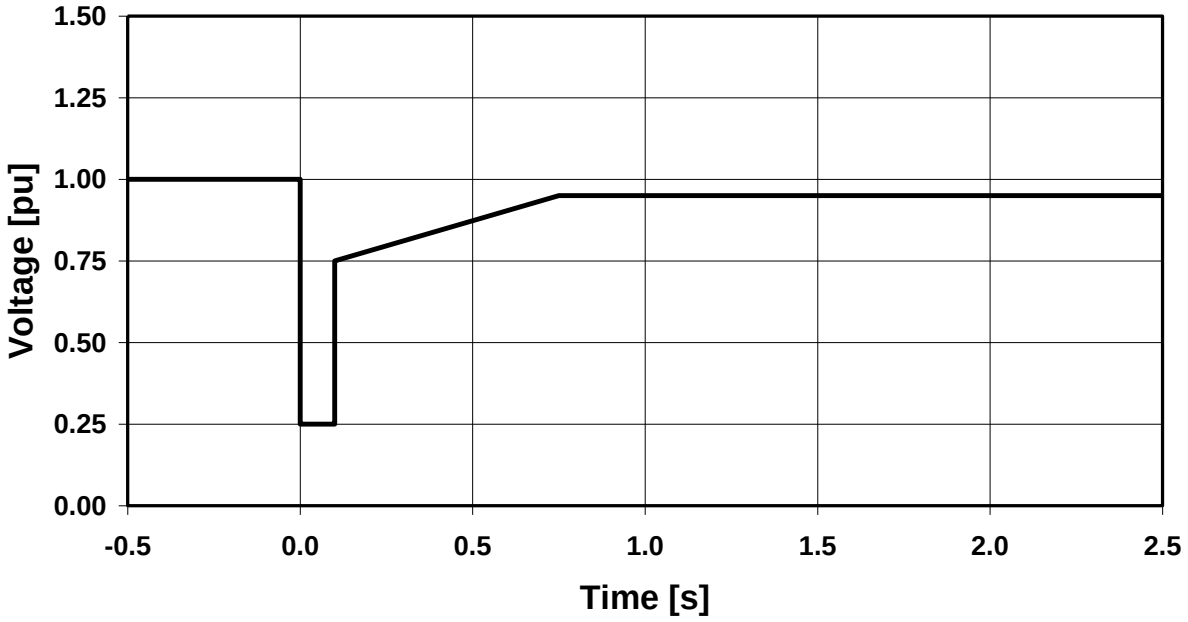
Figure C-3: Voltage Profile 3 (representing three-phase faults on the busbar in the NPP substation assuming correct operation of the busbar protection system and circuit breakers)



C.3.2 Disturbance Profile 4

Disturbance Profile 4 (Fig. C-4) can be caused by close-up three-phase faults on an outgoing transmission line assuming correct operation of the line protection and the line circuit breaker. The voltage during the fault depends on the short-circuit reactance of the generator step-up transformer and the sub-transient reactance of the generator. The power plant is not disconnected from the grid. After fault clearance the voltage remains low, due to the voltage drop across the transient reactance of the generator, when the transient rotor swing is decelerated. The frequency is almost constant and equal to nominal system frequency (50 Hz).

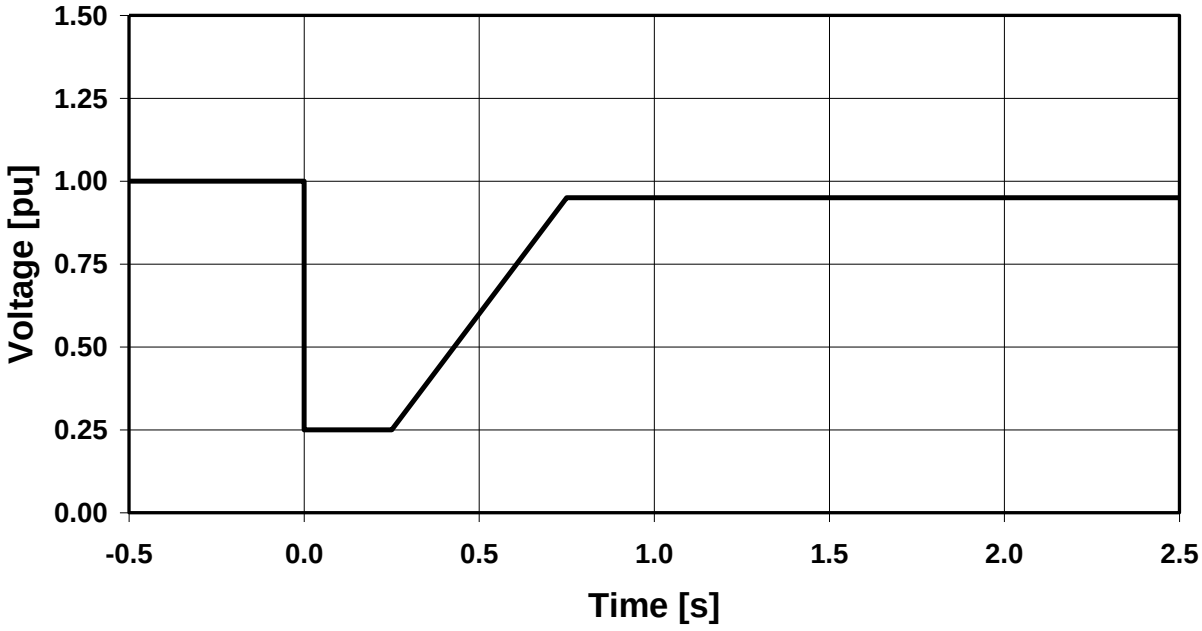
Figure C-4: Voltage Profile 4 (representing close-up three-phase faults on one outgoing transmission line from the NPP substation assuming correct operation of the line protection and line circuit breaker)



