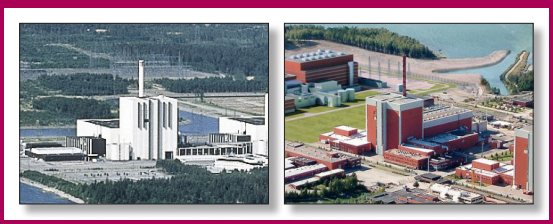
Nuclear Safety
2013

CSNI Technical Opinion Papers No. 16

Defence in Depth of Electrical Systems



OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Nuclear Safety

CSNI Technical Opinion Papers

No. 16
Defence in Depth of Electrical Systems

NEA No. 7070

NUCLEAR ENERGY AGENCY
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

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

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

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

This work is published on the responsibility of the OECD Secretary-General.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 31 countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, the Republic of Korea, the Russian Federation, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission also takes part in the work of the Agency.

The mission of the NEA is:

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

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

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

Cover photos: Forsmark-1, Sweden (SKB); Olkiluoto-1, Finland (Framatome ANP).

Foreword

The electrical transients that occurred in July 2006 at Forsmark-1 in Sweden and in May 2008 at Olkiluoto-1 in Finland revealed weaknesses in the general understanding of electrical power supply hazards to systems and components important to safety. Subsequent investigations showed that other units throughout the world also had weaknesses of a similar or related nature. There is therefore a need to better identify the potential challenges from the behaviour of the grid and in-plant generators to in-plant distribution systems.

The OECD Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) authorised the formation of a task group to examine the defence in depth of electrical systems and the grid interaction with nuclear power plants (DIDELSYS). The general objectives of the DIDELSYS task group review were to evaluate:

- the robustness of existing safety-related electrical systems in nuclear power plants (including design standards, acceptance criteria and design-basis disturbances);
- the basic principles used to develop a robust safety-related electrical system in terms of critical design features, redundancy, diversity and the use of proven technologies;
- methodologies used to demonstrate the robustness of safety-related electrical systems, considering the 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), and the definition of safety margins;
- 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 (NPPs).

This effort was completed following an international technical exchange workshop held at the OECD in May 2009 and summarised by a technical report issued in 2009. The CSNI subsequently authorised a DIDELSYS follow-up effort to:

- identify elements of guidance and methodology on how to periodically carry out a systematic hazard review of possible voltage transients which could occur from the grid and in NPPs;
- identify limiting characteristics which result from the faults and which can be used as design-basis events for NPP onsite electric system evaluations;

- gather information via a questionnaire on what modifications have been made to address the Forsmark event, and the technical bases and rationale upon which such modifications were made;
- identify the needs for comprehensive updates of existing electrical standards.

At the conclusion of these efforts it was requested that a technical opinion paper be prepared to summarise the current state of knowledge of in-plant and external grid-related challenges to nuclear power plant safety-related electrical equipment, which areas require further research and investigation, and how nuclear power plant operators can demonstrate adequate defence in depth against such voltage and frequency transients.

Table of contents

1. Introduction

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. 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. Lightning protection is accomplished via insulation ratings, grounding provisions, and incorporating design features, such as high voltage surge arrestors, sized according to internationally accepted industrial design standards.[1]

However components could be subject to other types of overvoltage events for which the withstand capability is not as clear. 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 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 the majority of currently operating nuclear power plants are powered via the preferred power supply any overvoltage transient in these

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

systems could lead to common cause failure. In the event of an unusual electrical system transient it is essential that safety related equipment be isolated or protected from the fault in some manner in order to assure ability to safely shutdown the reactor and remove decay heat. This is particularly important for reactor types which are totally dependent on onsite AC power sources for decay heat removal.

This TOP was prepared by the DIDELSYS working group based upon a multi-year CSNI sponsored effort which included two international technical exchange meetings (held in: May 2009, and May 2011); four DIDELSYS working group technical meetings; consultations with representatives of international standards (e.g. IEEE, IEC) and reactor design organisations (AREVA, Westinghouse, GE-Hitachi, Mitsubishi); and involvement of nuclear safety regulators from France, Germany, the Republic of Korea, Spain, Sweden, the United Kingdom and the United States. The DIDELSYS effort did not initiate new research projects in the areas of interest, but drew upon the ongoing efforts in OECD member countries to address the safety concerns of the July 2006 Forsmark and May 2008 Olkiluoto events. It is the result of a multi-year review carried out by the DIDELSYS working group of: actual operating experience, onsite electrical system designs, electrical equipment qualification and design standards, and possible methods of demonstrating adequate safety margins.

This TOP can serve as a basis for further international research co-operation, international electrical standards development, and safety analysis methods to address the concern of common cause failure or safety related electrical supplies.

2. DIDELSYS programme topics

2.1 General

The specific technical issues evaluated in the DIDELSYS effort include the following:

- Characterisation of grid challenges.
- Risks and benefits of capability to runback to house load operation.
- Communication interface between nuclear power plant and the electrical power grid.
- Nuclear power plant operators response to electrical events.
- Power supply requirements for protection and control systems.
- Power supply requirements for nuclear power plant operator information systems.
- Characteristics of high reliability onsite power supplies.
- Consideration of desired “fail safe” conditions.
- Challenges in evaluating FMEA and diversity of onsite power systems.
- Conflicts between protection and reliability.
- Special considerations for digital protective relays.
- Areas of potential gaps in current international electrical standards.
- OECD member activities to address the implications of the Forsmark and Olkiluoto events.

2.2 Characterisation of grid challenges

Electrical grid connections to a nuclear power plant (NPP) allow the 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. Typical design requirements include provision for an offsite electric power system and an onsite electric power system to permit functioning of structures, systems, and components important to safety. Even though NPPs always have on-site

emergency electrical supplies, (diesel generators, gas turbines, etc) the reliability of the grid connection makes a significant contribution to the overall reliability of post-trip cooling.

