Date: 2014-02-03

IAEA SAFETY STANDARDS

for protecting people and the environment

Step 12: Review by the CSS

Design of Electrical Power Systems for Nuclear Power Plants

DS430

DRAFT SAFETY GUIDE

New Safety Guide

Supersedes NS-G-1.8

IAEA

International Atomic Energy Agency

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide is issued in support of the Specific Safety Requirements publication on Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 [1], which establishes design requirements for nuclear power plants.

1.2. This Safety Guide provides recommendations on the necessary characteristics of electrical power systems for nuclear power plants, and of the processes for developing these systems, in order to meet the safety requirements of SSR-2/1 [1]. It reflects revisions that have been made to Ref. [1] and in particular to Requirement 68.

1.3. This publication is a revision of a Safety Guide issued in 2004 as Safety Standards Series No. NS-G-1.8 [1], and supersedes it. This revision takes into account developments in the design of emergency power systems for nuclear power plants and expands the scope to include all electrical power systems that provide power to systems important to safety (see Figs 1 and 2).

1.4. Safety Standards Series No.NS-G-1.8 also included guidance on non-electrical power systems that provided emergency power. Guidance for such systems will be provided in a new Safety Guide on auxiliary systems[2].

1.5. Electrical power systems that supply power to systems important to safety are essential to the safety of nuclear power plants. These electrical power systems include both on-site and off-site power supply systems. The on-site systems and the off-site systems work together to provide necessary power in all plant conditions so that the plant can be maintained in a safe state. Off-site power systems are not plant equipment. They are, nevertheless, essential to the safety of a nuclear power plant and they are important in the defence in depth concept.

1.6. The preferred power supply identified in this Safety Guide is the power supply from the transmission system, or from the main generator up to the safety classified electrical power system. This power supply is composed of the transmission system, the switchyard, the main generator and the distribution system up to the safety classified electrical power system. The parts of the preferred power supply that are part of the off-site power system (e.g. the transmission system) are not plant equipment and are therefore not part of the safety classification for the plant (see Fig. 2). The location of the boundary between the off-site power supplies and the on-site power supplies will be a plant specific decision.

---

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Emergency Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.8, IAEA, Vienna (2004).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Auxiliary Systems and Supporting Systems for Nuclear Power Plants, IAEA Safety Standards Series, IAEA, Vienna (in preparation).

1.7. It might not be practicable to apply all the recommendations of this Safety Guide to nuclear power plants that are already in operation or under construction. For the safety analysis of such designs, it is expected that a comparison will be made with current standards, for example as part of the periodic safety review for the plant, to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements.

OBJECTIVE

1.8. The objective of this Safety Guide is to provide recommendations and guidance on meeting the requirements for the design of electrical power systems established in Requirements 41 and 68, paras 6.43–6.45, and in the general requirements of Sections 2–5 of SSR-2/1 [1]. It is intended for the use by all those, including designers, reviewers, safety assessors, regulatory bodies, operating organizations and operators, involved in the design, operation, maintenance, modification, assessment and licensing of nuclear power plants. The Safety Guide does not provide guidance on details of implementation processes, methods to be used, or technology, except by way of explanation.

SCOPE

1.9. This Safety Guide makes recommendations and provides guidance on the provisions for electrical power systems that are necessary for both new and operating nuclear power plants. It applies to all electrical power systems important to safety in nuclear power plants and to the preferred power supply.

1.10. The Safety Guide applies to nuclear power plants of all types. The extent of the electrical power systems important to safety and of safety power systems, as given by classification of the electrical power systems, differs between different designs. The minimum recommended design requirements for electrical power systems necessary at different voltage levels for maintaining defence in depth and diversity are outlined in this Safety Guide. In all cases, this Safety Guide should be used together with the plant's safety analysis report in order to determine the safety significance and importance of different power supplies. For example, in plants with passive engineered safety features, the classification of the electrical power systems may be substantially different from that shown in Fig. 2.

1.11. Additional recommendations applicable to electronic devices used in the control and protection of the plant's electrical power systems are provided in Ref. [2].

1.12. Figures 1, 2 and 3 show examples of the electrical power systems of nuclear power plants to illustrate the scope of this Safety Guide and terminology used. Further explanation is provided in the list of definitions.

1.13. This Safety Guide is focused on electrical power systems. Guidance on the specification of loads is outside its scope, but it is necessary that such specifications are in accordance with the design guidelines for electrical power systems.

1.14. Electrical power for security systems (e.g. fences, surveillance systems, entrance access control) is outside the scope of this Safety Guide.

1.15. This Safety Guide should be used in conjunction with the other relevant safety standards in the IAEA Safety Standards Series.

1.16. Additional guidance on the design and development of electrical power systems and electrical equipment is available from States and from other organizations that establish standards. Such publications give much greater detail than is appropriate for IAEA safety standards. It is expected that this Safety Guide will be used in conjunction with detailed industrial standards.

1.17 While designing electrical power systems, potential interfaces between nuclear security and safety should be analysed and managed. Reference [3] gives guidance on security for nuclear facilities.

STRUCTURE

1.18. Section 2 introduces the main systems of a typical electrical power system for a nuclear power plant and recommends the fundamental goals to be met by each system.

1.19. Section 3 covers the application of safety classification to electrical power systems.

1.20. Section 4 outlines the content to be included in the design bases for electrical power systems.

1.21. Section 5 provides general recommendations that apply for all alternating current (AC) and direct current (DC) electrical power systems. These recommendations are the minimum recommendations for systems that are not covered in Sections 6–9. For systems that are covered in Sections 6–9, the recommendations of Section 5 should be used in conjunction with the specific recommendations.

1.22. Section 6 provides recommendations for the preferred power supplies. These are the normal supplies for all plant systems important to safety and are, if available, always the first and best choice of all plant power supplies.

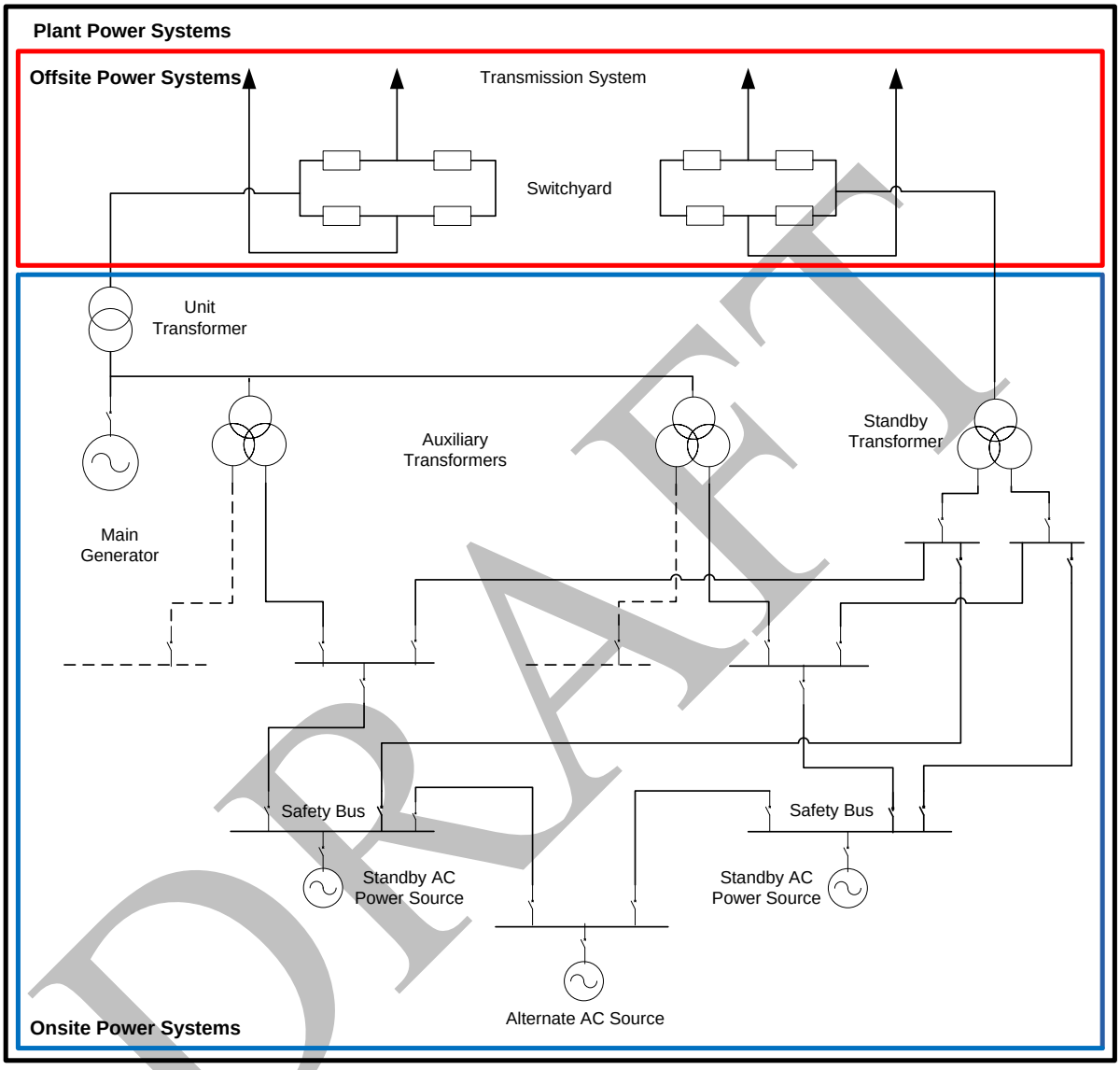
1.23. Section 7 provides recommendations that are specific to the design of safety power systems, including standby safety power supplies.

1.24. Section 8 provides recommendations that are specific to the design of alternate AC (AAC) power supplies. This supplements the guidance of Section 5 for these systems. Alternate AC power supplies are often provided to protect against the simultaneous failure of off-site AC power supplies and emergency on-site AC power supplies.

1.25. Section 9 provides recommendations for activities to confirm the adequacy of the design of electrical power system and the system level documentation that should be provided both to support the safety case for the plant and to support operations, maintenance, testing and verification.

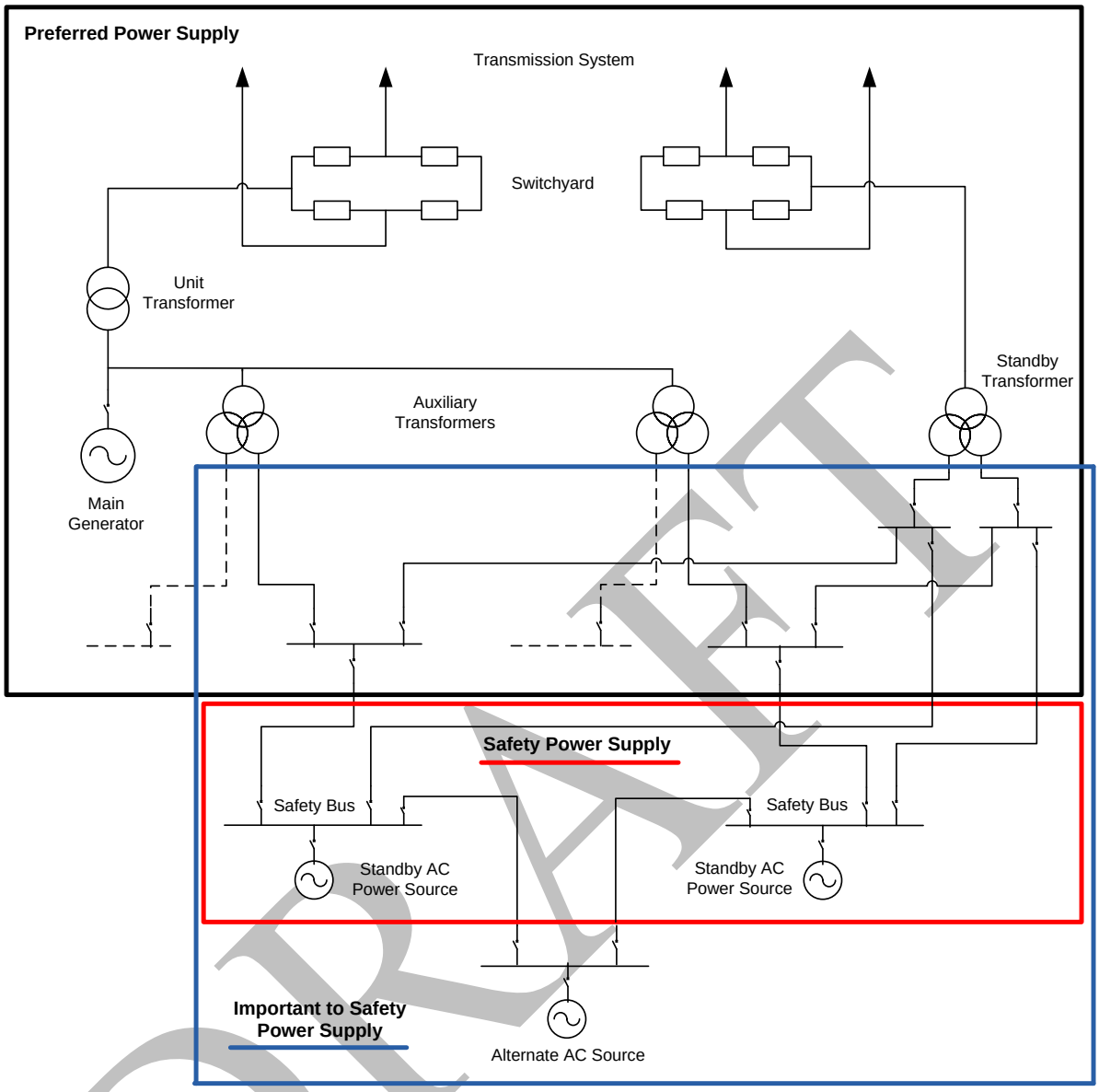
1.26. Annex I discusses the relationship between the design of electrical power systems and the concept of defence in depth as described in SSR-2/1 [1].

1.27. Annex II provides an example of analyses of electrical power systems for verification of the design of the nuclear power plant.