C.3.3 Disturbance Profile 5

Disturbance Profile 5 (Fig. C-5) can be caused by close-up three-phase faults on an outgoing transmission line from the NPP substation. The line protection system operates correctly but the line circuit breaker fails to interrupt the fault current and the Breaker Failure Protection (BFP) trips the adjacent circuit breakers. The fault clearance time includes the operate time of the line protection, delay of the BFP, and current interrupting time for the adjacent circuit breakers. The total fault clearance time is 250 milliseconds. The voltage during the fault depends on the short-circuit reactance of the generator step-up transformer and the sub-transient reactance and transient reactance of the generator. The power plant is not disconnected from the grid. After fault clearance the voltage remains low, due to the voltage drop across the transient reactance of the generator, when the transient rotor swing is decelerated. This is a standard case from grid code of NORDEL (Organisation for the Nordic Transmission System Operators). The frequency is almost constant and equal to nominal system frequency (50 Hz).

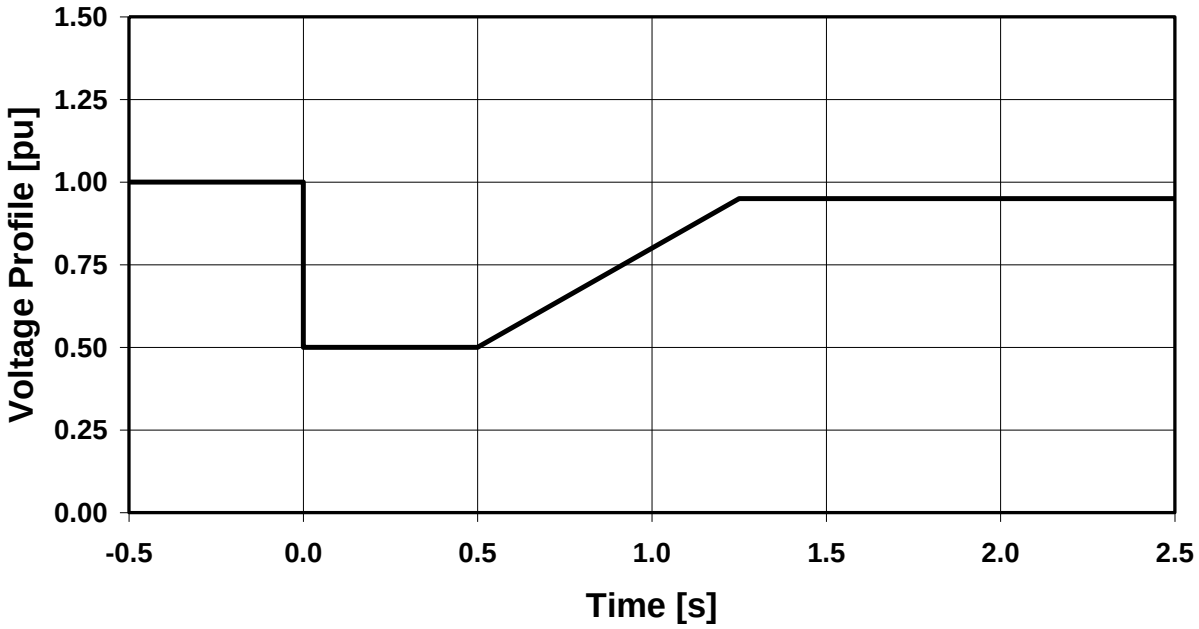
Figure C-5: Voltage Profile 5 (representing close-up three-phase faults on an outgoing transmission line assuming failure to operate the line circuit breaker - the NORDEL Voltage Profile)



C.3.4 Disturbance Profile 6

A three-phase fault occurs at the remote end of an outgoing transmission line or on the busbar in the substation at the remote end of the line. A long fault clearance time characterise this profile. In the case of a line fault the long fault clearance time originates from failure of the relay protection to communication with the protection of the substation busbar (interconnecting the power plant and the transmission system) in the case of line fault. In the case of a busbar fault the busbar protection is assumed to fail. The line protection of the power plant substation busbar is backup protection and the second distance step detects the fault and trip the line breaker. The total fault clearance time include trip signal from step two of the line protection and current interrupting time of the line breaker. The voltage during the fault depends on the short-circuit reactance of the generator step-up transformer, the sub-transient reactance and transient reactance of the generator and the line impedance. The power plant is not disconnected from the grid. After fault clearance the voltage remains low, due to the voltage drop across the transient reactance of the generator, when the transient rotor swing is decelerated. The frequency is almost constant and equal to nominal system frequency (50 Hz).