Faults 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 principles for NPPs require that the reactor can remain safely at power for a range of expected variations in grid conditions (voltage, frequency), 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 must not inhibit the operation of, or cause failure of, systems required for safe shutdown of the nuclear plant.

The design bases for the on-site electrical systems account for the continuous operating range of voltage and frequency, all possible events that could cause transient, dynamic or continuous variations of them, and internal and external hazards that threaten the availability of power supply to the plant. Incomplete design bases, resulting in equipment not qualified for the intended function, cannot be solved by redundancy or diversity. This section discusses some of the challenges.

Overvoltages from lightning and switching

Even if design bases information on overvoltages from lightning and switching is provided for the prime power plant components such as the main transformer and main generator it is important to recognise 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 (such as those used for local motor control) often require an additional overvoltage protection in addition to the busbar mounted surge arrester rating. It is of course important that equipment in Class 1E systems is not affected. However, non-Class 1E equipment should also be considered because a failure in non-Class 1E equipment (e.g. main generator protection), could lead to power frequency voltage transients, detrimental to Class 1E equipment.

Power frequency and voltage transients

Most grids 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 be designed to 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. Similar requirements are set for frequency transients. 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 cope with these extremes

simultaneously. The generating unit(s) in a nuclear plant assists in controlling the local grid voltage and frequency, consequently, tripping a reactor and its associated generating unit is likely to cause a change in local grid voltage ad frequency. 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 typically take this into account.

Voltage transients induced from the grid

Faults on the grid system will not only lead to the risk of initial fast overvoltages, e.g. lightning overvoltages, 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 off 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 though such faults and not be tripped by them. In many countries NPPs should also be designed and to meet these grid codes.

If the fault is not cleared by the primary electrical protection on the grid system the fault must be cleared by the back-up protection. Not all countries have grid system requirements for a power plant to be able to continue operation without tripping in the presence of such faults. However, with modern relay protection and modern breakers a shorter back-up protection clearance time can be achieved. During such a fault the generator cannot deliver the full power given by the turbine. 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

The frequency of the grid system (60 Hertz or 50 Hertz) input varies very slightly throughout the day with variation of demand[1] and events leading to

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

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.

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. PWRs address this concern by providing an automatic reactor trip if reactor coolant pump flow or pump speed is sensed to be inadequate.

In particularly when safety grade loads are modernised the proper co-ordination 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 load changes occur, not only the frequency changes, but 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 overvoltage 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 much 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.

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 overvoltage 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.

Voltage and frequency transients and variations induced from the NPP

One potential issue concerns rate of change of frequency. Fast transients of overvoltage 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 overvoltage and frequency, for the latter however with a rate-of-rise lower than for the voltage. 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 overvoltage transient might disable the Class 1E loads. Several different scenarios, for instance: with faults in the exciter, voltage regulator, etc. have to be considered. Overvoltage situations might of course also occur. The more difficult cases are gradual voltage reductions in isolated buses that could disable multiple safety systems.

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 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 overvoltage 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.

2.3 Characterisation of in-plant challenges

If a nuclear plant is separated from the grid and in operation supplying only house loads, 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 over-speed protection (as high as +10% with mechanical over-speed trips).

Fast transients of overvoltage in the auxiliary system of the NPP can occur when the generator, supplying power to the grid, is suddenly disconnected from

the grid. A high load and level of excitation on the generator will generate a high overvoltage 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 overvoltage 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 applied maximum excitation, and 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 safety classified flywheel generator systems, which are installed parallel to each main circulation pump to slow down the loss of recirculation flow in case of loss of power supply.

Overvoltage situations might of course also occur. The more difficult cases are gradual voltage reductions in isolated buses that could disable multiple safety systems. 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 2.4 “Risks and benefits of capability to runback to house load operation”, NPPs with house load capability have more scenarios to consider than NPPs without this capability. However, NPPs which are not designed to transition to house load operation are not automatically excluded from possible electrical transients.

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 of a single piece of 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 overvoltage relay protection fails to operate, 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 designed to cope with 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 number 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.

2.4 Risks and benefits of capability to runback to house load operation

The capability for power plants to operate completely isolated from the grid only supplying their own auxiliary power, often referred to as house load operation, is implemented on many 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 differ 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 currently no plants in the United States[2] 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[3] (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 and increases power supply capability to the auxiliary systems (see also Section 2.9). On the other hand, house load operation capability increases the cost of the NPP (e.g. the main condenser would need to be oversized) and can generate transients in the onsite electrical system if there is an incorrect installation or an unrecognised design fault in the equipment, 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.

2. Although Palo Verde Units 1, 2, and 3 in the United States 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 reactor protection system trips being generated by abrupt sensed changes to core power distribution.
3. This is the classical "n-1" criterion.

In NPPs designed for runback to house load operation, a main generator breaker is generally preferred[4] 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,[5] 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 the levels needed to support 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. Some nuclear power plants do not have a generator breaker installed, but only a generator disconnect switch (which is not designed to isolate electrical faults). 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.

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

4. 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.
5. The sizing of the main condenser and turbine bypass valve system is primarily driven by the need to maintain coolant system pressures within a controlled range following a turbine trip.

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 pressure and level controller (PWR);
- steam generator level controller (PWR);
- turbine speed governor;
- turbine pre-heater and drain tank level controllers;
- main generator voltage regulator;
- reactor power controller;
- steam bypass controller;
- condensate and feed water flow controllers.

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. Although not limited to power plant with house load capability, the power update and modernisation of process equipment could give rise to an increased risk from the loss of original design margins and introduction of new failure modes.

Units designed for transition 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, or under frequency relays. In the case the undervoltage remains beyond the anticipated breaker failure protection clearing time (typically 250 ms), an overvoltage 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. 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 as 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.

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 was described in Section 2.1, "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, the 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 be used for anticipatory EDG start to provide rapid re-energisation of safety buses. Even if the transfer to the alternative offsite power supply, or re-energising the 1E buses from the EDGs normally should not increase the risk of generating transients on all auxiliary loads, this needs to be verified.