Note: This figure provides only an example. Various possible arrangements of buses, loads, generators and interconnections would meet the requirements of Ref. [1]. Furthermore, many elements of the plant system, such as buses that are not important to safety and DC power systems, are not shown. Dotted lines indicate not important to safety power supply.

FIG. 1. Relationship of the plant electrical power system, the off-site electrical power system and the on-site electrical power system for a nuclear power plant.



Note: This figure provides only an example. Various possible arrangements of buses, loads, generators and interconnections would meet the requirements of Ref. [1]. Furthermore, many elements of the plant system, such as buses that are not important to safety and DC power systems, are not shown.
This figure is intended only to represent the relationship between the elements of the plant power systems that are within the safety classification and the preferred power supply.
The elements of the preferred power supply that are not within the bounds of the important to safety power supply are outside of the scope of the plant safety classification.
The system elements included in the important to safety power supplies will differ according to plant design and the classification methods applied in different States.
Some plant designs may not require safety standby power sources. All nuclear power plants are expected to have safety DC power supplies.
Dotted lines indicate not important to safety power supply.

FIG. 2. Relationship of electrical power supplies important to safety, safety power supplies, and the preferred power supply for a nuclear power plant.

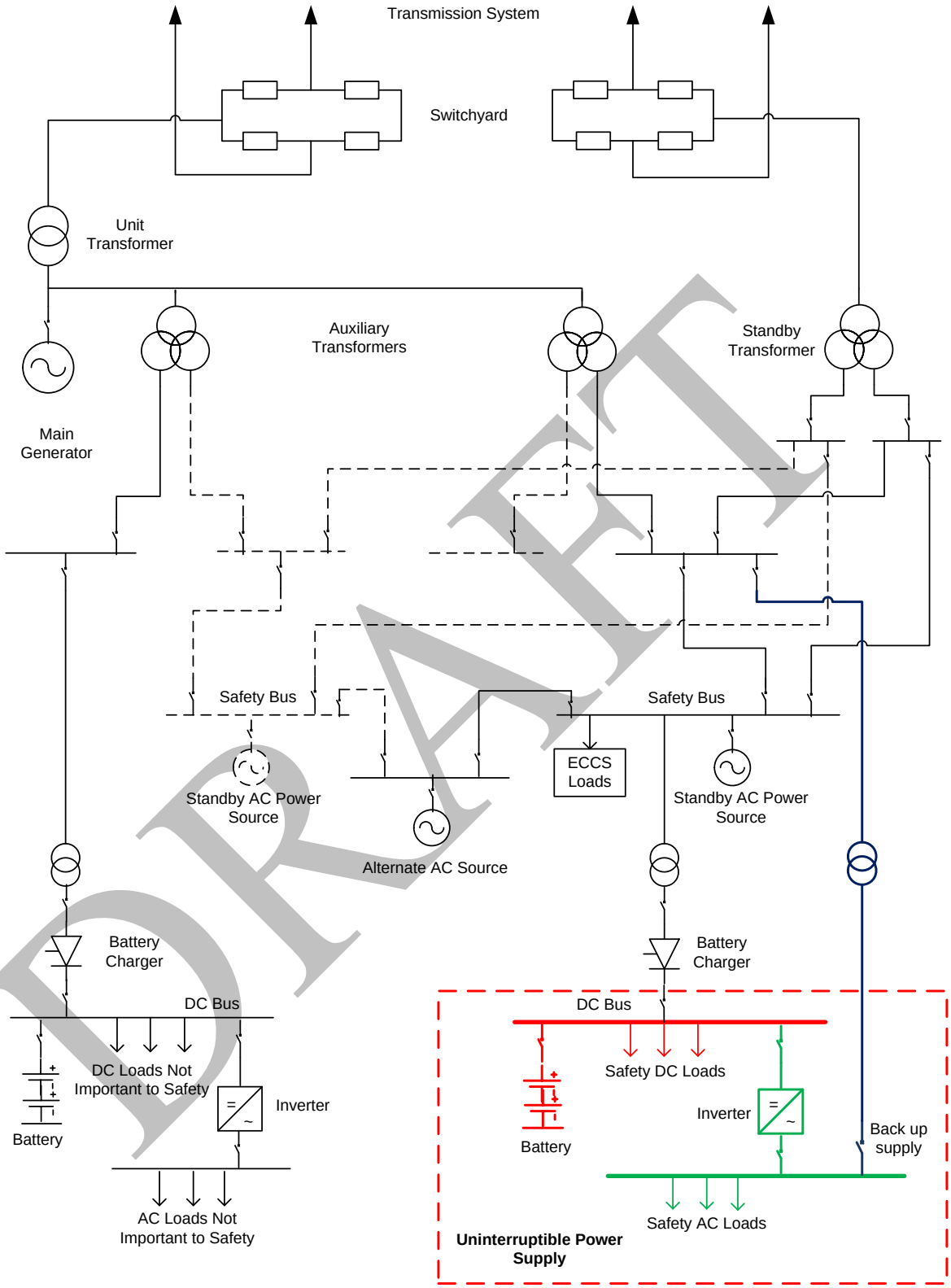


FIG. 3. Schematic representation of the different parts of the electrical power supplies for a nuclear power plant, as discussed in this Safety Guide, with their boundaries. (Typical for one train.)

2. ELECTRICAL POWER SYSTEMS AT NUCLEAR POWER PLANTS

DESCRIPTION OF THE ELECTRICAL POWER SYSTEM AT A NUCLEAR POWER PLANT

2.1. Figures 1, 2, and 3 show examples of the outline of the electrical power system for a nuclear power plant. The design of the electrical power system for a specific plant will depend upon the grid, on the design of plant systems and on decisions on engineering design that are beyond the scope of this Safety Guide., Figures 1, 2 and 3 are therefore not to be taken as a recommended design for any specific nuclear power plant.

2.2. The safety power system can be supplied by either the preferred power supplies or the standby power sources. Alternate AC power supplies can also supply the safety power systems in design extension conditions.

2.3. This Safety Guide discusses three major subsystems of the plant power system: the on-site power system, the off-site power system and the preferred power system. The following paragraphs explain these terms as they are used in this Safety Guide. The use of these terms elsewhere will depend on details of the plant design and may differ from their use in this Safety Guide.

Off-site power system

2.4. The off-site power system is composed of the transmission system (grid) and switchyard connecting the plant with the grid. The off-site power system will normally provide AC power to the plant in all modes of operation and in all plant states. It also provides transmission lines for outgoing power (see Fig. 1.) The boundary between on-site and off-site power systems is at the point where the items controlled by the transmission system operator connect to equipment controlled by the nuclear power plant operator. The boundary is generally at the bushings on the grid side of the transformer that connects to the transmission voltage, or on the grid side of the high voltage circuit breaker closest to the plant.

2.5. The off-site power system performs an essential role in terms of safety in supplying the on-site power systems with reliable power from multiple power sources: (1) main generator via auxiliary transformers; (2) grid power supply via the standby transformer. The off-site power system is part of the preferred power supply (see Fig. 2).

2.6. An inherently robust grid system provides a highly reliable off-site power supply as it rapidly dampens the effects of grid perturbations in normal conditions and minimizes the deviations in voltage and frequency in the connected electrical power system of the nuclear power plant. Similarly, large nuclear units with a fast turbine governor and generator excitation systems can impart considerable robustness to a grid system. Because of this interdependence, good functional integration by design and good operational co-ordination between the grid and nuclear power plant operators during major

operating changes either on the grid or at the nuclear power plant are important requirements for the safe and reliable operation of both the grid and the plant.

On-site power system

2.7. The on-site power system (see Fig. 1) is composed of distribution systems and power supplies within the plant. It includes the AC and DC power supplies necessary to bring the plant to a controlled state following anticipated operational occurrences or accident conditions and to maintain it in a controlled state, or a safe state, until off-site power supplies can be restored. Stand-alone power supplies, such as separate power supplies for security systems, are not included. The on-site power systems are separated according to their safety significance: systems important to safety (safety systems, safety related systems) and systems not important to safety (see Fig. 2).

2.8. The major components of the on-site power system include the main generator, generator step-up transformer, auxiliary transformer, standby transformer and distribution system feeding unit auxiliaries, service auxiliaries, switchgear, batteries, rectifiers, inverters and/or uninterruptible power supplies, cables and standby AC power sources. Parts of the on-site power system are part of the preferred power supply.

2.9. The on-site electrical power systems are generally divided into three types of electrical power systems in accordance with the different power requirements of the loads:

- An AC power system. The functions of the assigned AC loads will tolerate a certain interruption in the power supply. Usually the AC power system includes a standby AC power source and an alternate AC power source. Protective relays detect loss of the preferred AC power supply to the electrical power systems and automatically start a standby electrical power supply. In most cases it is assumed in the plant safety analyses that the standby AC power source will be used for plant shutdown following design basis accidents, and the alternate AC source for design extension conditions.
- A DC power system. This supplies DC loads, without interruption, from batteries. The DC system includes battery chargers that are connected to the AC system of the electrical power systems. Separate DC power systems are sometimes provided to support loads of different safety classification.
- An uninterruptible AC power system (UPS). This supplies power from inverters or motor generator sets that are in turn supplied from a DC source such as the DC power system or dedicated batteries with rectifiers, and includes a bypass circuit to allow feeding of safety loads directly from safety class AC power systems for maintenance and emergency cases.

Preferred power supply

2.10. The preferred power supplies are the normal supplies for all plant systems important to safety. They are, if available, always the first and best choice of power supply to the electrical safety power systems. The preferred power supply includes parts of both the on-site and off-site systems (see Fig. 2).

ROLE OF CODES AND STANDARDS

2.11. SSR-2/1 Requirement 9 [1] states that:

> "Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards."

2.12. The off-site power system should satisfy the nuclear safety criteria established in national and international standards, the grid code and electrical design criteria (as stipulated by national electrical codes).

2.13. The plant electrical power system should be designed and constructed in accordance with national and international nuclear standards and national safety codes to ensure a high level of reliability and availability in all modes of plant operation.

2.14. National safety codes provide guidance on acceptable design requirements for safe and reliable operation of electrical power systems. Compliance with these safety codes generally provides reasonable assurance for the capability of electrical power systems in the nuclear power plant.

DESIGN CONSIDERATIONS IMPOSED BY REQUIREMENTS FOR NUCLEAR SAFETY

2.15. The electrical power systems and components at a nuclear power plant supply electrical power to the plant's auxiliary systems from off-site and on-site power supplies.

2.16. The off-site power and off-site system for a nuclear power plant should be robust and should be highly reliable in all plant states and operating conditions. The design of the on-site power system should take into consideration the limitations of capability of the off-site power system and its impact on nuclear safety.

2.17. A stable and reliable grid (with reliable production units, transmission systems and distribution systems) is fundamental to the safety of the nuclear power plant.

2.18. Grid disturbances can challenge safety when the nuclear power plant acts as a:

- Production unit
- Consumer during startup and shutdown or
- High priority emergency load during certain events and operational occurrences.

2.19. Robust systems should have: sufficient margins and built in conservatisms such that equipment ratings, capabilities and capacities that are required to meet intended goals are not easily challenged; equipment protection set points that are chosen to accommodate anticipated variations in the operation of on-site and off-site power systems; the ability to support emergency operations involving sustained overload conditions or overvoltage conditions and protective actions that are initiated when necessary to preserve the functionality of the safety power systems.

2.20. The electrical power systems, at all voltage levels, are support systems for most of the items of plant equipment. A reliable power supply is critical for maintaining control during anticipated deviations from normal operation, as well as to power, control and monitor relevant plant safety functions in design basis accidents and design extension conditions.

2.21. During shutdown, parts of the power supply systems of the nuclear power plant may be out of service for testing or maintenance. The challenges to the robustness, reliability and availability of the electrical power system when the plant is shut down will differ from those that have to be addressed during operation at power.

2.22. SSR-2/1 Requirement 4 and para. 4.1 states that:

> "Fulfilment of the following fundamental safety functions shall be ensured for all plant states: (i) control of reactivity; (ii) removal of heat from the reactor and from the fuel store; and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.
>
> "A systematic approach shall be taken to identifying those items important to safety that are necessary to fulfil the fundamental safety functions, and to identifying the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions for all plant states."

2.23. A systematic approach should be followed to identify the structures, systems and components for electrical power that are necessary so that items that are essential to fulfilling the fundamental safety functions can be powered from electrical supplies of the appropriate safety classification and reliability.

2.24. 'Reliability' means that proper implementation of the design, testing, operation and maintenance provide assurance that electrical power systems can perform their mission with a minimum of disturbances.

2.25. A number of measures can be taken on and off the site to achieve the required reliability of the electrical power supplies. Such measures may involve increasing the reliability of the plant's normal power supply (the preferred power supply) or providing other sources of power to the electrical power systems when the normal power supply might not be available. This may also include the use of dedicated power sources for safety systems of special importance.

2.26. Elements in a defence against common cause failure are a good understanding of events that could challenge the electrical power systems and a robust defence against these challenges, clearly defined design bases that are regularly confirmed and a suitable diversity of the power supplies.

2.27. The interface between the safety systems and systems of lower safety classification should be carefully designed to ensure that there is no adverse impact on safety equipment from non-safety-related equipment as a result of disturbances in the plant electrical power systems.

DESIGN CONSIDERATIONS IMPOSED BY CRITERIA FOR ELECTRICAL DESIGN

2.28. SSR-2/1 Requirement 41 states that:

> "The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply."

2.29. Transient and quasi-stationary variations of voltage and frequency that could affect the electrical power systems and components of the nuclear power plant should be considered in the design.

2.30. The protection scheme for the plant and the design of the plant's components should be such that disturbances in the preferred power supply do not jeopardize the required operation of safety power systems and connected loads.

2.31. In an emergency action, equipment protection may be reduced to the essential set in order to give priority to the safety action.

A nuclear power plant as a power generating facility connected to the grid

2.32. In accordance with national legislation, national grid codes or bilateral agreements between each transmission system operator and each power generating facility, a power generating facility should be designed in such a way that it supports highly reliable operation of the grid system.