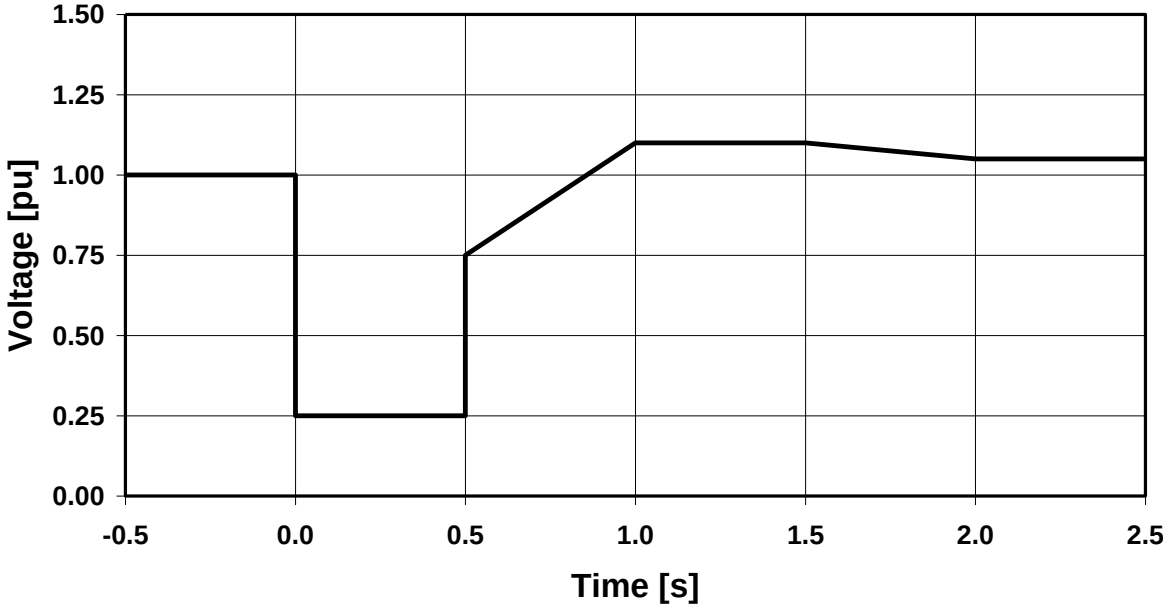
Figure C-6: Voltage Profile 6 (representing three-phase faults at remote end of outgoing transmission line accompanied by failure to operate of teleprotection channel or three-phase faults on busbar in the remote substation accompanied by failure to operate of busbar protection system)



C.3.5 Disturbance Profile 7

A three-phase short circuit occurs at the substation busbar interconnecting the power plant and the transmission system. This profile considers failure of operation of the busbar protection. The under impedance protection is backup protection for this event and initiates a trip signal for the breaker of the high voltage side of the generator step-up transformer. The fault clearance time is 500 ms and includes the trip time of the under impedance step that reach the busbar and current interruption time of the breaker. The voltage during the fault depends on the short-circuit reactance of the generator step-up transformer and the sub-transient reactance and transient reactance of the generator. After fault clearance the power plant is disconnected from the grid but operating in house load operation. The frequency is almost constant and equal to nominal system frequency (50 Hz).

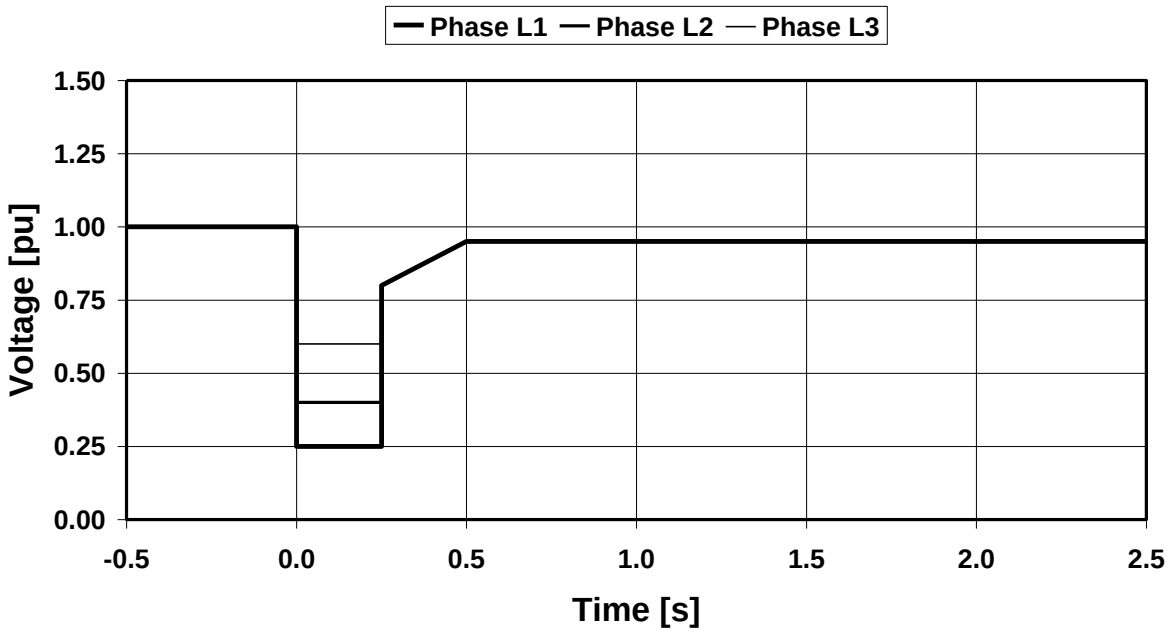
Figure C-7: Voltage Profile 7 (representing three-phase faults on busbar in NPP substation accompanied by failure to operate of busbar protection system)