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 Blackout (SBO) supply exists (e.g. a dedicated gas turbine unit which is normally disconnected from the grid or a dedicated connection to a hydroelectric facility). 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 system 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 overvoltage 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.

Summary of major benefits and risks

Benefits:

A nuclear power plant designed for runback to house load operation in general (following a unit breaker opening):

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

A nuclear power plant without house load operation capability in general:

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

Drawbacks:

An NPP with house load operation capability in general:

- needs a more complex control system design;
- is more likely subject to failure;
- has a higher investment cost;

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.

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

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.

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 stresses 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.

Hence we consider all four cases which should be part of the operational procedures to handle the interface of NPP with the grid. In the case of normal operation: the TSO will electronically acknowledge daily; the power values from the NPPs (which are base-load operated) are normally transmitted well in advance; 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 NPP's power recorder. There are also limits from the maximum voltage level in the high voltage switchyard.

Start-up and shutdown activities require in particular very good communication between the NPP operator and the grid operator, with agreed warning delays and dedicated responsibilities.

2.6 Nuclear power plant operators response to electrical-related operating experience events

Following the July 27, 2006 Forsmark Unit 1 event, the information about the event was spread through the International Reporting System (IRS) system (IRS Report 7788). In 2008, the European Union Clearinghouse on Operational Experience (European Clearinghouse) issued a report on the Forsmark event (NPP Clearinghouse report 2008/02) and included the actions taken by several EU countries. Additionally, many countries have also written their own technical reports about the event.

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 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 Unit 1 in 2006 and Olkiluoto in 2008 are such accident precursors.

At the 5th WGOE meeting in spring 2009, the regulatory practices and methodologies applied by member countries in response to the Forsmark event were discussed in a roundtable exchange, and it was agreed to write summaries on the WGOE member country activities taken in response to Forsmark event in a standalone NEA report. At the 6th WGOE meeting fall 2009, it was decided that Sweden would take the lead to write a WGOE report including updated regulatory responses to the Forsmark event and also include actions taken in response to the outcome from the DIDELSYS task group. Some countries provided several updates to their country's actions. At the 8th WGOE meeting fall 2010, it was decided to stop collecting input and publish this report. The status report summarised the country actions and responses to the event in short term and to the up to date responses to the DIDELSYS findings in long term, and was published in December 2010.

The CNRA WGOE Report on "Country Regulatory Response to the Forsmark-1 Event of July 27, 2006 and NEA/CSNI DIDELSYS Task Group Report recommendations" contains summary response to the Forsmark-1 event and DIDELSYS recommendations from 17 countries.

A number of reactor designs were represented in the WGOE Report, for which review had been performed and which involves PWR, BWR, VVER, CANDU, Magnox, and RBMK reactor designs. Electrical system design generally varies among nuclear power plants; it was observed that countries having similar plant design to Forsmark-1 had performed an in-depth review of their design against weaknesses identified during the Forsmark-1 event. Other countries, having different type of the plant design had performed a comparative review in order to verify whether similar design weakness as observed in Forsmark could be applicable to their plant specific design.

A scope of review varies from one country to another. What is important, however, is that every country carefully considered the lessons learned from the Forsmark-1 event. Some countries have also prepared detailed technical reports addressing specific issues relevant to their nuclear power plants.

A review approach focused primarily on evaluation of the potential impact of the voltage transient on individual safety related electrical equipment, e.g. emergency diesel generator, safety bus bar protections, UPS, etc. Some countries reported that they had identified the existing or potential design (or operational) deficiencies of the plant electrical system.

An update on the implementation status of the DIDELSYS Task group recommendations in some countries is provided as well; in particular country's confirmation as to whether the analysis of the plant electrical systems has covered all the potential susceptibilities as indicated in the DIDELSYS outcomes i.e. i) preventing electrical grid and plant from generated electrical faults, ii) robustness of nuclear power plant electric power systems, iii) improving training, procedures, and information capabilities, iv) coping capability of nuclear power plants, and v) electrical system recovery.

A list of corrective measures that some countries implemented in response to Forsmark event and DIDELSYS Task group recommendations is also provided. Nevertheless, there is little information available about what has actually been identified (system, component, deficiency, etc.), and what specific recommendations have been made to resolve the problem. In order to ensure maximum benefit from the sharing of lessons learned, as well as to provide practical experience for operational feedback, the responses of participating countries may provide more detailed information about the specific system, components and corrective action involved. With this regard, DIDELSYS 2 TG performed a survey in OECD/NEA member countries in order to get the latest update on corrective actions taken after Forsmark-1 event. TOP Section 2.14 (OECD member countries activities to address the implications of the Forsmark and Olkiluoto events) provides summary results of that survey.

2.7 Power supply requirements for protection and control systems

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 were: a) switchyard maintenance, b) unsuccessful House Load Operation, c) unsuccessful transfers to auxiliary power supply, d) dependence on UPS for the operation of the emergency diesel generator, and e) Performance of UPS.

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) a rugged DC bus system, b) a robust electrical grid, c) a successful transition to House Load Operation (if it is used in the specific plant design), d) a properly designed power transfer system, e) an onsite emergency power source (EDGs), and f) alternate AC Power Sources (AAC).

DC system

A reliable DC power system is one of the primary lines of defence 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.

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 overvoltage detection for Class 1E buses; power supply for AC instrument buses; breaker operation for ECCS pumps and for the ECCS pumps themselves. The failure of DC bus could disable the entire electrical train and steam/diesel driven systems.

DC buses generally demonstrate very low failure rates. 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.

Robust grid

In order to encourage competition and produce competitive pricing in production of electricity, certain countries have deregulated the energy sector. Electrical power has 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. 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.

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.

The USNRC 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.

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.

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.

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.

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.

2.8 Power supply requirements for nuclear power plant operator information systems

This section discusses electrical power supplies to the NPP operator information systems, information systems, norms and standards. The operators in nuclear power plants have to rely on information available to them to operate and control the plant. Different type of information is generally provided to operators:

- Modern control rooms are equipped with integrated displays and control systems which provide system status, displays, recorders, annunciators.
- Status lights: which provide indication that 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/set points.
- Control: push buttons to operate equipment like such as: valves, pumps, fans, switches.