2.33. High reliability of the grid is essential for a safe and reliable electrical power supply in a nuclear power plant. The transmission system operator has the responsibility of ensuring that there is a reliable electrical power supply to the nuclear power plant as well as the responsibility for transmitting its power to the electrical distribution operators.

2.34. The specific features and design requirements of nuclear power plants should be recognized in grid codes.

Personnel and equipment safety

2.35. Electrical power systems should be designed to minimize risks to personnel and to minimize damage to equipment due to high temperatures, arc flash or mechanical stress caused by rated current, overcurrent or any internal mechanical stresses on the equipment.

2.36. Electrical power systems should be designed and constructed in such a way that they could withstand voltages that could be expected to occur in any plant state or operating mode.

3. CLASSIFICATION OF ELECTRICAL POWER SYSTEMS

3.1. SSR 2/1 Requirements 18 states that:

> "The engineering design rules for items important to safety at a nuclear facility shall be specified and shall comply with the relevant national or international codes and standards and with proven engineering practices, with due account taken of their relevance to nuclear power technology."

3.2. SSR 2/1 Requirement 22 states that:

> "All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance."

3.3. SSR 2/1 para. 5.34 states that:

> "The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:
>
> (a) The safety function(s) to be performed by the item;
>
> (b) The consequences of failure to perform a safety function;
>
> (c) The frequency with which the item will be called upon to perform a safety function;
>
> (d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function."

3.4. SSR 2/1 para. 5.36 states that:

> "Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment."

3.5. A Safety Guide on safety classification of structures, systems and components in nuclear power plants [4] provides recommendations and guidance on how to meet the requirements established in Refs [1] and [4] for the identification of structures, systems and components important to safety and for their classification on the basis of their function and safety significance.

3.6. The safety classification process recommended in Ref. [4] is consistent with the concept of defence in depth as set out in Ref. [1]. The functions performed at the different levels of defence in depth are considered.

3.7. For a specific nuclear power plant, the classification process should primarily cover:

– The design basis of the plant and its inherent safety features;

– The list of all postulated initiating events, as required in Ref. [1], Requirement 16. The frequency of occurrence of the postulated initiating events, as considered in the design basis for the plant, should be taken into account.

3.8. The possibility that the failure or the spurious operation of an item important to safety may directly cause a postulated initiating event or make the consequences of a postulated initiating event worse should be considered when the list of postulated initiating event is established.

3.9. All electrical power system functions and design provisions necessary to achieve the main safety functions, as defined in Ref. [1], Requirement 4, for the different plant states, including all modes of normal operation, should be identified.

3.10. The electrical power system functions should then be categorized on the basis of their safety significance, with account taken of the following three factors:

(1) The consequences of failure to perform the function;

(2) The frequency of occurrence of the postulated initiating event for which the function would be called upon;

(3) The time following a postulated initiating event at which, or the period of time during which, the function will be required to be performed.

3.11. The electrical power systems and components performing each function assigned in a safety category should be identified and classified. They should primarily be classified according to the category assigned to the function that they perform.

3.12. Off-site power systems and main generator systems also have an essential role in ensuring the performance of fundamental safety functions, but these systems are not classified according to the safety classification for the plant.

3.13. When assigning the safety classification, the timeliness and reliability with which alternative actions could be taken and the timeliness and reliability with which any failure in the electrical power system could be detected and remedied should be considered.

3.14. In the Safety Guide on classification of structures, systems and components in nuclear power plants [4], three safety categories for functions and three safety classes for structures, systems and components are recommended, on the basis of experience of States. However, a larger or smaller number of categories and classes may be used if desired.

4. DESIGN BASES FOR ELECTRICAL POWER SYSTEMS

4.1. SSR-2/1 Requirement 14 and para. 5.3 states that:

> “The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant plant operational states, for accident

conditions and for conditions generated by internal and external hazards, to meet the specified acceptance criteria over the lifetime of the nuclear power plant.

"The design basis for each item important to safety shall be systematically justified and documented. The documentation shall provide the necessary information for the operating organization to operate the plant safely."

4.2. SSR-2/1 Requirements 15–19 [1] elaborate on specific topics to be considered in the development of system design bases.

4.3. The design basis should be specified for each electrical power system in the nuclear power plant.

4.4. The design bases should specify the required functional tasks, the necessary characteristics, the performance objectives, the operating conditions and environmental conditions, and the necessary reliability.

4.5. For each electrical power supply system in the plant, the voltage range and the frequency range for the continuous operation of connected loads should be defined.

4.6. The permissible transient and quasi-stationary voltage range and frequency range for the continuous operation of connected loads should be defined for each electrical power supply system in the plant.

4.7. Transients that should be considered include the internal events and external events, including grid events, that are described in para. 5.4.

4.8. The design bases should cover all modes of operation and should take into account all possible events that could impact the electrical power systems in the nuclear power plant, including:

(a) Symmetrical and asymmetrical faults;

(b) Sub-synchronous resonance phenomena;

(c) Large motor starts;

(d) Momentary perturbations in the grid system such as switching surges or lightning strikes;

(e) Capacitor bank switching;

(f) Loss of transmission system elements, including single phase open conditions;

(g) Formation of grid islands and resulting frequency excursions and voltage excursions.

4.9. The design bases should be confirmed when major replacements and major modifications of the electrical power system (on-site or off-site) as well as changes in loading are made and a cumulative evaluation is performed periodically, e.g. as part of periodic safety reviews.

4.10. The design basis should describe for each subsystem of the plant power systems:

(a) The plant operational states in which the system is required:

These include plant operation from startup to maximum licensed power with maximum auxiliary loading, plant shutdown from full power, and safe shutdown following a reactor trip and a design basis accident.

(b) Voltage range and frequency range for continuous operation:

These ranges define the operating requirements for equipment such as motors, pumps, inverters, battery chargers and valve actuators.

(c) Capacity requirements:

The equipment credited in the accident analyses normally defines capacity. Capacity, in terms of electrical equipment, includes for instance simultaneous start or reacceleration of components.

(d) Steady state, short term operation and transient conditions to which the systems might be subjected when they are required to perform:

Steady state conditions include, for example:

- Voltage ranges and frequency variation for heavy load and light load conditions, for all plant states, and for house load operation where applicable;
- Deviating grid voltage or grid frequency;
- Float voltage and charging voltage for DC systems.

Transient conditions include, for example:

- Switching surges;
- Lightning surges;
- Voltage interruptions caused by electrical faults on and off the site;
- Voltage sags and swells in conjunction with loss of load, motor starts, and clearing of faults on the on-site electrical power system or the off-site grid;
- Variations and transients in voltage and frequency when the grid (and main generator) are affected by faults;
- Harmonics due to switching surges or rotating equipment;
- Faults in the transmission system or the on-site power system (all voltage levels) cleared by first step protection or backup protection;
- Events involving loss of synchronization between the plant and the grid;
- Fault or open condition in a single phase;
- Malfunctions of the main generator excitation system (high and low excitation);

- Open conductors;
- Solar activity and geomagnetically induced currents.

(e) Variables to be monitored, such as the system voltage, the system current and the frequency, of the main bus bars:

This includes variables necessary for monitoring in and following an accident.

(f) Actuation conditions for operating standby electrical power supply:

This includes variables that are used to initiate required actions.

(g) Environmental and electromagnetic conditions to which components and cables will be subjected:

Environmental conditions include:

- Normal conditions;
- Abnormal conditions;
- Accident conditions;
- Conditions deriving from natural phenomena.

(h) Identification of all loads indicating safety classification and electrical characteristics:

This includes motor input power at run-out when applicable.

(i) Required performance characteristics of all components;

(j) Requirements for maintenance and testing:

This includes test acceptance criteria.

(k) Protection schemes and coordination of protection:

Protection schemes are to consider both symmetrical and asymmetrical faults. Refer to Annex II for details.

(l) Design acceptance criteria:

Design acceptance criteria include, for example:

- Standards to be used or considered;
- Requirements for design characteristics (e.g. independence characteristics, compliance with single failure criteria and diversity requirements).

(m) Reliability and availability goals for systems and key components:

For example, the reliability of the standby power supplies.

Reliability and unavailability limits for systems and components may be specified by using probabilistic criteria, deterministic criteria (e.g. compliance with the single failure criterion), or both.

(n) Voltage, speed, time to start and load, and other limits applicable to standby power supplies and their prime movers.

(o) The maximum time for standby power supplies to start and to accept loading in a specified load sequence:

The equipment credited in the accident analyses normally defines permissible starting time.

(p) The required performance characteristics of standby power supplies, including the capability for no load, light load, rated load and starting load as well as, in certain States, overload operation for the required time periods.

(q) The capability for step loading of the standby power supplies over the entire load range:

The step load capability specifies the conditions of voltage and frequency that the standby power supply has to maintain in order not to degrade the performance of any load below its minimum requirements, even during excursions caused by the addition or removal of the largest load.

(r) Conditions to be permitted to shut down or disconnect safety power sources:

This includes, for example, the need to protect equipment from catastrophic failures.

(s) The minimum time for which on-site power has to be capable of operating independently of off-site power and without replenishing consumable items from off-site:

This will be considered, for example, in setting the required capacity of batteries, emergency generator fuel and lubricating oil in storage, and the required storage of other consumables such as air filters.

(t) The variables, or combination of variables, to be monitored;

(u) The control functions required, and identification of whether actions are to be performed automatically, manually or both, together with the locations for the controls.

5. GENERAL DESIGN GUIDELINES FOR ELECTRICAL POWER SYSTEMS

GENERAL

5.1. Electrical power systems important to safety should fully implement the requirements of their design bases.

Anticipated electrical events

5.2. The electrical power systems of the nuclear power plant should meet all functional requirements under the steady state conditions, short term operation conditions and transient conditions defined in the design basis.

5.3. Electrical and internal events can cause symmetrical and asymmetrical perturbations in the plant. These events can be initiated:

- In the transmission system with the plant on line, off line or shut down, or as a consequence of the plant separating from the grid owing to anticipated faults or voltage variations and frequency variations beyond an acceptable level;
- By tripping of the main generator, leaving the on-site power systems connected to the off-site power systems or to other on-site power systems;
- In the on-site power systems, as a result of an electrical event such as a motor starting, a phase to ground fault or switching surges.

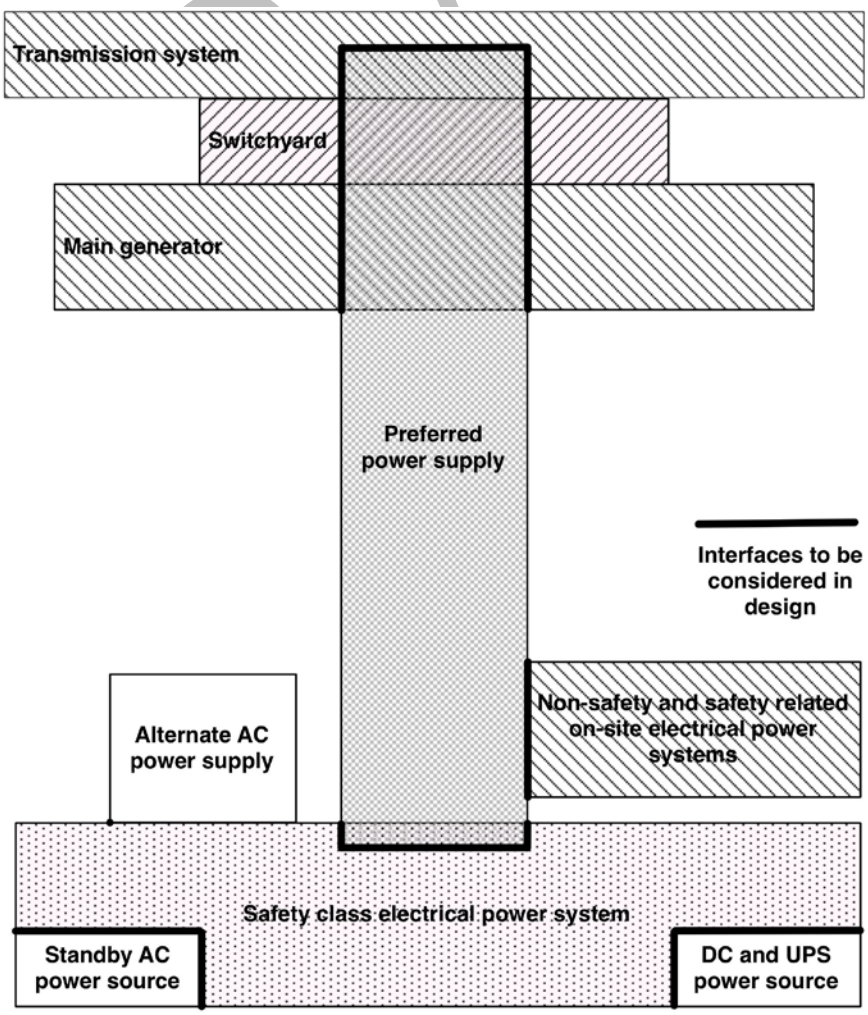


FIG. 4. Relationship between the preferred power supply and other elements of the electrical power system. UPS: Uninterruptible power supply.

5.4. The impact of such events on all the on-site electrical power systems (AC and DC) (see Fig. 4) should be evaluated and it should be confirmed by specific analysis that the requirements for the allowable voltage and frequency are met and the protection system is adequate.

5.5. The analyses of system stability for grid transients should demonstrate that the plant could ride through and could remain connected to the grid for perturbations that do not result in the generator losing synchronization with the transmission system voltage (see Fig. 5).