C.3.6 Disturbance Profile 8

A two-phase fault occurs on an outgoing transmission line from the NPP substation. The relay protection system operates correct but the line breaker fails to interrupt the current. The BFP detects the failure of operation and initiates trip signals to the adjacent circuit breakers, which clear the fault. The voltage during the fault depends on the short-circuit reactance of the generator step-up transformer and the sub-transient reactance and transient reactance of the generator. One of the line-line voltages at the high voltage side of the step-up transformer goes to zero. The voltage decrease of the two other line-line voltages but does not reach zero. Fault clearance time include trip of the line protection system, the BFP and the current interrupting time for the adjacent breakers. The power plant is not disconnected from the grid. After fault clearance the voltage remains low, due to the voltage drop across the transient reactance of the generator, when the transient rotor swing is decelerated. The frequency is almost constant and equal to nominal system frequency (50 Hz).

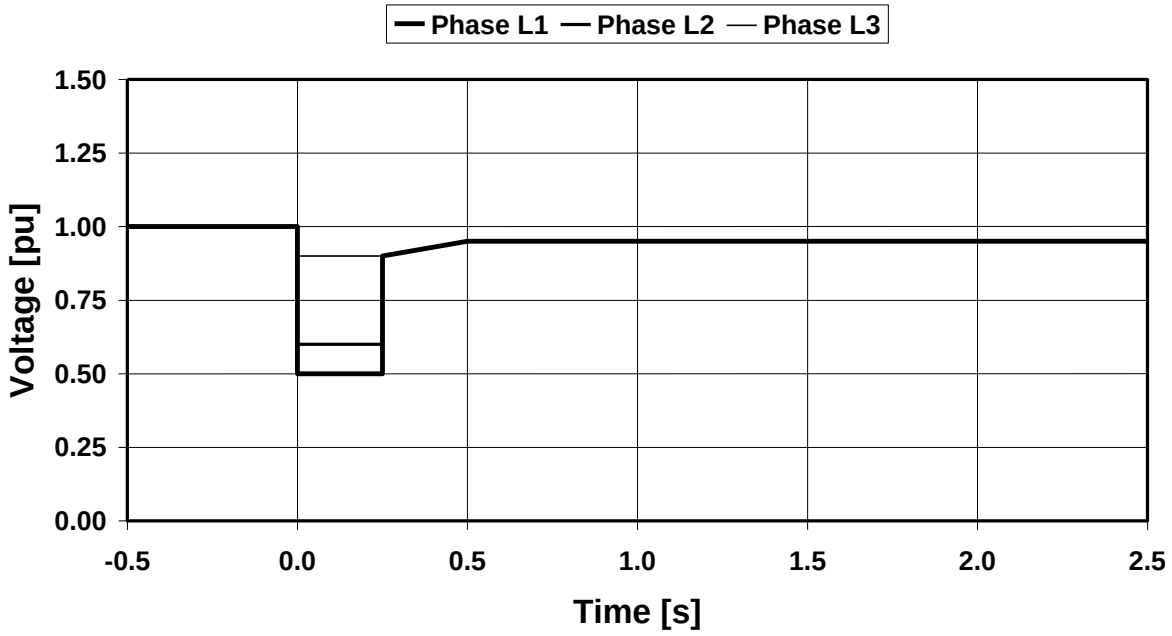
Figure C-8: Voltage Profile 8 (representing close-up two-phase faults on outgoing transmission line accompanied by failure to operate line circuit breaker)



C.3.7 Disturbance Profile 9

This profile represents single-phase faults on an outgoing transmission line from the NPP substation. The relay protection system operates correct but the line breaker fails to interrupt the current. The BFP detects the failure of operation and initiates trip signals to the adjacent circuit breakers, which clear the fault. The voltage during the fault depends on the short-circuit reactance of the generator step-up transformer and the sub-transient reactance and transient reactance of the generator. One of the phase voltages at the high voltage side of the generator step-up transformer goes to zero. The voltage decrease of the two other line-line voltages does not reach zero. The fault clearance time includes trip of the line protection system, the trip time of the BFP and the current interrupting time of the adjacent breakers. The power plant is not disconnected from the grid. After fault clearance the voltage remains low, due to the voltage drop across the transient reactance of the generator, when the transient rotor swing is decelerated. The frequency is almost constant and equal to nominal system frequency (50 Hz).