In addition, computers can provide for complementary information on the history in log files. Modern digital technology can further provide for information better “formatted” to assist the operators in monitoring and controlling the plant parameters. In the control room, operational (e.g. turbo generator) as well as safety systems are monitored and controlled. If computer based display and control is used, there could be a backup system based on conventional control boards to operate and

monitor systems important to safety in case of loss of the computerised part. In same design there is also a 2nd control room in case the main control room is not accessible.

All these systems need to be powered by reliable electrical power supplies. Depending on the design of the I&C systems, the power supply could be: AC, or DC, or a combination of both. Recent experiences showed that this information could be partially or even totally lost by failure of their respective power supply. The loss of all annunciators in one channel/train may cause undesirable challenges for the operators during plant events/emergency conditions. According to the country, different norms and standards are used. A number of countries use IEEE standard or norms, others use requirements found in IEC standards.

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

- *Redundancy* – there must be several divisions available to cope with a single failure, depending on the standards, also preventive maintenance/test/ repair has to be considered in addition.
- *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 shall be separated from each other and independent.
- *Quality* – 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 like internal and external hazards. The ability to operate under such conditions has to be demonstrated by adequate qualification programmes.
- *Capability* – the power supplies to safety systems shall 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 essential features of the systems including the protection systems are maintained.

In general, the redundancy of an I&C power supply system is determined by the plant design criteria which apply to the I&C system.

Regulatory requirements

Regulatory guidance documents (e.g. Regulatory Guides in the United States, KTA in Germany, YVL in Finland, RCC-E in France, AERB in India) describe acceptable approaches to the design of safety related electrical power systems. Depending on the country and guidance in place, redundancy and diversity may be required for the most important power supplies like for I&C and control voltage. Some regulators require in addition an independent severe accident power supply

to mitigate and monitor severe accidents. In order to facilitate accident management critical information, there should be diverse power sources to provide uninterrupted information for the operators. If there is a backup control room, the power supply to this control room has to be independent from the one of the main control room to ensure that in case of internal hazard one control room remains available.

Plant contingencies

The so-called "combined" loss of onsite power supply can be defined as a loss of one or more division of safety classified UPS (with no backup via bypass) or DC power supplies. 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.

Existing and future designs

As for existing designs in most cases the electrical power supply system for display and control systems in the control room is not redundant (as divisional interconnections should be avoided). Each division has a separate safety classified electrical power supply (AC, DC, or both) and the loss of one division leads to losing the information supplied by this division. New designs provide for redundant (and even diverse) electrical power supplies. There are also diverse HMI systems to monitor and control the plant and their power supply architecture follows the design requirements of these systems. Redundant power supply may be achieved by having dual supplies decoupled via diodes (for DC supply) or using swing UPS (for AC supply) could be a solution. However, it has to be assured that failures may not propagate from division to another by applying proper protection and design measures.

2.9 Characteristics of high reliability onsite power supplies

For this discussion the on-site power supplies are plant systems that provide power to plant equipment. The system boundary is taken between the primary and secondary windings of the main plant supply transformers, e.g. auxiliary and start-up transformers. The main generator is not considered within this system.

The onsite power supply has two functions:

- To distribute power from the main generator or the transmission system to plant loads.
- To provide power from sources which are independent of the main generator and transmission system and to distribute it to the critical loads.

The onsite power systems are linked together thus an electrical event on a non-safety bus will in most cases also affect the safety power systems. A reliable onsite power system implies an installation with low possibility of failure of loads

and other equipment. The substantial part of this is covered by national electrical codes, but qualification of equipment (environmental and electrical) as well as equipment specifications based on design bases contribute.

Design bases

The design bases for the on-site electrical systems are the fundamental base for reliability and robustness. The bases set up of the required system capacity and capability and define the continuous operating range of voltage and frequency. Also the design bases define the hazards with which the electrical systems must cope. These must include all possible events that could cause transient including the associated dynamic or continuous variations in voltage and frequency, the internal hazards such as the effects of equipment failures or abnormal plant conditions, and external hazards such as natural phenomena and failure of nearby human built systems that can pose a threat. As a nuclear power plant is a generating facility, the voltage and frequency excursions that will arise from different events will be different from normal industrial events. Incomplete design bases, resulting in equipment not qualified for the intended function, cannot be solved by redundancy or diversity.

Architecture

The architecture of onsite electrical systems should implement the defence in depth strategy discussed in IAEA NS-R-1 and it should support the defence in depth strategy for the plant. The NS-R-1 defence in depth strategy consists of five levels.

The first level of defence in depth prevents abnormal operation and failure. At this level the on-site electrical supply acts as a single, highly interconnected system to supply power from the grid to all plant loads. Conservative design and high quality in construction and operation are applied to provide a robust and reliable power supply.

The second level of defence in depth detects failure and controls abnormal operation. At this level the on-site electrical supply continues to act as a single, highly connected system to supply power to all plant loads, except those that may present a hazard to the electrical power system itself (e.g. faults). The system also responds to abnormal operation by providing the capability to supply power from alternative offsite supplies such as alternative grid connections or the plant main generator if the plant is designed to accommodate house load operation. The ability to supply house loads from the main generator increases the reliability of the alternative supply, but it may also increase the vulnerability of the system to transient conditions created by interactions between the main generator and the grid.

The third, fourth, and fifth levels of defence in depth deal with accident conditions of increasing severity, but decreasing likelihood. At the different levels the priorities for what systems should receive power supply change, but the onsite electrical power supply will continue to operate normally unless the accident itself or independent failures cause loss of one or more power supplies. Therefore, at the third, fourth, and fifth levels the onsite system design is to ensure power supply to

the priority systems while dealing with increasingly severe failures of the electrical supplies.