5.6. The electrical fault clearing time should be defined by the grid operator.

5.7. This desired defence in depth capability supports the preferred power supply operation.

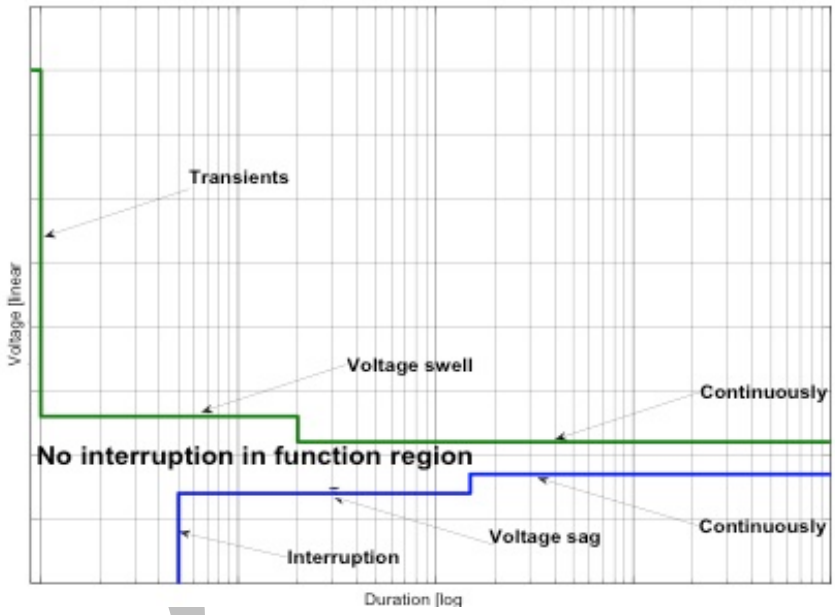


FIG. 5. Voltage swell and sag (note that initial conditions could be anywhere within the continuous band).

Station blackout

5.8. International operational experience has shown that loss of the preferred power supply concurrent with a turbine trip and unavailability of the emergency AC power system is a credible event. Such an event may affect a single unit, and even all units on one site. Such an event is called and its frequency of occurrence should be low enough to be considered and analysed as a design extension condition (DEC) event. The term does not include the simultaneous failure of uninterruptible AC power supplies or DC power sources, or the failure of alternate AC power sources that are diverse in design and not susceptible to the events that caused the loss of on-site and off-site power sources.

5.9. The plant's capability to maintain safety functions and to remove decay heat from spent fuel should be analysed for the period for which the plant is in station blackout condition. Adequate provisions should be included in the design to prevent any significant fuel damage for the period during which the plant is in a station blackout condition.

5.10. Several design measures are possible as a means of increasing the capability of the electrical power systems to cope with a station blackout. These measures include, for example, increasing the capacity of batteries to supply power to safety instrumentation and control equipment, and to other vital equipment; use of unit to unit connections; or installing an alternate AC power source that is diverse in design and is protected from hazards that could degrade the normal power sources and standby power sources.

DESIGN FOR RELIABILITY

General

5.11. SSR-2/1 Requirement 23 states that:

> "The reliability of items important to safety shall be commensurate with their safety significance."

5.12. In the design of electrical power systems important to safety, design features such as redundancy, diversity, tolerance of random failure, independence of equipment and systems, tolerance of common cause failures, testability and maintainability, and fail safe design, and selection of high quality equipment are typically used to provide the specified reliability of safety functions.

Redundancy

5.13. Electrical power systems important to safety should be redundant to the degree necessary to meet design basis reliability requirements.

5.14. Redundancy is commonly used in electrical power systems important to safety to achieve system reliability goals or conformity with the single failure criterion. For redundancy to be fully effective, independence is also necessary. Taken alone, redundancy increases the reliability of safety actions, but it also increases the likelihood of spurious operation.

5.15. Operating experience indicates that additional redundancy within a train or division provides operational flexibility and increased availability.

Independence

5.16. SSR-2/1 Requirement 24 states that:

> "The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity,

redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability."

5.17. SSR-2/1 Requirement 21 states that:

> "Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate."

5.18. SSR-2/1 para. 5.35 states that:

> "The design shall be such as to ensure that any interference between items important to safety will be prevented, and in particular that any failure of items important to safety in a system classified in a lower safety class will not propagate to a system classified in a higher safety class."

5.19. Independence is provided to prevent a failure or an internal or external hazard from affecting redundant elements of safety systems. It also prevents a failure or hazard from affecting systems that provide different levels of defence in depth. Failure processes to be considered include: failures resulting from design basis events; exposure to the same internal or external hazards; failure of common support systems; electrical connections between systems or divisions; data exchange between systems or divisions; and common errors in design, manufacture, operations or maintenance.

5.20. Safety items should be unaffected by the accidents to which they respond.

5.21. Safety systems should be independent from systems of lower safety classification as necessary to ensure that the safety systems can perform their safety functions during and following any event that requires these functions to be performed.

5.22. Redundant portions of safety groups should be independent of one another to ensure that the safety group can perform its safety functions during and following any event that requires these functions to be performed.

5.23. Failure of one part of the electrical power structures, systems and components should not render other parts inoperable when they are required to function.

5.24. The functional failure of the support features of safety systems should not compromise the independence between redundant parts of safety systems or between safety systems and systems of lower safety classification. For example, assigning a safety system support feature such as room ventilation to the same division as the safety system it supports prevents the loss of mechanical function in one division causing a loss of electrical power system function in another division.

5.25. When isolation devices are used between systems of different safety importance, they should be a part of the system of higher importance.

5.26. The adequacy of design features provided to meet the requirements for independence should be justified.

Physical separation

5.27. Physical separation:

- Protects against common cause failure due to the effects of internal hazards. Internal hazards of concern include: water hazards from direct and indirect sources of water, such as spray and seepage through roofs, walls, raceways and conduits, fire, missiles, steam jets, pipe whip, chemical explosions, flooding and failure of adjacent equipment.
- May be used to protect against common cause failure due to normal, abnormal or accident conditions, the effects of design basis accidents, or the effects of internal and external hazards. Environmental, seismic and electromagnetic qualification may also be used by themselves, or in conjunction with physical separation, to protect against the effects of accidents, internal hazards or external hazards.
- Might reduce the likelihood of common cause failures as a result of events that have localized effects (e.g. the impact of a small aircraft).
- Reduces the likelihood of inadvertent errors during operation or maintenance on redundant equipment.

5.28. Physical separation is achieved by barriers, distance or a combination of the two.

5.29. NS-G-1.7 [5] and NS-G-1.11 [6] give guidance on protection against fires and other internal hazards.

5.30. Some areas that might present difficulties owing to convergence of equipment or wiring are:

- Containment penetrations;
- Motor control centres;
- Switchgear areas;
- Cable spreading rooms;
- Equipment rooms;
- The main control room and other control rooms;
- The plant process computer.

Electrical isolation

5.31. Electrical isolation is used to prevent electrical failures in one system from affecting connected systems. Electrical isolation controls or prevents adverse interactions between equipment and

components caused by factors such as electromagnetic interference, electrostatic pickup, short circuits, open circuits, grounding or application of the maximum credible voltage (AC or DC).

5.32. As far as reasonable practicable, non-safety loads should not be powered by electrical safety power systems.

5.33. If it is necessary to power non-safety loads from electrical safety power systems the non-safety loads should be isolated by means of safety classified isolation devices.

5.34. An example of a preferred isolation device is a safety grade circuit breaker that is automatically tripped by an accident signal or loss of voltage signal generated within the same safety division as the isolation device.

5.35. Redundant divisions of safety classified electrical power systems should not be interconnected.

5.36. Temporary connections between redundant divisions may be made during operation if a safety assessment confirms that the reliability of a power supply is increased significantly and that sufficient independence of the redundant divisions is ensured.

5.37. Temporary connections between redundant divisions may be made during shutdown if a safety assessment confirms the following:

- That the interconnections have interlocks that cannot be defeated by simple switch operation;
- That the effects of these connections on the reliability of plant safety functions and on their vulnerability to common cause failure is acceptable.

5.38. These interconnections could also be used in station blackout conditions.

5.39. Examples of provisions for electrical isolation include circuit breakers, relays, electronic isolation devices, optical isolation devices (including optical fibre), cable or component shielding, separation distance, internal mechanical structures, or combinations of these.

5.40. Qualification for electromagnetic compatibility complements electrical isolation by protecting against electromagnetic interference and electrostatic pickup.

Associated circuits

5.41. When it is impractical to provide adequate separation and isolation from electrical faults between a safety circuit and a circuit of a lower class function, the lower class circuit (associated circuit) should be:

(a) Analysed or tested to demonstrate that the association does not unacceptably degrade the safety class circuits with which it is associated,

(b) Identified as part of the safety division with which it is associated, and

(c) Electrically separated from other components in the same manner as the circuits of the safety division with which it is associated.

Diversity

5.42. Safety power systems should be supplied from diverse electrical power supplies.

5.43. Diversity in power sources is usually inherent in the architectural design of the power system.

5.44. Typically safety power system loads can be supplied from:

- The off-site power system, via the preferred power supply;
- The main generator, which is the normal power source, or during house load operation will supply power;
- The standby power source, which will supply the safety power systems on loss of off-site power; or
- An alternate AC power source in station blackout conditions.

5.45. DC loads can be supplied from batteries or (via rectifiers) from any of the above mentioned sources.

5.46. Uninterruptible AC power systems can be supplied from batteries or battery chargers (via inverters) or from safety system AC buses using bypass switches.

5.47. Where the design basis requires diversity for software based devices of an electrical power system, the guidance of Ref. [2] should be followed.

5.48. Diversity of power supply sources for specific loads, for example, instrumentation and control systems, might often improve the availability of the overall system.

5.49. If non-electrical power systems are provided as a diverse means of accomplishing a given safety function, any of their associated power supplies and instrumentation and control systems should be independent of the system together with which they are intended to be diverse.

5.50. This recommendation applies to multiple non-electrical power systems that are diverse as well as non-electrical power systems (such as steam or engine driven pumps) that are provided for diversity from electrical power systems.

5.51. In addition to physical separation and electrical isolation, diversity might be necessary to increase independence between redundant systems or between systems supporting different levels of defence in depth. This may be achieved by the use of diverse power sources or by supply from uninterruptible power supplies.

Common cause failures

5.52. SSR-2/1 Requirement 24 states that:

> "The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity,

redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability."

5.53. The possibility of common cause failures, which could render the safety power systems unavailable to perform their safety functions when called upon, should be considered in the design, maintenance, testing and operation of the safety power systems and their support systems.

5.54. The principles of diversity and independence (physical separation and functional isolation) should be applied to protect against credible common cause failures originating in the equipment of the safety system itself, in switching surges or voltage and/or frequency excursions from connected systems or from human involvement (e.g. in operations and maintenance).

5.55. The use of features of independence and diversity helps to ensure — but does not fully guarantee — that common cause failures will not be the primary cause of system unavailability.

5.56. As the nuclear power plant is normally connected to only one transmission system, one event on the grid could influence redundant parts of the safety power systems. If the nuclear power plant has two turbines and two generators, the possibilities of common cause failure will be reduces. If the redundant safety power systems are fed from independent connections to the grid, the possibilities of common cause failure will also be reduced.

5.57. Operating experience of events relating to voltage transients, on both off-site and on-site power supplies, has demonstrated the need for increased attention to the design of the electrical power systems in order to minimize the risk of common cause failures. A 'no interruption' concept is desirable, realized as a series of design measures to minimize the impact of transients (see Fig. 5).

5.58. Owing to the voltage excursions, frequency excursions and phase angle excursions that can occur in a power generating facility, operating experience from industrial applications is of limited value when screening for vulnerabilities for common cause failure originating from the preferred power supply.

5.59. The primary protection features against common cause failures originating from the grid are:

- Comprehensive design bases and guidelines that identify all possible events that could challenge the safety power systems;
- Verified capability of the safety power systems to cope with these events, either by means of built in features or by relay protection; and
- Verified capability not to transmit voltage excursions and frequency excursions to buses fed from rectifiers and inverters.

5.60. After an event that ends in a loss of off-site power, if the safety power systems are not fed from the main generator(s), the standby power sources will start and will supply the safety power systems. Even if the safety power systems are divided into different divisions, the starting sequence of the

standby power sources has a potential for common cause failure as the same physical properties are used to initiate all divisions.

5.61. The primary protection features against common cause failures for the standby power sources are:

- Comprehensive design bases and guidelines that identify all possible events that could challenge the control, start and operation of the standby power sources;
- Verified capability of the standby power sources to cope with these events, either by built in features or by relay protection; this also includes the transient performance during loading of the standby power sources;
- Proper redundancy of control circuits and equipment to ensure reliability in starting and endurance in operation and to prevent unnecessary tripping.

5.62. In order to minimize the risks of common cause failure for software based devices, appropriate design features for instrumentation and control equipment as recommended in Ref. [2] should be used.

Failure modes

5.63. SSR-2/1 Requirement 26 states that:

> "The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety."

5.64. The failure modes of electrical components important to safety should be known and should be documented.

5.65. Knowledge of component failure modes is necessary in order to apply the fail-safe concept.

5.66. Failures of electrical components important to safety should be detectable by means of periodic testing or revealed by means of alarms or indications of anomalies.

5.67. The design should be such that failures are self-revealing except where such a design might result in an unsafe state or might cause a spurious actuation of a safety system.

Protection coordination

5.68. The electrical protection scheme should prevent failures from disabling safety functions, to an acceptable level.

5.69. The protective actions of each load group should be independent of the protective actions provided by a redundant load group.

5.70. Protective relays should be used for the prompt removal from service of any element of a power system when abnormal conditions occur such that operating equipment might be degraded or might fail.

5.71. Selective tripping of circuit breakers should be used to minimize the impact of fault conditions.

5.72. The protection scheme should be capable of the following:

(a) Operating the required devices upon detection of unacceptable conditions to reduce the severity and extent of disturbances of electrical power systems, equipment damage, and potential hazards to personnel and property;

(b) Monitoring the connected preferred power supply with provisions to initiate, automatically or manually, transfer to an alternative supply:

The alternative supplies in this case may be different off-site supplies or standby AC power supplies. Fast bus transfers using best technology and adequate interlocks with protective schemes can reduce stresses on operating equipment:

(c) Providing indication and identification of the protective operations;

(d) Monitoring the availability of power for the protection systems control power;

(e) Ensuring that only faulted equipment is disconnected from the power source with minimum impact on operating equipment.