Figure C-9: Voltage Profile 9 (representing close-up single-phase faults on outgoing transmission line accompanied by failure to operate line circuit breaker)



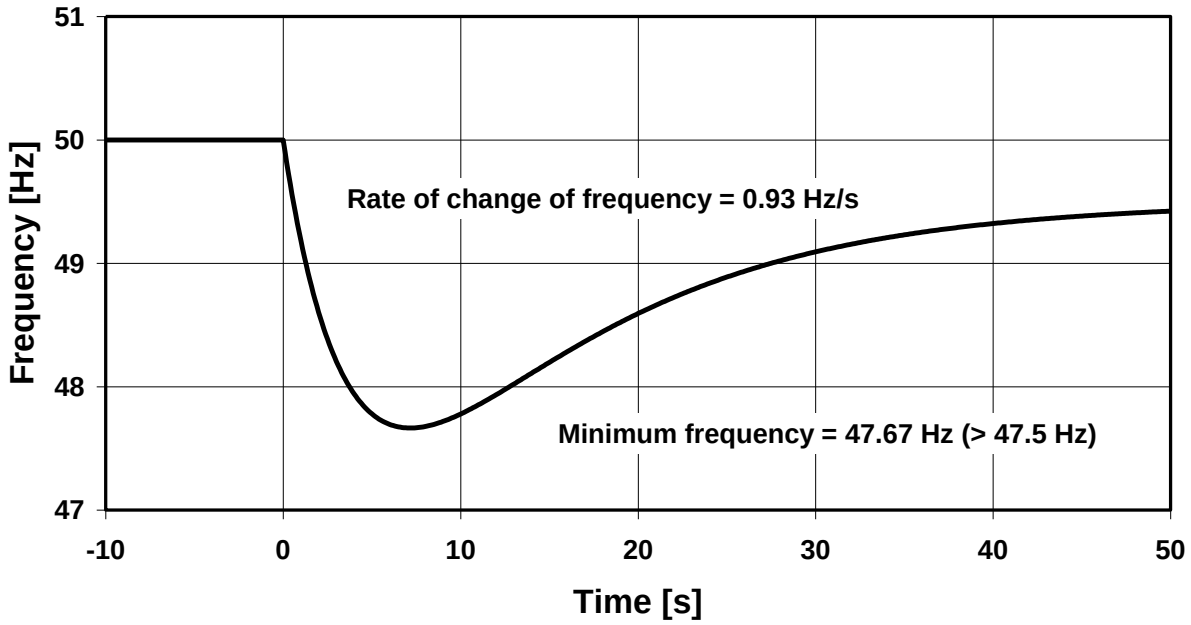
C.4 Wide area disturbances

Wide area disturbances strikes entire or large parts of a power system. The event is exceptional and is generally caused by a degradation of the capability of generate and transfer power.

C.4.1 Disturbance Profile 10

The spinning reserve in the NORDEL system is dimensioned for withstanding a shedding of the largest power generating plant in operation. Radial connected plants with surplus of generated power that is expected to be disconnected from the grid more frequently than every third year are also included in the dimensioning. The instantaneous backup for loss of generation is dimensioned for a lowest frequency of 49 Hz and a recovery to at least 49.5 Hz within 30 seconds. The grid frequency usually reaches its minimum within 10 s after the loss of generation, which has been registered at several disconnections of larger power plants. Avoiding severe impacts from a large loss of generation can be achieved by employing Automatic Load Shedding (ALS), Emergency Power Control (EPC) i.e. HVDC power transfers from other synchronous areas and starts of gas turbines. A larger loss of generation than the dimensioned causes a larger frequency drop. The grid code specifies an under-frequency limit of 47.5 Hz when the power plant should be instantaneous disconnected from the grid. The profile is mathematically developed for a frequency minimum at 47.5 Hz that occurs 5 to 10 seconds after the loss of generation is initiated and a recovery to 49.5 Hz in accordance with the NORDEL operating conditions regarding frequency control. The voltage on the busbar in the NPP substation is almost constant and equal to the voltage during normal operation.

Figure C-10: Frequency Profile 10 (representing loss of several power plants)



C.4.2 Disturbance Profile 11

Voltage collapse is a wide area disturbance that seldom occurs in the south of Sweden. In modern time two disturbances have been experienced, in 1983 and 2003. The voltage (Fig. C-11a) and frequency (Fig. C-11b) profiles have not been based on an analysis of an exact course of events, since experiences from the operation of the system showed that the event originates from several events and failures unlikely to occur. The profiles are mainly developed on the base of the recordings of the wide area disturbance in Sweden 1983 and the condition that the power plant is interconnected in a part of the power system with a large lack of generation. This leads to rapid frequency decay and stored energy in the rotating part of the plant is quickly fed into the power grid. The large load current causes a large voltage drop in the sub-transient and transient reactance of the plant. The maximum rate of change of frequency reached 4 Hz per second. The maximum rate of change of voltage varied in the interval of 10%- 20% per second. The voltage and frequency profile have been chosen on the basis of these characteristics. Intended for auxiliary power system studies the characteristics represents a good approximation of a fast voltage collapse. The voltage profile relates the NPP substation voltage.