The third level of defence in depth is the control of accidents within the design bases. The priority at this level is to power safety systems that ensure core cooling and containment functions. It is equally important to power systems that are necessary to support these functions. These support systems include, for example, equipment and room cooling, safety I&C, and the onsite power system itself. At this level it is advantageous that the design provide a path to feed safety systems directly from the auxiliary and start-up transformers so that any damage to non-safety distribution caused by the accident does not cause safety systems to lose connection to offsite power. At this level of defence in depth the electrical supply system must be able to cope with a loss of offsite power. In this case the safety portion of the system is separated from normal feeders and is supplied by on-site emergency generators. The onsite generators must have capability, capacity, and supply of consumables (e.g. fuel and grease oil) to continuously operate until offsite power sources can be restored. DC power systems support this capability. DC power systems may include uninterruptible power supplies for AC powered equipment that needs continuous supply. A better alternative for modern plants is to power all uninterruptible loads directly from the DC source, thus eliminating inverters as a failure point. Passive plant designs may be able to ensure critical safety functions without the need for significant amounts of AC power. In such plants emergency power may still be provided as discussed here to avoid challenging the passive systems and to avoid the economic consequences that might result from operation of passive safety systems.

The fourth level of defence in depth is to control severe accident progressions. At this level the priority is to provide power to any equipment that may be useful, regardless of safety classification. For this purpose the flexibility to establish beyond design power feed paths, and the ability to do so without damaging equipment is important. Also at this level it is necessary to cope with the loss of offsite power and emergency onsite AC supplies. This coping capability is usually provided by a combination of the plant design to fulfil critical safety functions for some period of time without significant supplies of AC power, batteries with the capacity to support these plant features, and alternative AC power sources that can be put into service during the time period for which the plant can survive without AC power.

The fifth level of defence in depth is the mitigation of radiological consequences of radioactive materials. Historically the systems allocated for this function are not dependent on the onsite electrical power supplies. The Fukushima experience, however, indicates a need to take a different view. It is necessary to provide power for cooling and containment safety functions even in the event of complete failure of the onsite electrical supplies. For this purpose there is a need for emergency supply equipment located in areas that will not be subject to the same hazards as the plant power supply. It must be possible to rapidly and reliably transport this equipment to the site when needed. It must also be possible to quickly connect these supplies to critical loads. To support this, the onsite supply needs to include predefined areas where temporary supplies and support facilities can be located, standardised

connections to critical equipment, feeders that bypass the normal onsite distribution systems, and reliable means to energise equipment via the alternate feeders.

Independence between levels of defence in depth

The independent effectiveness of each of the different levels of defence is a necessary element of defence in depth. Independence features must protect against several possible types of common causes such as: electrical faults, environmental conditions; failures of co-located equipment; and errors in design, operations, or maintenance. For all levels of defence in depth conservative design and high quality construction, operation, and maintenance provide a degree of independence from the effects of normal and abnormal environments and from errors in design and operation. Independence features between defence in depth level 1 and other levels focus on fault clearing and the proper co-ordination of electrical protective devices to limit the consequences of electrical faults. Protection co-ordination and a fault clearing should only disconnect the faulted equipment. If the primary protection or fault-clearing device fails, there should be adequate backup. Since battery chargers, inverters and motor generator sets have unique short-circuit features, special attention should be given to co-ordinating protective device sensitivity and systems with the expected fault current. Protection co-ordination must work properly both during power operation and during shut down conditions. Between levels 1 and 2 the possible dependences stemming from hazards with low occurrence probability are generally accepted.

Strong independence features are provided between the third level of defence in depth and other levels. The design, operation, and maintenance of systems and equipment supporting the third level receive closer scrutiny in order to further reduce dependencies that may be caused by errors in design and operation. Systems at this the level are physically separated from the systems at all other levels so that they cannot be influenced by the same plant environments or the same failures of co-located equipment. Components at this level are either protected from or qualified to survive the effects of all credible hazards, not just those with the highest probability of occurrence. Electrical isolation from the other systems is achieved using redundant protective and interruption devices that operate on diverse signals such as voltage, frequency, current, and accident signals rather than depending primarily on fault current alone. The inclusion of emergency generators and batteries at this level provides supply that is diverse from the offsite power.

At the fourth level of defence in depth an alternate source of AC power is provided that is physically separated from, and not normally connected, to the equipment to the rest of the onsite power system. If both the offsite and emergency AC power sources fail to operate, the alternate source can be started, and after integrity of the necessary distribution is confirmed, loads can be manually connected as needed. The fourth level depends also upon some portions of the distribution system and DC power systems remaining intact. Fault clearing in the distribution system is considered sufficient to ensure the continued operability of sufficient distribution capability. DC power supplies are considered to be simple and robust enough so that independent DC sources are not needed to ensure the capability to ride-through loss of AC power for the time needed to put the alternate

power source into service and to provide for switching necessary to connect the alternate AC power supply to loads.

At the fifth level of defence in depth the systems and equipment are by nature inherently diverse from those at the first four levels. This level includes environmental monitoring that is powered from distributions systems outside of the plant. Often these environmental monitors have their own back-up battery. The transportable systems for power supply will by their nature be inherently diverse from the other elements of the plant electrical supply and will be remotely located.

Independence between the different levels of the onsite electrical system is worthless unless the systems that support these different levels are themselves independent.

Under severe accident conditions it should be possible to supply power to any load from any compatible source and in particular it should be possible to charge any battery from any AC source.

2.10 Consideration of desired "fail safe" conditions

The final report on the lessons learned from the Forsmark event [1] included a section on the desirable fail safe conditions. It focuses on the concept of "fail safe" as a design principle that achieves defence in depth for electrical control systems primarily for nuclear safety. The level of analysis for ensuring the fail-safe condition varies as evidenced by the Forsmark event where defence in depth for nuclear safety systems was not considered as part of their design bases. Therefore, key lessons learned from the Forsmark event demonstrated the need to evaluate the failure modes of reactor protection systems and accident mitigations systems beyond consideration of the single failure by performing system level analysis with a combination of component level analysis to achieve robustness and reliability.