5.73. Typically, a protection scheme that disconnects only faulted equipment has the following characteristics:

- In case of short circuits and overloads, protective devices are designed to operate selectively in all planned connection conditions of the electrical power systems.
- Protective devices are designed to initiate the circuit breaker for clearing fault currents rapidly enough to avoid hazards and to minimize disturbances.
- The plant's switchgear that is provided with reliable arc protection, or other appropriate protection, to minimize damage to the switchgear caused by potential arc faults and to ensure the safety of the plant and to protect the operating and maintenance personnel.
- Individual protective devices installed to protect components during testing are listed and designed so that their operation does not endanger a system's capability to operate in an actual event.

5.74. The protection scheme should consider reacceleration currents after voltage sags and interruptions or bus transfer.

5.75. The design of protective devices should include consideration of both symmetrical and asymmetrical faults.

5.76. Faults to be considered include all possible types of series and shunt faults, including events such as loss of a phase and ground faults in systems not connected to ground. Protection coordination also includes consideration of measuring principles.

5.77. Provision of means to capture transients in events is desirable in order to support verification of the analysis performed and protection coordination.

5.78 Digital protective devices should be verified for use in accordance with the safety function that they are intended to perform.

5.79. The design of the protective devices for electrical power systems and for components of nuclear power plants should also comply with national standards that apply to the safety of electrical equipment and electrical installations, as well as with other relevant regulations on electrical equipment and electrical installations.

Confirmation of reliability

5.80. For all systems important to safety, a systematic assessment should be conducted to confirm that the reliability requirements of the design basis for the systems are achieved in the design.

5.81. The use of software or complex multi-element logic modules could cause difficulties in the confirmation of reliability and sensitivity to common cause failures. The confirmation of reliability may therefore depend on assurances of freedom from error in the design and implementation process. Reference [2] provides recommendations and guidance on this subject.

5.82. Test facilities that are part of the safety system should be considered in determining the availability of systems.

RATING

5.83. All items of equipment used in the electrical power systems in the plant should have a sufficient margin in operating parameters in comparison with their nominal rating.

5.84. Analyses and simulations should be performed to confirm the design margins, on the basis of conservative assumptions and qualified methods.

5.85. The adequacy of the margin in equipment rating should be confirmed regularly and at least in conjunction with the replacement of major components, plant modifications and periodic safety reviews.

5.86. Electrical equipment should be specified with an adequate design margin to ensure that future plant upgrades and modifications can be implemented without exceeding equipment ratings.

Motor loads

General

5.87. Motors for items important to safety should be designed with pull-out torque high enough to permit starting with minimum allowable design voltage, as specified by the design bases of the electrical power system.

5.88. Motors and other devices for items important to safety that are connected to the power system should withstand the overvoltages and undervoltages as well as the over frequencies and under

frequencies that could result from the applicable steady state, short term operation and transient conditions that are specified in the design basis.

5.89. The loads used for rating motors and for the design of components in safety power systems, as well as for settings for overload protective devices, should reflect the actual motor loads and, where applicable, the run-out torque.

5.90. Valve actuators should be designed to close with enough torque at low voltage and low frequency, not to exceed maximum permissible torque at high voltage and high frequency, and to be able to open the valves at low voltage.

5.91. Protective devices for motor drive actuators should be coordinated with torque switch settings to avoid nuisance trips during operation.

Design for overload operation

5.92. Electrical equipment and cables should be designed to permit necessary overload operation without exceeding their rating.

5.93. It might be necessary in some situations to operate equipment for a short time period in overload. Typically this might occur when large pumps start with minimum backpressure resulting in operation under run-out conditions. For example, the set points of circuit protective devices may be set higher than the levels necessary to protect the equipment from damage due to continuous overloads.

5.94. Cables should be protected against overload in accordance with their capability for carrying continuous current.

5.95. Where operation of overloaded equipment is permitted, such operation should not adversely affect other circuits or associated equipment.

5.96. The continued operation of safety system equipment under overload conditions with the consequent risk of its damage should not be credited in the safety justification for operation under accident conditions.

5.97. Sustained loading above continuous rating should be indicated in the control room.

5.98. If circuit protective devices are set at a higher level, an undetected overload could remain in the system under normal operating conditions, thus possibly accelerating the failure of the equipment necessary in the particular situation.

ELECTRICAL EQUIPMENT, CABLES AND RACEWAYS

General

5.99. Electrical equipment as discussed here comprises switchgear, motor control centres, transformers and cable systems.

5.100. Electrical equipment should be selected, rated and qualified for its service conditions and environmental conditions.

5.101. Electrical equipment should be sufficiently fire retardant to prevent the propagation of fires.

5.102. Aspects of fire safety are considered in Ref. [5].

Rating and sizing

5.103. Electrical equipment should have a voltage rating greater than (typically 110% of) the nominal system voltage and an impulse rating greater than any transient voltage to which the equipment might be subjected.

5.104. Electrical equipment should be sized:

(a) To carry the currents of the main circuits and branch circuits required under allowable voltage variations;

(b) To meet the demands of the loads without exceeding rated temperature;

(c) To withstand short circuits (e.g. fault current during the specified clearing time for faults);

(d) To withstand peak currents without exceeding mechanical strength.

5.105. Factors to be considered in the calculation of conductor temperatures include:

- Maximum environmental temperatures;
- Normal currents and fault currents;
- Load factors;
- The arrangements of other cables in the same or nearby raceways;
- The influence of cable supports, wall penetrations, floor penetrations, fire stops and fire retardant coatings on cable heating.

Installation

5.106. Buses, raceways (i.e. trays or conduits) and their supports should be designed to withstand, with an appropriate margin, the mechanical loads imposed by the cables and their associated fittings.

5.107. Safety system buses, cubicles and cables should be adequately protected against the hazards that could result from postulated initiating events.

5.108. Hazards that could affect buses, cubicles and cables include: the effects of fire, and the failure or malfunction of fluid systems and mechanical or structural components.

5.109. Generally the design should be such as to ensure that cables that are part of safety systems are routed or protected so that external events such as a fire, failure of rotating mechanical equipment or failure of support systems do not damage more than the minimum set that is justified in the safety analysis report (normally one division of any safety group). Failure of mechanical equipment includes

possible effects of pipe whip, jet impingement and the generation of missiles as a result of the failure of rotating equipment or other high energy systems. Recommendations and guidance on protection against the failure of mechanical equipment are provided in Ref. [5].

5.110. Raceways and cables should be permanently identified with their respective divisions.

5.111. Common practice is to identify raceways and cables permanently at each end and at regular intervals (except for cables in closed raceways). The identification of raceways usually also includes the cable voltage class.

5.112. Each cable, on installation, should be given adequate identification to ensure its installation in the proper raceway.

5.113. In general, the use of cable splices in raceways should be prohibited.

5.114. Cable splices may be used for connections between field cables and equipment provided that the cable splices are qualified for the service. Such termination techniques may be necessary for safety cables and equipment in the containment to protect against high leakage currents that might be generated by exposure to environmental conditions caused by accident conditions.

Cable separation

5.115. Physical separation by use of appropriate methods (e.g. distance or a physical barrier) should be provided between:

(a) Cables classified as safety and cables without safety classification;
(b) Cables belonging to different safety divisions;
(c) Cables of different voltage classes.

5.116. Separation by safety classification is intended to avoid damage to safety classified cables as a result of failures in systems or cables without safety classification. Separation between cables of different safety divisions is intended to prevent a single hazard from affecting more than one redundant item in a safety system. Separation by voltage classes is intended to prevent the electromagnetic interference expected in higher energy circuits from unacceptably affecting lower energy circuits.

5.117. Physical separation should be provided between cables in the following voltage classes:

(a) Instrumentation and control cables;
(b) Low voltage power cables (1 kV or less);
(c) Medium voltage power cables (greater than 1kV to 35 kV);
(d) High voltage power cables (greater than 35 kV).

5.118. High voltage power cables are not commonly used in on-site power systems in nuclear power plants.

5.119. Only cables of the same voltage class should be placed in the same raceway (i.e. ladder, tray or conduit).

5.120. Cables and raceways of different voltage classes should be separated according to class either by spatial separation or by means of barriers that prevent one class from having a detrimental effect on the other.

5.121. A grounded metallic conduit represents an acceptable separation barrier.

GROUNDING PRACTICES

General

5.122. Grounding serves to ensure both electrical safety and the functionality of electrical power systems and instrumentation and control systems. Detailed design guidelines for grounding are available in national and international standards.

5.123. In any power generating plant there are generally four conceptually identifiable, but not necessarily physically distinct, grounding systems: for personnel safety, for lightning, for electrical power systems and for instrumentation and control systems, including signal grounding.

5.124. All grounding systems should be connected to a single grounding grid.

5.125. The ground resistance value should reflect:

(a) Fault current capacity of equipment;

(b) Electrical safety; i.e. the allowable step and touch voltage with assumed lightning discharge or fault current to the ground.

5.126. International standards describe a number of solutions for grounding of instrumentation and control systems. Typically, power generating plants use one of two approaches for grounding of instrumentation and control systems: single point grounding or multiple point grounding. The preferred solution is design specific.

5.127. The grounding approach used should be justified and coordinated with the overall design provisions for electromagnetic compatibility.

Electrical safety

5.128. Overall grounding should be designed, installed and maintained so as to effectively protect people from harm, and buildings and equipment from damage, as well as to protect electrical power and instrumentation and control systems from damage.

5.129. The metallic frames of all equipment and apparatus should be connected to ground, except when the connection will interfere with its functionality.

5.130. If frames are not connected to ground, additional provisions for ensuring safety should be made.

5.131. In the design of grounding systems, an electrical power system should be considered one entity, since inadequate grounding of even one part of the system might affect the entire system.

Functionality

5.132. Medium voltage AC electrical power systems should preferably be high impedance grounded.

5.133. High impedance grounding limits fault currents and allows continued operation of the affected equipment.

5.134. Other grounding solutions such as solid grounded or insulated systems may be used when justified.

5.135. In high impedance grounded systems, the electrical power system should be monitored for ground faults at every voltage level and it should allow easy identification of the location of a failure.

5.136. Detection of low impedance to ground should only alarm and should allow the equipment still to perform its function.

5.137. Protective schemes may trip equipment on multiple faults.

LIGHTNING AND SURGE PROTECTION

5.138. Provision should be made that a lightning strike will not prevent the power systems and instrumentation and control systems from fulfilling their required safety functions.

5.139. The systems for achieving such a provision may rely on external or internal protection. Typically a combination of both methods will be necessary.

5.140. External provisions will normally include either lightning conductors or a Faraday cage comprising the metal parts of the building which shield the building and its equipment from the effects of a lightning strike. Internal provisions could include specific electromagnetic shielding for rooms in order to create an environment protected from electromagnetic hazards.

5.141. Internal lightning protection will normally include shielding and surge arresters to protect against both the induced high voltage caused by the lightning current and high transferred voltage. High transferred voltages are caused by voltage differences between the ground and parts of the external lightning protection system and the associated grounding connections.

5.142. To protect the safety power system from induced voltages, safety classified raceways and cables should not be located close to the outer walls of buildings.

5.143. External lightning protection should be grounded so as to conduct the lightning current to ground outside the building.

5.144. The internal protection grounding should be connected to the rest of the lightning grounding in such a way that it protects personnel and equipment against high transferred potentials.

5.145. Connections of lightning protection systems to ground should be routed so that the effects of lightning discharges do not jeopardize either the safety functions of safety power systems or the lightning protection grounding.

5.146. The plant grounding may be supplemented by specific ground connections.

5.147. Structures that are not an inherent part of the plant, such as warehouses, offices and workshops for maintenance and support staff, should generally not be supplied from power distribution systems at the plant.

5.148. If plant buses are used to supply power to ancillary buildings, adequate measures should be taken to ensure that electrical noise and voltage perturbations generated by equipment in these buildings does not adversely affect the plant power systems.

5.149. Power systems for control and monitoring should not be distributed outside the plant so as to minimize the risk for disturbances due to induction or other influences.

5.150. Connections to other buildings — with adequate protection, such as grounded steel walls, against induced voltages and rise in ground potential caused by lightning — can be justified if the cable route is protected in a similar way.

5.151. Voltage surge suppressors or surge arresters should be provided to prevent surges from exceeding the allowable voltage limits set for equipment or its insulation.

5.152. Overvoltage surges can be caused by lightning strikes, electrical faults or switching phenomena. Suppressors might be necessary on various voltage levels.

5.153. Switching operations, rectifiers, inverters and rotating equipment can generate harmonics and electrical noise that may be detrimental to equipment designed to operate at nominal frequency and voltage. Additional equipment to filter or suppress electrical noise may be necessary for the reliable operation of equipment sensitive to electrical noise in the power system.

EQUIPMENT QUALIFICATION

General

5.154. SSR-2/1 Requirement 30 states that:

> "A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing."

5.155. Electrical power systems and components important to safety should be qualified for their intended function over their service life.

5.156. The qualification should assure confidence commensurate with the safety classification of the system or component.

5.157. The qualification programme(s) should address all topics affecting the suitability of the system or component for its intended functions important to safety, including:

(a) Suitability and correctness of functions and performance;

(b) Environmental qualification of components;

(c) Seismic qualification of components;

(d) Electromagnetic qualification.

5.158. Qualification should be based on an appropriate combination of methods, including for example:

(a) Use of engineering processes and manufacturing processes in compliance with recognized standards;

(b) Demonstration of reliability;

(c) Past experience in similar applications;

(d) Type testing;

(e) Testing of supplied equipment; or

(f) Analysis to extrapolate test results obtained or operating experience gained under pertinent conditions.

5.159. It is generally not necessary to apply all of the methods mentioned. The specific combination of methods will depend on the system or component under consideration. For example, the qualification of pre-existing items might place more emphasis on past experience and analysis to compensate for a lack of completely documented verification and validation in engineering and manufacturing.

5.160. The method or combination of methods used for equipment qualification should be justified and documented.

5.161. Where operating experience is used to support equipment qualification, it should be shown to be relevant to the proposed use and to the environmental conditions of the target application.

5.162. An analysis that is part of the evidence for equipment qualification should include a justification of the methods, theories and assumptions used.