Figure C-11a: Voltage Profile 11 (voltage collapse in wide area disturbance)

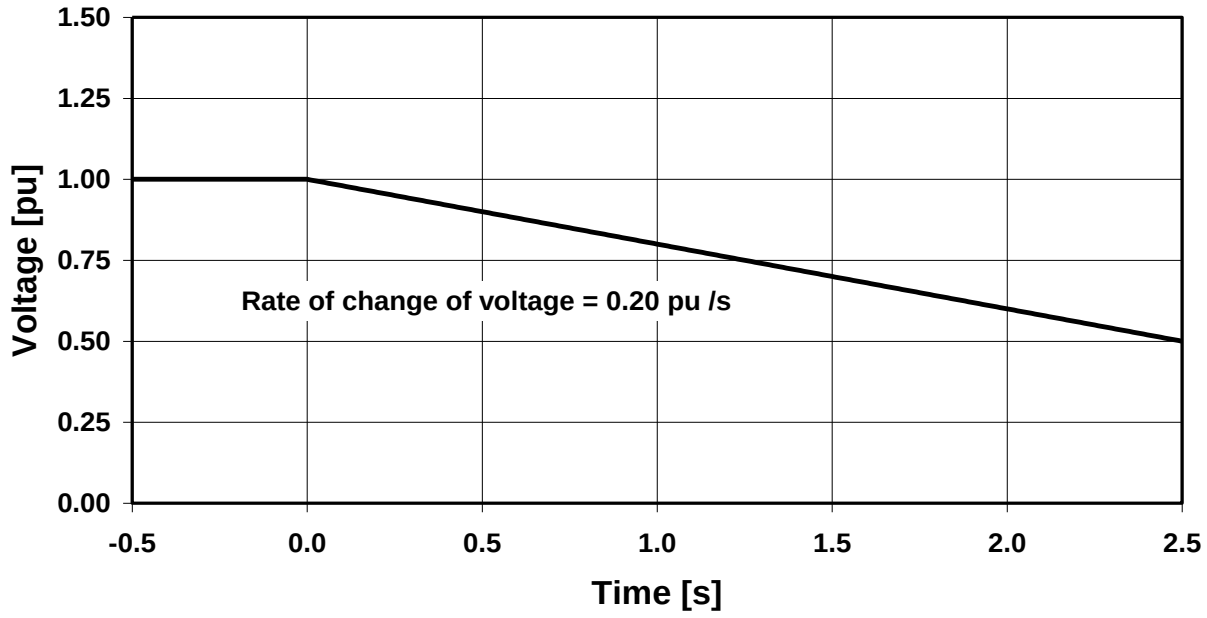
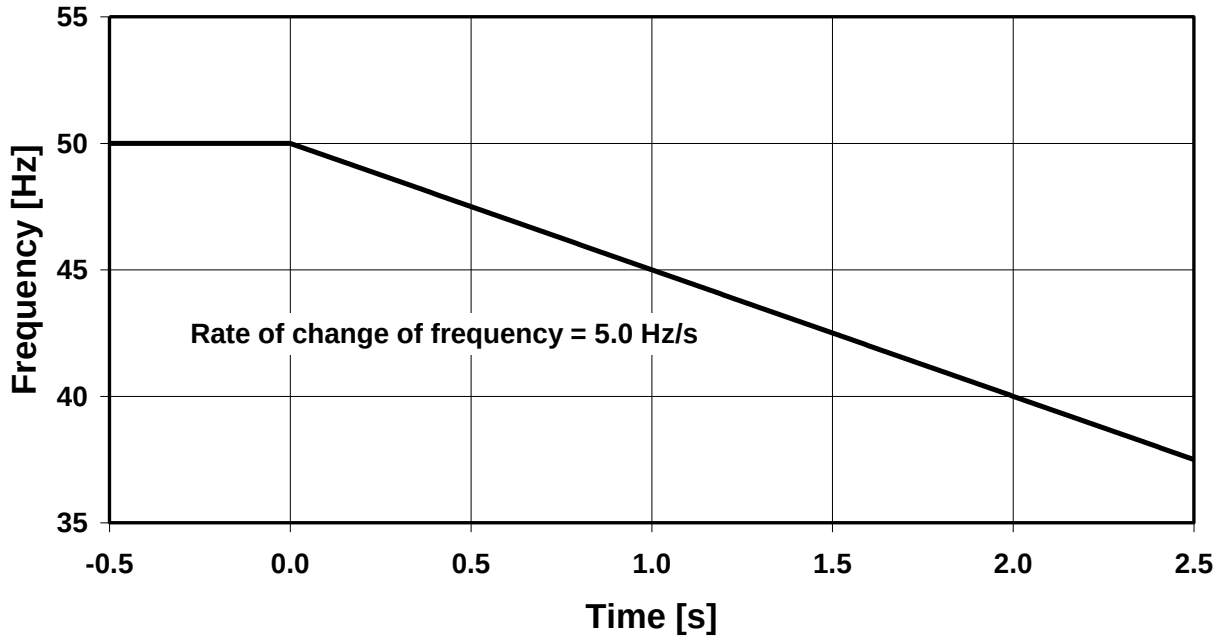


Figure C-11b: Frequency Profile 11 (frequency collapse in wide area disturbance)



C.4.3 Disturbance Profile 12

The wide area disturbance in Koeberg (South Africa) 1998 showed that a voltage collapse could be slower than the voltage collapse in Sweden 1983. The course of events of the disturbance is not possible to predict since it originates from a number of several events and failures unlikely to occur. The voltage and frequency profiles are developed on the basis that the power plant is

interconnected in a part of the power system with a lack of generation where the voltage collapse after a while. The weak system is interconnected with another part of the power system. The voltage drop is caused by a rapid load increase and the control of tap changing transformers that cause an increase of power generation in another part of the system. This means an increased power transfer towards and within the weak network.