The Forsmark automatic depressurisation system logic was not designed with the possibility of losing more than one UPS. When two channels of power were lost the logic system demonstrated the undesirable failure modes of the logic system to open relief valves. Reference 1 looked into the logic deficiency and provides techniques to avoid undesirable failure modes in the reactor protection system and core cooling system. It illustrated the approach in diagrams that are based on two-out-of-three and two-out-of-four logic that demonstrate an acceptable approach to avoid undesirable failure modes in a reactor protection system and core cooling system. The design considers single failure and any degradation in motive force outside the operating band of any of the critical support systems to constitute a condition to trip a channel of the trip system and a combination of two such channels which lead to a trip of the reactor. The design also considers spurious reactor trip challenges from isolated instrument failures and malfunctions, it places importance on the validity of any trip condition when it verifies that the logic system whether two-out-of-three, two-out-of-four, or other combinations in order to validate the actual trip conditions. One of the precautions is to have the design logic designed with provisions that avoid common cause failures.

2.11 Challenges in evaluating FMEA and diversity of onsite power systems

Failure Modes and Effects Analysis (FMEA) is an important design and safety demonstration tool for both equipment designers and nuclear regulators. The DIDELSYS working group observed that current FMEA practice 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 international standards for electrical systems (such as: IEEE Std. 379) define a failure as "*The termination of the ability of an item to perform its required function",* and 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.

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

It is recommended to augment the tools available for comprehensively assessing the outcome of specific electrical faults by use of systems simulation tools such as (but not limited to) MATLAB for onsite power systems and SPICE-type computer codes 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.

2.12 Conflicts between protection and reliability

Safety related onsite electric systems provide an essential support system for numerous safety functions such as: reactor makeup, decay heat removal, containment cooling, and fission product removal etc. Except for some passive designs, 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 the protective logic in preventing major equipment failures so that essential safety features may be relied upon once a fault is cleared and power restored to the bus. The need for reliable automatic fault detection and breaker trip logic is thus obvious. What has not always been recognised in electrical system designs is the potential impacts when *uncertainties in set-points* vs. *uncertainties in operational ranges of equipment* begin to overlap.

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, inverter, or battery charger load. This problem requires

better simulation to determine design margins between possible operating ranges and uncertainties in set-points.

Role of standards in maintaining margins

Accepted electrical design standards (e.g. IEEE Std. 741 "Standard Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations") provide 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. 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 for overvoltage and voltage surges*.

The various OECD countries address this problem differently. In the United States, the US Nuclear Regulatory Commission 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 overvoltage protection should include coincidence logic on a per bus basis to preclude spurious trips of the offsite power source." 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.

2.13 Special considerations for digital protective relays

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. They present many advantages as replacement parts due to their versatility, the ease to adjust the settings and their capability to improve the protection of electrical components. Digital protective relays are less sensitive than electronic or electromechanical devices to environmental conditions.

However, they may introduce unanticipated features that were not present in the previous relay type and that could cause unexpected failures. They also introduce new types of failure that should be anticipated as much as possible. The use of analogue to digital converters as well as the algorithms used to work out the protective actuation can be source of problems. 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.

2.14 OECD member activities to address the implications of the Forsmark and Olkiluoto events

A survey was performed by the DIDELSYS group to collect information from the OECD member countries on the actions taken to address the issues identified by the Forsmark and Olkiluoto events. This survey covered the following areas:

- Voltage/frequency transients considered.
- Relationship with the grid operator.
- Problems related to the main generator.
- Problems related to the steam turbine.
- Problems related to the emergency diesel generator.
- Problems with the station blackout power supply.
- Problems with the uninterruptible power supply.

The main results of this survey [Reference 2] can be summarised as followed.

General

Most of the countries considered that the lessons learned from these events were relevant and applicable to their power plants. Some considered that it was not the case, mainly because of large differences in the design of electrical systems. In some cases, it was mentioned that previous improvements either during periodic safety assessments or due to other implementations of lessons learned made the electrical systems capable to withstand the scenarios encountered at Forsmark and Olkiluoto.

Voltage/frequency transients considered

Voltage transients were reconsidered in most of the countries. Typical transients were developed based on scenarios similar to what occurred at Forsmark. In some countries, very detailed studies were performed and resulted in the definition of most penalising voltage/frequency transients, with values as high as 160% Un/60 Hz with time dependent evolutions. The transition to house load operation, with additional failures of exciter/generator control and protections, was considered as the worst case design scenario for relatively slow voltage transients (as opposed to lightning voltage transients).

The capability of electrical components to withstand voltage transients was generally performed for rectifiers, inverters, transformers, motors, relays and cables. Potential effects of frequency transients were also checked in some cases.

Relationship with the grid operator

Depending to the previously existing situation, the relationship between the nuclear power plant licensee and the grid operator was either not changed (or

slightly improved) or reconsidered in depth. Transients from the grid are generally not considered as most penalising for nuclear safety and only a few countries mentioned that they required the grid operator to perform additional simulations of transients.

One country mentioned that there are regularly planned interactions between nuclear safety authorities and the grid regulator.

Main generator

In a few cases, the settings of the overvoltage protection were revised; most were checked to verify their reliability and ability to prevent unacceptable voltage transients. The overvoltage protection system was rarely modified, in one case because of already foreseen replacement for modernisation.

The house load capability, where provided by design, was generally not modified. Sometimes, settings were changed e.g. according to lessons learned from Olkiluoto and periodic testing was recommended.

Main turbine

Neither the over speed protection settings nor the over speed protection system were changed due to the Forsmark and Olkiluoto events.

Emergency diesel generator

Except in a few cases, no modification had to be done to the power supply of the auxiliary systems of the emergency diesel generators. Checks were performed to verify their black-start capability.

Station blackout power supply

In general, no modifications of the station blackout power supply were mentioned. Verifications were performed and, in one case, periodical testing was added.