5.163. For example, the validity of the mathematical models used for equipment qualification may be justified on the basis of experimental data, test data or operating experience.

5.164. Traceability should be ensured between each installed system and component important to safety and the applicable evidence of qualification.

5.165. This includes traceability not only to the component itself, but traceability between the qualified configuration and the installed configuration.

Suitability and correctness

5.166. The equipment qualification programme should demonstrate that the design of electrical power structures, systems and components and software meet all requirements for capability, capacity and reliability important to safety contained in the applicable design bases and equipment specifications.

5.167. Examples of reliability requirements include, for example, requirements for fail-safe behaviour, conformance with the single failure criterion, independence, failure detection, maintainability and service life.

5.168. The equipment qualification programme should demonstrate that the as-built electrical power systems and installed components correctly implement the qualified design.

Environmental qualification

5.169. In this Safety Guide, 'environmental qualification' means qualification for temperature, pressure, humidity, contact with chemicals, radiation exposure, meteorological conditions, submergence and ageing mechanisms as conditions that could affect the proper functioning of components.

5.170. Structures, systems and components important to safety should be designed to accommodate the effects of, and should be compatible with, the environmental conditions associated with all plant states in which they are required to function.

5.171. Components important to safety should be shown to meet all requirements for the design basis when subjected to the range of environmental conditions specified in the design basis.

5.172. A component might have a safety function even when full operability is not required, for example, to maintain mechanical integrity, or not to fail in certain modes.

Components exposed only to mild environmental conditions

5.173. Environmental qualification of components of electrical power system that are important to safety and whose environmental service conditions in accidents are at no time significantly more severe than conditions in normal operations (i.e. in mild environmental conditions) may be based on supplier certification that the components are suitable for the specified operating conditions.

Components exposed to harsh environmental conditions

5.174. Environmental qualification of safety classified components of electrical power systems whose environmental service conditions in accident conditions are at any time significantly more severe than conditions during normal operation (i.e. harsh environmental conditions) should show that the component is, at the end of its qualified life, capable of performing its safety functions under the full range of specified service conditions.

5.175. Showing that components can function as required at their end of their qualified life involves addressing significant ageing effects (e.g. radiation ageing and thermal ageing) to show that the required functionality is maintained at the end of the qualified life. Usually, this includes providing further conservatism, where appropriate, to allow for unanticipated ageing mechanisms.

5.176. In defining the equipment qualification programme, the worst credible combinations of environmental service conditions, including synergistic effects between service conditions, should be addressed.

5.177. If it is necessary to test separately for different environmental conditions (e.g. separate tests for radiation effects and for temperature effects), the sequence in which these tests are conducted should be justified as one that appropriately simulates the degradation caused by the combined environmental conditions.

5.178. The most rigorous environmental qualification methods may be applied only to safety components.

5.179. Environmental qualification of safety components that are expected to operate in harsh environmental conditions should include type testing.

5.180. When protective barriers are provided to isolate equipment from possible environmental effects, the barriers themselves should be subject to a qualification programme to validate their adequacy.

Internal and external hazards

5.181. The plant design basis and the plant's safety analysis will identify internal and external hazards, such as fire, flooding and seismic events, that the plant is required to withstand for operation or is required to withstand safely, and for which protection or system qualification is necessary.

5.182. Electrical power systems and components should be protected against the effects of fire and explosion in accordance with the recommendations and guidance of NS-G-1.7, Ref. [5].

5.183. Electrical power systems and components should be protected against the effects of other internal hazards in accordance with the guidance of recommendations and NS-G-1.11 Ref. [6].

5.184. Electrical power systems and components should be designed and qualified to withstand seismic hazards in accordance with the guidance of NS-G-1.6, Ref. [7].

5.185. Electrical power systems and components should be protected against or designed and qualified to withstand other external hazards in accordance with the guidance of NS-G-1.5, Ref. [8].

Electromagnetic qualification

5.186. The undisturbed operation of electrical and electronic systems and components depends upon the electromagnetic compatibility of components with the conditions in their operating environments;

that is, on a component's capability to withstand more disturbances than are caused by the components around it or connected to it.

5.187. Equipment and systems important to safety, including associated cables, should be designed and installed to withstand the electromagnetic conditions in the environments in which they are located.

5.188. Significant sources of electromagnetic interference include, for example, fault current clearance by switchgear or circuit breaker or fuse operation; electric fields caused by radio transmitters; other human made sources of electromagnetic interference internal or external to the plant; and natural sources of electromagnetic interference such as lightning strikes.

5.189. Electromagnetic qualification of electrical power systems and components depends upon a combination of system design and component design to minimize the coupling of electromagnetic noise to electrical components; testing to demonstrate that components can withstand the expected levels of electromagnetic noise; and testing to demonstrate that electromagnetic emissions are within tolerable levels.

5.190. Techniques for minimizing the production and coupling of electromagnetic noise include:

- Suppression of electromagnetic noise at the source;
- Separation and isolation of signal cables for instrumentation and control systems from power cables;
- Shielding of equipment and cables from external magnetic and electromagnetic fields sources;
- Filtering electromagnetic noise before it can become coupled to sensitive electronic circuits;
- Neutralization or isolation of electronic equipment from ground potential differences; and
- Proper grounding of electrical equipment, raceways, cabinets, components and cable shields.

5.191. Detailed requirements for electromagnetic compatibility should be determined for all electrical power systems and components and the compliance of these systems and components with the requirements should be demonstrated.

5.192. Appropriate practices for installation and maintenance should ensure the proper implementation and continued effectiveness of these provisions.

5.193. International standards for electromagnetic compatibility for industrial environmental conditions may serve as the basis for the requirements provided that such standards are supplemented, where necessary, to cover the electromagnetic compatibility of components of a nuclear power plant, which might be more demanding. Determining the requirements for electromagnetic compatibility includes considering the subjection of components to possible repetitive surges (e.g. switching off of inductive loads and ringing of relays) and high energy surges (e.g. due to power faults and lightning).

5.194. Establishing the electromagnetic compatibility of electrical power systems and components at a nuclear power plant unit involves making unit specific analyses. The adequacy of each electrical component's requirements for electromagnetic compatibility is evaluated on the basis of these unit specific analyses.

5.195. The types of electromagnetic interference that should be considered in the design of electrical power systems and components include:

- Emission of and immunity to radiated electromagnetic disturbances;
- Emission and conduction of electromagnetic disturbances via cables;
- Electrostatic discharge;
- Switching transients and surges;
- The emission characteristics of wireless systems and devices used at the plant as well as those of repair, maintenance and measuring devices. Wireless systems and devices include, for example, mobile phones, radio transceivers, and wireless data communication networks.

5.196. It should be considered whether it is necessary to establish exclusions zones in the vicinity of certain sensitive equipment within which the operation of wireless devices and other portable sources for electromagnetic interference (e.g. welders) is not permitted.

5.197. Limits on radiated and conducted electromagnetic emissions should be established for all plant equipment.

5.198. Any electrical or electronic equipment in the plant will contribute to the electromagnetic conditions. The limits to electromagnetic emissions should therefore apply to all plant equipment, not just to equipment important to safety.

5.199. Emission limits placed on individual components should be below the operating envelope for electromagnetic interference by an amount that is sufficient to ensure that no single item makes a significant contribution to the hazards due to electromagnetic interference.

5.200. The equipment qualification programme should show that electromagnetic emissions of all items of plant equipment are within the specified limits.

5.201. Equipment and systems, including associated cables, should be designed and installed so as to appropriately limit the propagation (both by radiation and by conduction) of electromagnetic interference among items of plant equipment.

5.202. Instrumentation cables should have twisting and shielding sufficient to minimize interference from electromagnetic interference and electrostatic interference.

5.203. Reference [2] provides additional recommendations and guidance for the electromagnetic compatibility of the electronic elements of the electrical power system.

DESIGN TO COPE WITH AGEING

5.204. SSR-2/1 Requirement 31 states that:

> "The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life."

5.205. SSR-2/1 para. 5.51 states that:

> "The design for a nuclear power plant shall take due account of ageing and wear out effects in all operational states for which a component is credited, including testing, maintenance, maintenance outages, plant states during a postulated initiating event and plant states following a postulated initiating event."

5.206. SSR-2/1 para. 5.52 states that:

> "Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help to identify unanticipated behaviour of the plant or degradation that might occur in service."

5.207. SSR-2-1 Requirement 31 and paras 5.51 and 5.52 are aimed at ensuring that ageing effects will not impair the ability of safety components to function under severe environmental conditions. Such degradation could occur well before the functional capabilities under normal conditions are noticeably affected.

5.208. Ageing mechanisms that could significantly affect electrical components, and means for following the effects of such mechanisms, should be identified in the design process.

5.209. Identification of potential ageing effects involves initially understanding of the relevant ageing phenomena, which forms part of the design process.

5.210. Ageing effects are most commonly due to heat and to radiation exposure, but other phenomena (e.g. mechanical vibration or chemical degradation) could be important ageing mechanisms for certain components.

5.211. Maintenance programmes, surveillance programmes and ageing management programmes should include activities to identify any trend towards degradation (ageing) that could cause equipment to become incapable of performing its safety function.

5.212. Examples of monitoring techniques include:

- Testing of plant components or of components subject to ageing that is representative of that of plant components;

- Visual inspections; and
- Analysis of operating experience.

5.213. Examples of means to address ageing impacts include:

- Component replacement before the end of its qualified life;
- Adjustment of functional characteristics to account for ageing effects; and
- Changes to maintenance procedures or environmental conditions that have the effect of slowing the ageing process.

5.214. The qualified life of safety components that have to perform their safety function in harsh environmental conditions should be determined.

5.215. Safety classified components should be replaced before the end of their qualified life.

5.216. Ongoing qualification could show that the qualified life of a component is validated or is indicated to be different from the expected lifetime. Information from ongoing qualification may be used to increase or decrease the qualified life of a component.

5.217. Reference [9] provides additional recommendations and guidance on ageing management, including the interface between equipment qualification and the ageing management programme.

CONTROL OF ACCESS

5.218. SSR-2/1 Requirement 39 states that:

> "Unauthorized access to, or unauthorized interference with, items important to safety, including computer hardware and software, shall be prevented."

5.219. Access to equipment in systems important to safety should be limited so as to prevent unauthorized access and to reduce the possibility of error.

5.220. Effective methods include appropriate combinations of physical security, e.g., locked enclosures, locked rooms, alarms on enclosure doors and administrative measures.

5.221. Areas of particular concern are access to set-point adjustments and calibration adjustments, because of their importance in preventing degradations in the performance of systems due to operating errors and maintenance errors.

5.222. Reference [2] provides additional recommendations on access control and on the security of computer based applications used in electrical power systems.

Test provisions

5.223. All systems important to safety should include provisions for testing, including built-in test capabilities where appropriate.

5.224. Design of the test provisions should be coordinated with the design of the operational test programme so that availability requirements of systems and components can be fulfilled. This includes taking into consideration failure rates of components in establishing test frequencies. It is envisaged that certain tests could only be performed during refuelling outages.

5.225. Arrangements for testing include procedures, test equipment interfaces, installed test equipment and built in test facilities.

5.226. Testing and calibration of safety system equipment should be possible in all modes of normal operation, including power operation, while retaining the capability of safety systems to fulfil their safety functions.

5.227. Periodic tests during plant operation will normally be necessary to achieve the reliability required of safety systems; however, it is sometimes desirable to avoid conducting tests during operation if they could jeopardize the safe operation of the plant.

5.228. The capability for testing and calibration during power operation is not necessary if it would adversely affect the safety or the operation of the plant.

5.229. If means are not provided for testing safety equipment during power operation, the following should be provided:

(a) Justification that the reliability of the functions that could be affected is acceptable;

(b) The capability for testing during shutdown.

Test programme

5.230. The design of systems important to safety should include identification of a testing programme that supports implementation of the guidance given in: NS-G-2.2, Ref. [10]; NS-G-2.4, Ref. [11], NS-G-2.6, Ref. [12]; and NS-G-2.14, Ref. [13].

5.231. A test programme will normally include:

– A description of programme objectives;

– Identification of systems and components to be tested;

– A master test schedule;

– Bases and justification for the tests to be conducted and test intervals;

– Acceptance criteria;

– A description of the documentation and reports required;

– Periodic review of the effectiveness of the programme;

– The individual test procedures to be used to control the conduct of tests.

5.232. The scope and frequency of testing should be justified as consistent with functional requirements and availability requirements.

5.233. Implementation of the test programme should provide:

(a) Objective information on the status of systems and components;

(b) Assessment of the degradation of components;

(c) Data on trends to assist in detecting degradation of components;

(d) Indications of incipient failure within the system;

(e) Requirements for evaluations that should be conducted before repetition of the failed test can be credited as establishing operability.

5.234. Evaluation and documentation of the causes of a failed test, and of the remedial actions taken, are necessary before the results of a repeated test can be used to demonstrate operability of the systems or components involved. Corrective actions may, for example, include calibration, maintenance or repair of components, or changes to test procedures.

5.235. The test programme for electronic components of electrical power systems, including protective devices that include electronic components, should also meet applicable parts of guidance in Ref. [2].

5.236. The test programme should define processes for periodic tests that:

(a) Ensure the safety of the plant during the actual testing;

(b) Neither compromise the independence of safety systems nor introduce the potential for common cause failure;

(c) Should not cause deterioration of any plant component beyond that provided for in the design;

For example, the operability or reliability of diesel engines might be degraded by operation under no-load conditions or frequent rapid starts.

(d) Order tests into a sequence such that the overall condition of the systems or components can be immediately assessed;

(e) Confirm that design basis functional requirements and performance requirements are met;

(f) Include acceptance criteria;

(g) Test all inputs and output functions important to safety, such as alarms, indicators, control actions and operation of actuation devices;

(h) Minimize the possibility of spurious initiation of any safety action and any other adverse effect of the tests on the availability of the plant;

(i) Minimize the time interval during which equipment is removed from service;

(j) Wherever possible, be accomplished under the actual, or simulated, operating conditions prevailing when the system is called upon;

(k) Require post-test verification that any items that were disturbed for periodic testing have been properly returned to their original operating state;

(l) Forbid the use of makeshift test set-ups, temporary 'jumpers' or temporary modification of computer code or data in plant components.