The slow initial rate of change of voltage is chosen to 3% per minute while the final rate of change of voltage is chosen to 20% per second. The transition between the slow and fast rate of change of voltage occurs at 70% of nominal voltage. This value originates from a theoretical consideration of a radial system transferring only active power at the maximum operating point. If more power is transferred the voltage will decrease and the active power will decrease. Probably the states are changed rapidly hence the characteristic will be much like the wide area disturbance in Sweden 1983. The grid frequency remains stable until the transition from slow to fast rate of change of voltage where a rate of change of 5 Hz/second is chosen. The voltage profile relates the NPP substation voltage.

Figure C-12a: Voltage Profile 12 (Koeberg, South Africa, 1998 voltage collapse)

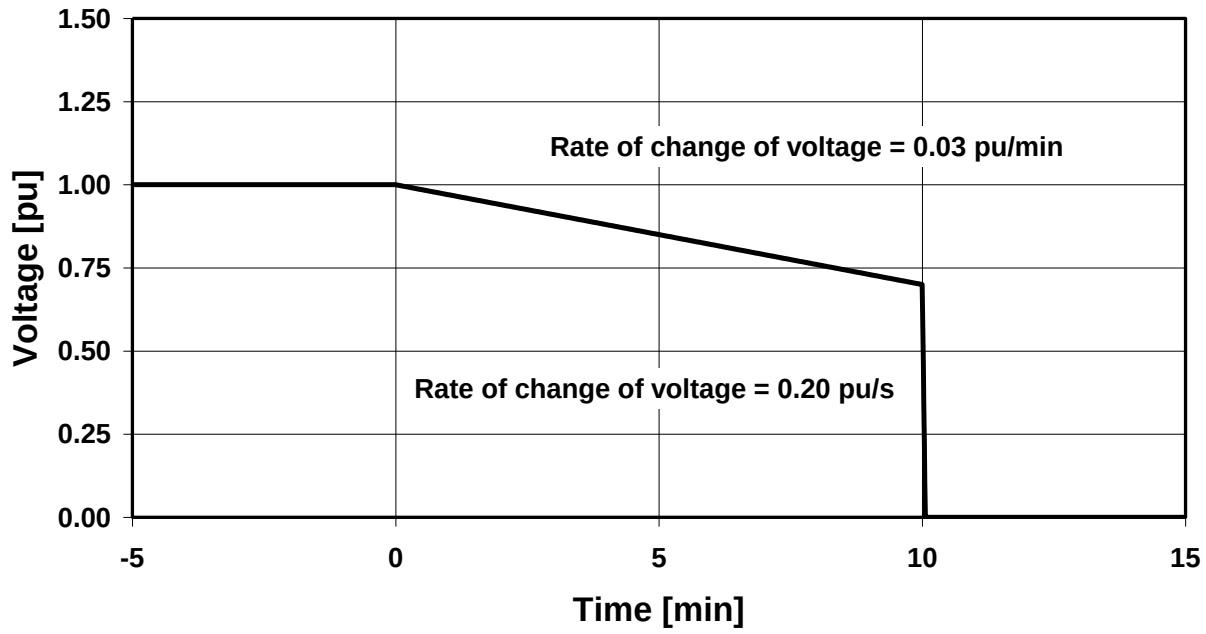
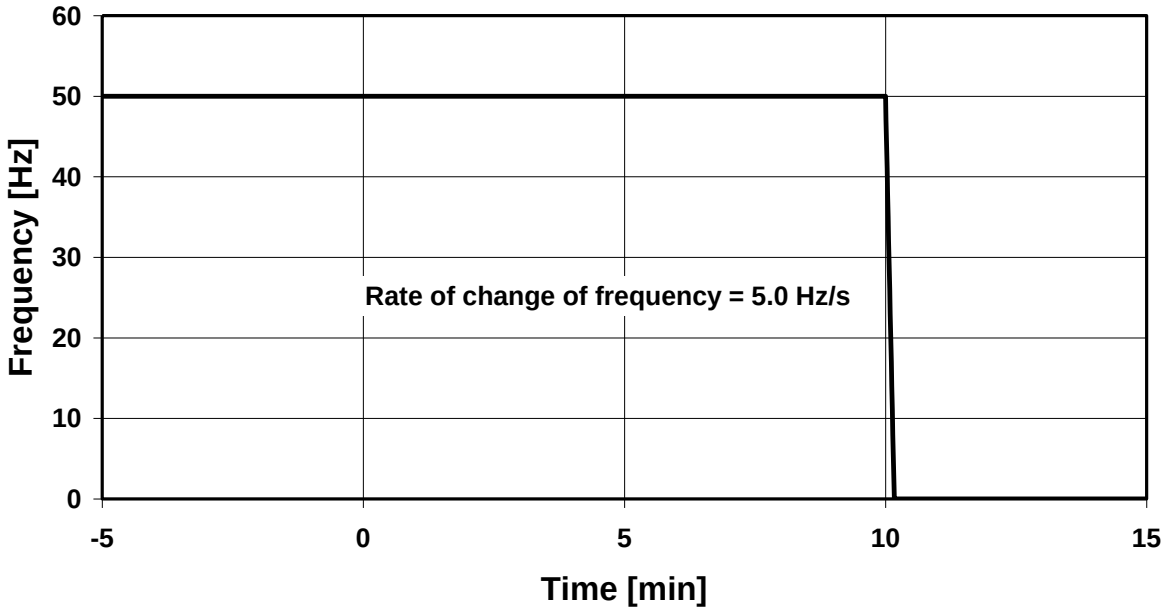