Uninterruptible power supply

The overvoltage settings of the rectifiers were very often modified (and sometimes added) to provide for better protection of the inverters and to avoid switch off of the inverter. Actuation time delays were adapted to improve co-ordination. In the same way, overvoltage protection settings of the inverters (on the DC side) were either set at a higher value (possibly with time delay) or removed.

The main modification introduced in design specification of UPS was an overvoltage limiter system (“crow bar” or “transient killer”) to avoid DC overvoltage at the input of the inverter. Improved inverter capability qualification to withstand overvoltage was mentioned.

Power supply to signalling, indicators and recorders systems

The power supply to signalling systems and related items can be summarised in two different designs. The first one has safety related channels with multiple redundancies each of them being fed by independent safety related power supplies. These power supplies are provided by batteries (DC) or by UPS. The loss of these power supplies in a channel result in the loss of the information in that channel. The other one has, for each redundant safety related channels, redundant power supplies. A single failure of one of these power supplies does not lead to the loss of the information in the given channel. Some countries made changes in order to improve both the redundancy of these power supplies and their diversity (AC + DC supply). In case of DC, diodes are mentioned as separation devices to ensure the independency of power supplies.

3. Conclusions and recommendations

General recommendations

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*[1] 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[2] 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.

1. 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
2. *Électricité de France* (Edf) reviewed the Forsmark event and additionally decided to evaluate the consequences of a voltage regulator failure. VGB considered several simultaneous failures (e.g. excitation current control, overvoltage generator protection, and turbine speed control). The DIDELSYS working group did not have the ability to evaluate the probability or consequences of such events but agree it should be considered in individual plant hazard assessments if *the risks of such events are assessed to be significant*.

- 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.

Grid and in-plant challenges

- Nuclear power plant safety analysis must consider the expected frequency and duration 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.). Safety analysis should account for both possibilities. It should also be noted that a loss of grid event may occur following a period of degraded grid conditions (low voltage and/or low frequency).
- It is 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 Blackout gas turbine or diesel generator).
  - Emergency Diesel Generators.
  - All possible combinations of the above, within the specific NPP scheme.
- 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, need to be considered in safety analysis. Comprehensive analysis of possible transients in the power system, using verified models and methods, are strongly recommended if the risk of such events are assessed to be significant.
- The susceptibility of voltage and frequency transients and the acceptable voltage and frequency limits have to be assessed to confirm that Class 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.

Risks and benefits of capability to runback to house load operation

NPP's designed for house load operation have been subjected to overvoltage 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, the following issues have to be addressed:

- Existing and future schemes must be subject to comprehensive analysis using verified models and methods. The analysis must take into account the individual initial conditions and variations of each plant.
- House load operation capability should not be credited in safety analysis. Potential failures in the transition to house load operation should be considered, including the variation in initial process status and the possibility of several component malfunctions are very significant uncertainties.
- 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.
- 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 to be decreased and not to be impaired by the capability of house load operation.
- The house load capability is a desirable option for increasing the availability of the grid through rapid re-powering of the grid after plant isolation from grid. It is also an additional line of defence (an immediate source of electrical power to station auxiliaries). 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 might adversely affect all the redundant safety systems. The onsite electrical system should therefore be designed and 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 overvoltage 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 differ 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.
- In both cases (e.g. plants designed for house load operation or without house load operation) if equipment that has a direct influence on safety (such as: protection relays, control equipment for the turbine, the generator breaker, etc.) will be replaced with another type, or functional changes will be made, a test should be provided demonstrating that the equipment fulfils all necessary functions.

Communication interface between nuclear power plant and the electrical power grid

- 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 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 marketplace, review, periodic approval, and training of communication and interaction procedures between the grid operator and the NPP operator 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.

Power supply requirements for protection and control systems

The requirements for addressing defence in depth of electrical power supplies are currently not very explicit. There are certain high level requirements and industry

standards that address general requirements. The adequacy of design on reactor control system was 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-cause failures and consequences of common-cause failures were not adequately evaluated. The following recommendations are made:

- Consider revising IEEE Std. 308 and 765 and other suitable standards to indicate a rugged onsite electrical power system for nuclear power stations.
- Comprehensive regulation is necessary to prescribe the minimum defence in depth required for nuclear safety. As an example USNRC General Design Criteria 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 network or the loss of power from onsite electric power supplies."

Power supply requirements for nuclear power plant operator information systems

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 non-available power from the rectifier or by the bypass in case of failure of the inverter (assuming safety classified AC power is available). However, in some implementations the power supply via bypass is not safety classified or during diesel start there is an interruption in this power source. If there is a failure in the bypass switch, this would also lead to an interruption in the power supply. These observations mean that with a current UPS system alone a redundant power supply in one division may be not achieved.

The following is recommended:

- Investigate the design and operation of UPS in order to verify their robustness and eventually a need to provide for redundant (and diverse?) UPS inside each division.
- Operating experience with UPS should be investigated.
- In order to accommodate CCF and single failures, the design should have adequate diversity to provide uninterrupted display of all 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.

- Care should be taken regarding the power supply of the illumination of the control room to ensure appropriate conditions for the staff to perform their work in case of power system failures.

Characteristics of high reliability onsite power supplies

Conservative design, construction, and operation of electrical power systems, qualification for design-basis conditions, fault clearing and electrical protection co-ordination are critical to both the independence between levels of defence in depth and the reliability for the individual systems. In addition there are several reliability strategies that are applied at the level of these individual systems as discussed below.

- *Redundancy* – safety classified power systems are required to meet the single failure criterion. This criterion does not explicitly require that safety power systems be redundant, but in practice it nearly always results in redundancy. Redundancy is also applied to a more limited extent in the non-safety portion of the onsite electrical supply system. It is generally requested to supply offsite power via two independent power lines and to arrange distribution systems to provide separate paths by which any load centre can be supplied from either power line. Redundancy is generally not provided for alternate AC supplies, however, at multi-unit sites the ability to cross connect power between units may establish multiple sources of alternate AC supply.