Test equipment may be temporarily connected to equipment important to safety if the equipment to be tested has facilities specifically designed for the connection of this test equipment.

MAINTAINABILITY

5.237. The design of electrical power systems should include maintenance plans for all systems and components.

5.238. Electrical power systems important to safety should be designed and located to make surveillance and maintenance simple, to permit timely access and, in the case of failure or error, to allow easy diagnosis and repair and to minimize risks to maintenance personnel.

5.239. Design to facilitate maintenance, troubleshooting, and repair includes:

- Not locating equipment in areas where conditions of extreme temperature or extreme humidity are common.
- Not locating equipment in areas where there could be high radiation levels.
- Taking into account human factors (capabilities and limitations) in performing the required maintenance activities.
- Leaving sufficient space around the equipment to ensure that maintenance staff can perform their tasks in normal working conditions.

5.240. Means provided for the maintenance of electrical power systems important to safety should be so designed that any effects on the safety of the plant are acceptable.

PROVISIONS FOR REMOVAL OF ELECTRICAL EQUIPMENT FROM SERVICE FOR TESTING OR MAINTENANCE

5.241. Provisions for removing electrical equipment from service should ensure the equipment is properly isolated in order to protect personnel and to avoid spurious operation.

5.242. If the use of a facility for testing or maintenance can impair a function, the interfaces should be subject to hardware interlocking to ensure that interaction with the test or the maintenance system is not possible without deliberate manual intervention.

5.243. There should be a design feature to provide evidence that the electrical system concerned is ready for operation.

5.244. Removal from service of any single component of a safety system should not result in loss of the required minimum redundancy unless the acceptably reliable operation of the system can be adequately demonstrated.

5.245. Safety system designs that follow the recommendation of para. 5.244 will include provisions to allow for periodic testing of part of a safety system while the parts remaining in service can perform the required safety task.

5.246. Inoperability or bypass of safety system components should be indicated in the control room.

5.247. For items that are frequently bypassed or frequently rendered inoperable, indications in the control room of inoperability or bypass should be automatic.

5.248. NS-G-2.6, Ref. [12] provides guidance for returning systems and equipment to service after testing and maintenance.

SHARING OF STRUCTURES, SYSTEMS AND COMPONENTS IN MULTI-UNIT PLANTS

5.249. SSR-2/1 Requirement 33 states that:

> "Safety systems shall not be shared between multiple units unless this contributes to enhanced safety."

5.250. Each unit in a multi-unit power plant should have separate and independent power systems important to safety.

5.251. Electrical power systems or electrical components important to safety should not be shared between reactor units unless it can be shown that such sharing will not significantly impair the ability of the systems or components to perform their safety functions, including their ability to perform their safety functions in a simultaneous accident in all shared units.

5.252. In any demonstration that sharing of systems or components between units does not increase the likelihood or consequences of an accident, potential common cause failures and the possibility that one or more units are shut down while maintenance is performed on common parts of shared systems should be considered.

5.253. In applying the single failure criterion to units with shared systems, the analysis should show that the following conditions are met with regard to the units sharing systems or components:

(a) The safety systems of all units can perform their required safety functions despite a single failure in the shared systems or components or in supporting features or other systems with which the shared systems interface;

(b) The safety systems of each unit can perform their required safety functions despite concurrent single failures in the non-shared systems of each unit.

5.254. It is not necessary to show that conditions (a) and (b) in para. 5.253 can be met simultaneously.

MARKING AND IDENTIFICATION

5.255. SSR-2/1 para. 5.33 states that:

> "Safety system equipment (including cables and raceways) shall be readily identifiable in the plant for each redundant element of a safety system."

5.256. A consistent and coherent method of naming and identifying all electric power components should be used throughout the design, construction and operation stages of the plant.

5.257. Such an identification should not require frequent reference to drawings, manuals or other material.

5.258. The components of different safety divisions should be readily distinguishable from each other and from components of lower safety classification.

5.259. Identification may take the form of tagging or colour coding, for example.

5.260. Coherent and easily understood naming and identification of systems and components reduces the likelihood of operating, maintaining, testing, modifying, repairing or calibrating an item other than the one intended.

5.261. Components or modules mounted in equipment or assemblies that are clearly identified do not themselves need identification. Configuration management is generally sufficient for maintaining the identification of such components and modules and embedded computer software.

CONTAINMENT ELECTRICAL PENETRATIONS

5.262. Electrical penetrations are elements of accomplishing the safety function of the containment and should always be safety classified.

5.263. Structural integrity functions include the ability to withstand rated currents and fault currents without the penetration leak rate exceeding the levels specified in requirements. The safety classification of a penetration's electrical functions that do not affect structural integrity will follow the safety classification of the in-containment items that depend on the penetration.

5.264. An electrical penetration assembly should be considered part of the cable system between the load and the primary interrupting device.

5.265. Containment penetrations should be rated:

(a) For continuous service at a voltage that is greater than or equal to the voltage of the systems of which the conductors are part;

(b) For impulse voltages that are greater than or equal to the maximum credible transient voltage;

(c) To continuously carry demands from loads expected in all plant states without exceeding allowable conductor temperatures or degrading the assembly pressure boundaries;

(d) To carry short circuits safely over the period of time required for the protective device to clear fault currents, with account taken of credible voltage variations;

(e) To withstand, without loss of mechanical integrity, the maximum possible overcurrent condition that could occur following a single random failure of a device protecting against circuit overload.

5.266. The continuous current ratings and capabilities of the electrical penetrations should be considered in the settings of the protective devices.

5.267. Conductors in containment penetrations should be protected by redundant safety protective devices that operate separate interrupting devices.

5.268. A single passive protective device (e.g. a fuse) may be used if analysis of compliance with the single failure criterion shows with high confidence that a failure of that passive protective device is very unlikely and that its function would remain unaffected by the postulated initiating event.

5.269. A containment penetration that can indefinitely withstand the maximum current available due to a fault inside the containment does not need redundant protection.

5.270. The penetrations should meet the same separation criteria as the cables to which they are connected.

DISTRIBUTION SYSTEMS

Capability

5.271. Each distribution system should have sufficient capacity and capability:

(a) To supply the required loads under all required operating conditions;

(b) To withstand the maximum credible overcurrent under electrical fault conditions;

(c) To withstand transient conditions without damage to, or adverse effects on, any of its components;

(d) To withstand power supplies and loads as demanded.

Protective devices of the main circuits and branch circuits and their loads

5.272. All main circuits and branch circuits should be protected against overloads and short circuits, and be supervised for ground faults and protected where applicable.

5.273. Protective devices should be properly sized, set and coordinated to protect equipment, buses and cables of the main circuits and branch circuits from damage in overload conditions and fault conditions.

5.274. The protective devices for safety systems should be part of the safety system.

5.275. Protective devices should be located in enclosures and structures designed to protect them from environmental conditions, to limit electromagnetic emissions and to protect personnel.

5.276. The function of the protective devices is to minimize damage to equipment and any unnecessary interruption of electrical service resulting from mechanical or electrical failures or other unacceptable conditions. Protection includes equipment required to support the safety power system in

the performance of its safety function, and components whose function is to increase the availability and reliability of the safety equipment.

5.277. The coordination of the protective devices should be such that only the faulty part of the power system is isolated and the remaining intact circuits are unaffected.

CONTROLS AND MONITORING

5.278. Sufficient instrumentation and control equipment should be provided in the main control room to monitor and control the on-site and off-site power systems.

5.279. The human–machine interface for electrical power systems is subject to the relevant recommendations of Ref. [2].

5.280. Adequate methods of monitoring should be provided to assess the operability of the safety power systems. This includes the display of:

(a) Breaker positions (safety power system, power sources and large loads);

(b) Bus bar voltage and current;

(c) Voltage, current and frequency of standby power sources.

5.281. Indications of bypasses and of equipment taken out of service should be provided.

5.282. Procedures should be put in place for operation of the power systems in all plant states and all events relating to electrical systems.

5.283. Sufficient instrumentation and control equipment should be provided in the supplementary control room to monitor and control the safety power systems necessary for performance of the safety functions that are assigned to that location.

5.284. The alarm and annunciation systems relating to the electrical power systems should be designed for efficient and error free detection, diagnosis and action by operators.

5.285. Alarms warning about the loss of the operational status of the safety power supplies should be actuated by de-energized logic.

5.286. Means should be provided to initiate and control all safety actions automatically.

5.287. When a claim is made that manual action alone is acceptable, it should be shown that:

(a) The operator has sufficient and clearly presented information from sensors and equipment of the safety system to make reasoned judgments on the need to initiate the required safety actions;

(b) The operator is provided with written procedures and training for the safety tasks;

(c) The operator is allowed sufficient time to evaluate the status of the plant and to complete the required actions;

(d) The operator is provided with sufficient means of plant control to perform the required actions;

(e) The communication links between operators carrying out the actions are adequate to ensure the correct performance of these actions.

5.288. Means should also be provided to manually initiate safety actions at system level and at component levels.

5.289. Manual initiation of safety actions provides a form of defence in depth for abnormal operation and supports long term post-accident operation.

5.290. Controls for on-site power systems should include the following capabilities:

(a) Automatic selection of alternative off-site power supply when the normal off-site power supply is not available;

(b) Manual or automatic transfer to this alternative supply;

(c) Automatic disconnection of loads (as specified in the design basis) and all other power supplies from a division of the safety power system when the preferred power supply is degraded and not restored;

(d) Automatic start and connection of the standby AC power source and loads to the safety power system in the specified sequence;

(e) Manual selection of the alternate AC power supply;

(f) Synchronization of the safety power system back to the normal power supply when the latter is being reinstated;

(g) Manual switching to facilitate testing, maintenance and repair in normal operation or in shutdown mode.

5.291. Automatic load sequencers should work correctly irrespective of the actual sequence of demand; that is, the loss of off-site power and an accident signal can occur in any sequence.

SAFETY RELATED STANDBY AC POWER SOURCES

5.292. Some designs have standby AC power sources that are not designated as safety system support features. The general guidance for safety standby AC power sources applies, but the degree of equipment qualification, design confirmation and documentation should be in accordance with principles for safety related components.

5.293. Plants that do not require designated as safety system support features standby AC power sources should have safety related standby AC power sources to provide reliable power for defence in depth functions that supplement the safety systems and reduce the challenges to them.

5.294. Standby power sources should consist of an electrical power generating unit complete with all auxiliaries and dedicated separate and independent stored energy supply for both starting and running the prime mover.

5.295. The standby power source should have sufficient capacity and capability to start and supply all loads as specified in the design basis.

6. DESIGN GUIDELINES FOR PREFERRED POWER SUPPLIES

GENERAL

6.1. SSR-2/1 Requirement 41 states that:

> "The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply."

6.2. The transmission system should be able to supply the nuclear power plant with power during startup, during shutdown and during emergencies in a stable and continuous way.

6.3. The preferred power supply to the safety power systems is the supply from the grid. In power operation the power supply is normally from the main generator, connected to the grid. The generator will act as a stabilizer against voltage variations on the grid and can power the on-site power systems during house load operation.

6.4. The transmission system should be able to dispatch the energy from the nuclear power plant in a stable and continuous way.

6.5. This applies also after anticipated grid events when the plant remains connected to the grid.

6.6. The preferred power supply could also come from a separate connection to the grid. In order to minimize the risk for common cause failure caused by events on the grid, the switchyard or the main generator, it could be investigated whether the different divisions of the electrical power systems of the nuclear power plant could be connected to different preferred power supplies without a significantly increased risk of undue trips and other disturbances.

RELIABILITY OF PROTECTIVE DEVICES AND HIGH VOLTAGE EQUIPMENT

6.7. The design of the connection to the grid, the control circuits and the relay protection should be of high quality and should contribute to a reliable preferred power supply.

6.8. Events to be considered in the design of the grid connection and the relay protection include:

- Anticipated electrical events including loss of load and out of step scenarios;
- Anticipated electrical events during shutdown;
- Pollution of outdoor equipment;
- Geomagnetic storms;
- Events such as winding to winding faults in transformers and loss of one phase of the grid connection.

6.9. In areas with a high risk of pollution, an increased length of insulator may be necessary to ensure that insulator contamination does not pose a risk of common cause failure of off-site supplies.

OFF-SITE POWER SUPPLIES

6.10. The off-site power supply should have adequate capacity and capability to power plant loads in all modes of the nuclear power plant's operation.

6.11. It should be noted that voltage levels on the grid could be different when the plant is in shutdown mode.

6.12. The transmission system is the source of power to the on-site power system. The transmission system is also a significant contributor to defence in depth for the plant's safety design. The means for safe shut down of a nuclear power plant in transients and accidents, as well as normal shutdown, are more flexible and more reliable if off-site power is available. The power supply should therefore have adequate capacity and capability.

6.13. Off-site power should be supplied by two or more physically independent off-site supplies that are designed and located to minimize, to the extent practicable, the likelihood of their simultaneous failure.

6.14. The total number of transmission line connections to the electrical grid will depend on the capabilities of the entire grid and on the design of the nuclear power plant.

6.15. A single transmission line for each off-site power supply may be acceptable if the safety analysis report shows that this arrangement achieves the technical safety objectives as defined in SSR-2/1 [1]. For example, a single off-site power supply might be acceptable for reactors of a design that employs passive engineered safety features.

6.16. Nuclear power plants with a single transmission line might have a higher forced outage rate owing to line tripping. This should be taken into considered in particular in areas where the frequency of lightning strikes on the line is high. In such cases, the nuclear power plant may prematurely reach design thermal stress cycles unless the plant is designed to withstand the effects of the forced outages or unless measures are taken to reduce the number of forced outages, such as by means of additional transmission lines and a greater level of protection.

6.17. As a minimum, each off-site power supply should have the capacity and capability to power all electrical loads required to mitigate the consequences of all design basis accidents and anticipated operational occurrences.

6.18. Each off-site supply required for normal plant operation, startup and shutdown should have the additional capability to power all the normal electrical loads.