Figure C-12b: Frequency Profile 12 (Koeberg, South Africa, 1998 frequency collapse*)*



C.4.4 Disturbance Profile 13

Assume the transmission system would be experiencing a major disturbance that could lead to voltage collapse if not automatic or manual load shedding is applied. Today a very limited part of the consumers are disconnected at low voltage in the south of Sweden. On the other hand the Swedish transmission system operator (TSO) Svenska Kraftnät (SvK) may in the future employ EPC with manual load shedding on transmission lines in order to avoid a voltage collapse. The voltage may be stabilised at a level where the gas turbines in the south of Sweden cannot be phased to the grid. The phase automatics in the gas turbines normally operate in the interval between 90 and 110% of the nominal voltage. Generally the generator step-up transformer of the gas turbine is not equipped with tap changers and can therefore not be phased into the grid at lower voltages than 90% of the grid nominal voltage. If the transmission link voltage decreases below 70% a voltage collapse will most likely occur. Hence the voltage dip expects to be stabilised at 80% of nominal voltage. The voltage profile has been derived on the basis of recordings of disturbances in Finland and South Africa and has a rate of change of voltage of 5% per minute and stabilises at 80% of nominal voltage. The voltage profile relates the NPP substation voltage.

Due to the load shedding in the south of Sweden a surplus of generation arise in the power system. The frequency may increase above the normal operation value, which is in the interval of 49.9 and 50.1 Hz. It cannot be omitted that resolute load shedding in the south of Sweden is followed by a rapid shedding of generation in the synchronous operated power system. The estimated shedding of power may reach up to between 2000 and 4000 MW. With a power-frequency characteristic in the interval from 4000 to 6000 MW/Hz a frequency increase to 50.3 Hz is reasonable. This value is lower than the upper frequency threshold (51.0 Hz) that large thermal power plants should comply with, specified by the NORDEL grid code for thermal power plants. The frequency profile is designed with a rate of change of frequency with 0.1 Hz/minute and is initiated a certain time after the disturbance occurs.

Figure C-13a: Voltage Profile 13 (representing voltage degradation)

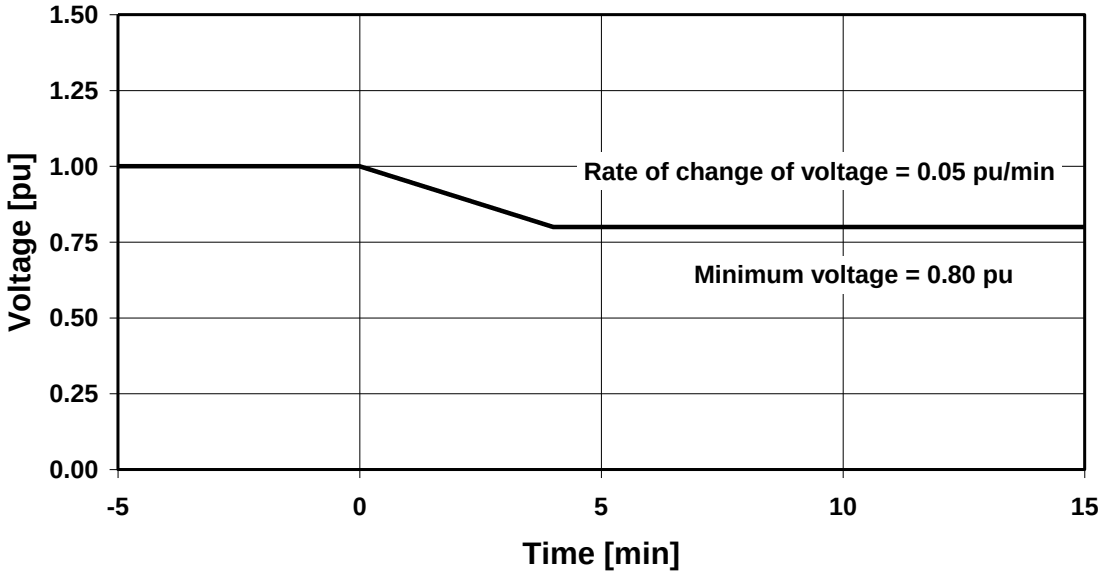


Figure C-13b: Frequency Profile 13 (representing voltage degradation)