- *Independence* – the reliability increase provided by redundant systems is strongly affected by the degree of independence between the redundant systems. For safety systems elaborate provisions for independence are provided including rigorous physical separation, electrical isolation, and protection and qualification for the worst envisioned consequences of internal and external hazards. Independence between non-safety systems is less rigorous, but redundant equipment is generally housed in different enclosures, equipment is protected from or qualified to withstand expected hazards, and cascading failures are limited by fault clearing and co-ordination of electrical protection.

- *Testing, monitoring, and corrective maintenance* – testing and effective facilities for corrective maintenance reduce equipment outage times, thus controlling one factor of unreliability. Where functions are implemented with redundant equipment the ability to rapidly detect and correct failures can reduce the probability of completely losing the function at sometime during the life of a plant to a few percentage points. All parts of the onsite electrical power supply are monitored during their operation. Functional testing is a normal part of the operational regime and very frequent testing is required for equipment in safety systems.

Consideration of desired "fail safe" conditions

- Random failures can be addressed with redundancy while common cause failures can be addressed with diversity. The DIDELSYS report [1] presents

design provisions that provide robustness against the possibility of random failures and thus provide information for prompt corrective action.

- The recommended actions presented in the DIDELSYS report [1] provide a comprehensive review of the current control systems for reactor trips and emergency core cooling systems. It also offers the need to further evaluate failure modes beyond consideration of the single failure to achieve defence in depth of electrical power systems and thus preserve nuclear safety.

Challenges in evaluating FMEA and diversity of onsite power systems

It is recommended that designers and regulatory authorities augment 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 under/above those precluded by existing over/overvoltage protection set-points.
- Degraded frequency on offsite/onsite AC power supplies above those precluded by existing protection set-points.
- Voltage surges on onsite AC power supplies below those physically limited by existing surge arrestors 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.

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

- The higher level standards and requirements for FMEA and single failure assessments appear appropriate – but the *lower level implementation guidance on scope of an acceptable FMEA and the types of faults to explicitly be considered needs revision.*
- The postulation of a wider range of scenarios involving overvoltage and overvoltage events needs to be considered and documented as a part of the single failure analysis in the design and safety analysis of the electrical power system, per the requirements of international standards. (Examples of such standards include: IEEE Std. 308, IEEE Std. 603, and IEEE Std. 379.)
- IEEE Std. 352 (an "informative document" which has not recently been updated) is limited in the types of faults suggested to be considered in a standard FMEA. It does not mention faults such as overvoltage and overvoltage events. Standards such as this need to be upgraded to incorporate operating experience.
- The evaluation and disposition of new postulated failure scenarios on installed electrical equipment would best be carried out using numerical simulation tools capable of evaluating the complex non-linear voltage and current relationships arising from overvoltage, overvoltage, over-frequency,

and under-frequency events. Such simulation tools would need to have appropriate verification and validation for their intended uses in nuclear safety analysis.

- Design standards (e.g. IEEE Std. 379) that allow excluding overvoltage and overvoltage events from the single failure analysis if and only if one can credit Design Qualification and Quality Assurance Programmes need to be more specific. The term Design Qualification is not well defined in standards for the specific types of voltage/frequency hazards identified from recent operating experience. The specific attributes of an acceptable Design Qualification programme to preclude the issues of voltage/frequency transients are not addressed in current international standards such as IEEE Std. 379, nor is reference made to another IEEE or IEC standard. This needs to be improved.

Conflicts between protection and reliability

Assuring appropriate design margins by properly simulating and analysing the potential ranges of equipment operation vs. protective logic operation, and use of redundant voltage protection logic both contribute to assuring high likelihood of providing required protection while minimising the possibility of spurious operation. In order to assure high probability of detection in time to prevent equipment damage:

- A systematic analysis of equipment voltage requirements should 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.

Special considerations for digital protective relays

- 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, in addition to include a verification of all applicable safety functions, should consider failure modes from all connected systems and actuated components.

References

[1] OECD/NEA (2009), "Defence in Depth of Electrical Systems and Grid Interaction, Final DIDELSYS Task Group Report", NEA/CSNI/R(2009)10, Paris.

[2] OECD/NEA (2012), Survey on "OECD Member Activities to Address the Implications of Forsmark-1 and Olkiluoto-1 Events", NEA/SEN/SIN/DIDELSYS(2012)1, Paris.

NEA PUBLICATIONS AND INFORMATION

The full **catalogue of publications** is available online at www.oecd-nea.org/pub.

In addition to basic information on the Agency and its work programme, the **NEA website** offers free downloads of hundreds of technical and policy-oriented reports.

An **NEA monthly electronic bulletin** is distributed free of charge to subscribers, providing updates of new results, events and publications. Sign up at www.oecd-nea.org/bulletin/.

Visit us on **Facebook** at www.facebook.com/OECDNuclearEnergyAgency or follow us on **Twitter** @OECD_NEA.

OECD/NEA PUBLISHING, 2 rue André-Pascal, 75775 PARIS CEDEX 16

CSNI Technical Opinion Papers No. 16

As all safety systems in the majority of existing nuclear power plants use the preferred power supply, any voltage surges in these systems could lead to common-cause failures. In the event of an unusual electrical system transient, it is essential that safety-related equipment be isolated or protected from the fault in order to ensure its ability to safely shut down the reactor and remove decay heat.

Based on the analysis of the voltage surges observed at Forsmark-1 in 2006 and Olkiluoto-1 in 2008, this technical opinion paper summarises the current state of knowledge of in-plant and external grid-related challenges to nuclear power plant safety-related electrical equipment. It will be of particular interest to nuclear safety regulators, nuclear power plant operators and grid system regulators and operators.

OECD Nuclear Energy Agency
12, boulevard des Îles
92130 Issy-les-Moulineaux, France
Tel.: +33 (0)1 45 24 10 15
nea@oecd-nea.org www.oecd-nea.org

NEA No. 7070