6.19. At multi-unit plants, each unit should be connected to two off-site power supplies such that the technical safety objectives as defined in SSR-2/1 [1] are fulfilled simultaneously for all units.

6.20. The off-site power supplies, provided to meet the recommendation of the above paragraph, may be shared among two or more plants or units, or they may have separately dedicated circuits.

6.21. For multi-unit plants, a single off-site power supply may be acceptable for some reactor designs if it is shown in the safety analyses report that one off-site power connection is sufficient.

6.22. Where off-site power supplies are shared between multiple units at a multi-unit plant, the ability to disconnect a unit should not affect the availability of the off-site supply to any other units.

AVAILABILITY

6.23. A minimum of one off-site circuit should be designed to be automatically available to provide power to its associated safety divisions within a few seconds in a design basis accident to be able to meet the requirements for accident analysis.

6.24. A second off-site circuit should be designed to be available within a short period of time.

6.25. The second circuit should preferably also be available within a few seconds in a design basis accident.

6.26. The transfer system for the auxiliary loads should be evaluated against the safety requirements for the design.

6.27. The transfer to the second circuit, both manually and automatically, should be easy to accomplish.

6.28. The transfer capability should only be used when necessary as switching between two live circuits could pose risks.

6.29. It is preferred to energize from the secondary circuit after a loss of voltage from the primary circuit. Interlocks between breakers may be used to preclude setting circuits in parallel that could result in adverse voltage or current conditions on common buses.

6.30. Variations in voltage and in-rush currents during the transfer should be considered in the design of the transfer sequence.

6.31. The more reliable power supply should be selected for use in normal operation of the plant.

6.32. Selection of the most reliable power supply for normal operation of the plant minimizes the transfer demands on switchgear.

6.33. Some nuclear power plants are designed for load rejection on separation from the transmission lines, and for the subsequent reduction of the reactor output and the generator power output to levels sufficient to meet the needs of the disconnected plant for electrical power (the house load) without tripping the steam supply or tripping the turbogenerator. This transfer to house load operation will result in frequency excursions and voltage excursions before stable operation is achieved.

6.34. In plants designed for house load operation, the on-site power system should be designed to accommodate the variations and transients of voltage and frequency from the generator when transferring from the normal source of supply to house load operation.

6.35. A generator circuit breaker may be used as a means to power the on-site AC power systems immediately from the off-site circuits following the tripping of a main generator. Generator load break switches can be used for this purpose, but the switchover will not be immediate.

INDEPENDENCE OF OFF-SITE CIRCUITS

6.36. Two off-site circuits should be designed and located to minimize, to the extent practicable, the likelihood of their simultaneous failure under all plant conditions and in design basis environmental conditions.

6.37. Examples of events that could cause simultaneous failure of both off-site circuits include:

- The use of a common take-off structure for both off-site circuits;
- Failure of a single breaker, switchyard bus cable or control power supply that could cause failure of both off-site circuits.

SWITCHYARD

6.38. The physical design of the switchyard should be such as to minimize the possibility that a single equipment failure will cause the failure of off-site circuits that are credited with supplying safety loads.

6.39. At least two supplies should not share the same control power source.

6.40. The switchyard control power should be unique to the switchyard and not be fed from the power supplies of the nuclear power plant.

6.41. Control circuits to outdoor switchyards should be equipped with overvoltage protection where they enter the plant and be isolated from the control circuits inside the plant.

6.42. Switchyard equipment should be designed to withstand the stresses of worst case faults.

6.43. Protective systems should minimize the probability of failure of both off-site circuits that are credited with supplying safety loads.

6.44. Design features suggested for consideration include:

- Primary and backup relay systems;
- Breaker failure relaying;
- Dual battery systems;
- Dual breaker trip coils.

GRID STABILITY AND RELIABILITY

6.45. The electrical grid should provide stable off-site power; that is, it should be capable of withstanding load variations without exceeding the specified voltage limits and frequency limits.

6.46. The grid should have enough running inertia to make certain that the loss of a big power generating unit, the trip of the nuclear power plant main generator or busbar faults in the grid do not jeopardize the stability of the grid.

6.47. The degree to which the grid can maintain an uninterrupted power supply to the nuclear power plant with sufficient capacity (i.e. voltage and frequency) is a measure of the reliability of the grid.

INTERFACE AND INTERACTION BETWEEN TRANSMISSION SYSTEM OPERATOR AND NUCLEAR POWER PLANT OPERATING ORGANIZATION

6.48. The nuclear power plant operating organization and the transmission system operator should determine and establish requirements for equipment interfaces and communication interfaces, including:

(a) Channels of communication;

(b) Operating procedures;

(c) Preferred corridors to supply energy to the nuclear power plant in shutdowns or in accident conditions;

(d) Feedback of operating experience;

(e) Coordination of planning for maintenance and outages;

(f) Requirements for maintenance;

(g) Coordination in circumstances and conditions arising from sustained degradation in voltage conditions at the plant that could necessitate manual disconnection of the off-site power supply by the nuclear power plant operating organization.

6.49. In many States the energy market is undergoing division of the electrical power system and the establishment of separate production companies, transmission companies and distribution companies.

6.50. A nuclear power plant requires particular coordination between the transmission system operator and the nuclear power plant operating organization for the purpose of ensuring safe plant operation and safe shutdown. This cooperation is based on the common goals of ensuring nuclear safety and ensuring the security of supply of the electrical power system. One or more transmission system operators can supply electrical power to the nuclear power plant.

6.51. Experience has shown that a formal agreement between the nuclear power plant and the transmission system operator on the coordination of planning, including the specification of responsibilities, is beneficial.

6.52. The nuclear power plant should notify the transmission system operator with regard to outages, modifications and maintenance activities as well as any changes to the design, configuration, operations, limits, electrical protection systems or capabilities of the plant that would affect the ability of the transmission system operator to meet the current requirements.

6.53. The transmission system operator should notify the nuclear power plant with regard to outages, modifications and maintenance activities that could affect the availability and reliability of the grid connection of the nuclear power plant. Examples of such activities are maintenance work in substations served by the transmission lines to the nuclear power plant.

6.54. The nuclear power plant operating organization should coordinate electrical protection schemes with the transmission system operator in order to maximize the availability of the plant and grid supply in case of grid faults.

6.55. This coordination also applies to plant or grid modifications that could influence the interaction between grid and plant.

6.56. The nuclear power plant operating organization should coordinate with the transmission system operator and validate the accuracy and conservatism of the post-trip voltages predicted by the online grid analyses tools.

6.57. The operating organization of the nuclear power plant should ensure that the licensing requirements and design requirements for the plant are understood by the transmission system operator in order to prevent challenges to nuclear safety from arising as a result of disturbances, transients or operating conditions affecting the transmission system.

6.58. Because of the need for secure grid connections to the nuclear power plant, it might be necessary to reach an agreement with the transmission system operator that the grid equipment (including control equipment and electrical protection equipment) in the nuclear power plant switchyard, and the transmission circuits that are connected to it, is maintained to a higher standard, or is tested or inspected more frequently, than for other grid equipment.

6.59. Note that structures, systems and components of the preferred power supply (e.g. switchyard or grid) that are not under the direct control of the plant operating organization and the nuclear regulatory body are nevertheless site characteristics that are required to ensure plant safety.

6.60. The preferred characteristics of the power supply that are essential to plant safety should be documented in the plant safety analysis and it should be ensured by the licensee that the power supply has these characteristics.

ASSESSMENT OF THE RELIABILITY OF GRID CONNECTIONS

6.61. Analyses should be performed on a regular basis to ensure that the nuclear power plant has adequate electrical power (at the correct voltage and frequency) from the grid and to assess the reliability of the grid connections.

6.62. Factors to be considered in such analyses include loss of generation by the nuclear power plant, loss of any other critical source of power generation, loss of power from a transmission system

element, and the failure rate of protective devices and transmission system breakers and other equipment.

6.63. Reference [14] gives additional background information on the integration of nuclear power plants and the power grid.

7. DESIGN GUIDELINES FOR ELECTRICAL SAFETY POWER SYSTEMS

GENERAL

7.1. Variations in voltage and frequency in the nuclear power plant's electrical power system in any mode of plant operation should not degrade the performance of any safety system equipment.

Anticipated electrical events

7.2. A systematic approach should be taken to identify the variations and transients in voltage and frequency on the safety classified buses that could result from events on the preferred power supply or events in any of the on-site electrical power systems, and to confirm the adequacy of the protection scheme.

7.3. Examples of anticipated electrical events to be considered are given in Section 5.

7.4. Standby power supplies used for on-site power systems will have variations in voltage and frequency during load sequencing.

7.5. The magnitude of these variations in voltage and frequency should not affect equipment that is starting, already sequenced or operating.

7.6. All modes of operation and both symmetrical and asymmetrical events should be considered in the analyses. An event could challenge different components in the electrical power systems, depending on rise time, fault time, amplitude or asymmetry.

Monitoring and switching of buses

7.7. Degradation of the preferred power supply of each safety power system bus (i.e. overvoltage, undervoltage, over frequency and under frequency) should be detected on the buses of the safety AC power systems.

7.8. Buses affected by degradation of the preferred power supply should be automatically disconnected from their power source if the degradation exceeds the levels specified in the design requirements.

7.9. After a bus is disconnected from a preferred power supply that has been degraded, the bus should automatically be connected directly to alternative sources in the following order:

(a) The alternative off-site power source;

(b) The standby power source for that division of the safety power system.

7.10. A time delay may be associated with the disconnection to allow the system to ride through minor disturbances.

7.11. The time delay should be supported by the assumptions made in the accident analyses.

7.12. It is preferred that two breakers be provided to disconnect each preferred power supply feed to a safety system bus (see, for example, Fig. 3).

7.13. If automatic connection to the alternative preferred power supply is not used, it should be shown that this arrangement is in accordance with the design criteria of the plant.

7.14. The parameters of the safety power systems — including the availabilities claimed in the design analysis — that are relevant to the safe operation of the plant in operational states and under design basis accident conditions should be identified and used in the establishment of operational limits and conditions for the plant.

7.15. Each division should have an independent detection and protection to disconnect the safety buses from the preferred power supply, to shed loads from the safety buses and to start the standby power sources in the event of degradation in voltage, degradation in frequency or loss of voltage.

7.16. The following recommendations apply to bus voltage and frequency monitoring and protection schemes for protection against degradation in voltage, degradation in frequency or loss of voltage:

(a) Bus voltage and frequency should be detected directly from the safety system buses to which the standby power sources are to be connected.

(b) Degradation in voltage or frequency should be alarmed in the main control room.

(c) Degradation in voltage or frequency to below acceptable limits should automatically disconnect the affected supply from the safety buses.

Two levels of voltage protection with different time delays are necessary: one level to detect loss of off-site power at the safety buses, and a second level to detect degradation in voltage.

(d) On sensing unacceptably high voltage on a preferred power supply, the affected preferred power supply should be automatically disconnected from the safety system buses:

- The set point and time delay should be coordinated with the overvoltage capability of connected equipment;
- The reset value of the monitoring equipment should be lower than the lowest anticipated operating range of voltage of the standby supply.

(e) Each scheme should monitor all three phases.

(f) Measuring circuits should be immune to harmonics.

(g) The protection system design should be redundant.

(h) Failures in the measuring circuits should not cause incorrect operation or prevent correct operation of the monitoring and protection scheme.

(i) The design should minimize unwanted disconnection of the preferred power supply.

The use of coincident logic and time delays to override transient conditions is a way to minimize unwanted disconnection.

(j) A capability should be provided for testing and calibration during power operation.

(k) Indications should be provided in the main control room for any bypasses incorporated into the design.

7.17. Voltage monitoring that is used only for alarms does not have to follow the recommendations of para. 7.16.

7.18. The undervoltage and time delay set points for degraded voltage protection should be determined on the basis of an analysis of the voltage requirements of the safety loads at all on-site distribution system levels.

7.19. Improper voltage protection logic can cause adverse effects on the safety systems and equipment such as spurious shedding of safety loads from the standby power sources and spurious separation of safety systems from off-site power due to normal motor starting transients.

DESIGN FOR RELIABILITY

Single failure criterion

7.20. SSR-2/1 Requirement 25 states that:

> "The single failure criterion shall be applied to each safety group incorporated in the plant design."

7.21. SSR-2/1 para. 5.39 states that:

> "Spurious action shall be considered to be one mode of failure when applying the concept to a safety group or safety system."

7.22. SSR-2/1 para. 5.40 states that:

> "The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event."

7.23. While SSR-2/1 [1] applies the single failure criterion only to safety systems, the application of concepts of the single failure criterion is a powerful technique for ensuring high functional reliability for any system.

7.24. Normally concepts such as redundancy, independence, testability, continuous monitoring, environmental qualification and maintainability are employed to achieve compliance with the single failure criterion.

7.25. Each safety group should perform all actions required to respond to a postulated initiating event in the presence of the following in combination:

(a) Any single detectable failure within the safety system;

(b) Any undetectable failures, i.e. any failure that cannot be detected by means of periodic testing, alarm or indication of anomalies;

(c) All failures caused by the single failure;

(d) All failures and spurious actions of systems that cause, or are caused by, the design basis event requiring the safety function;

(e) The removal from service or bypassing of part of the safety system for testing or maintenance that is allowed by the plant operational limits and conditions.

7.26. In justifying non-compliance with the single failure criterion, it is advisable to pay particular attention to the possibility of low frequency external hazards and to the long term availability of support systems that are necessary for the operation of power supplies.

7.27. Non-compliance with the single failure criterion should be exceptional and should be clearly justified in the safety analysis.

7.28. Non-compliance with the single failure criterion may be justified for:

- Very rare postulated initiating events;
- Very improbable consequences of postulated initiating events;
- Withdrawal from service of certain components for purposes of maintenance, repair or periodic testing, for limited periods of time;
- Features that are provided only for design extension conditions; and
- Postulated failures whose likelihood can be shown to be sufficiently remote as to be able to be discounted.

7.29. Reliability analysis, probabilistic assessment, operating experience, engineering judgement or a combination of these may be used to establish a basis for excluding a particular failure from consideration when applying the single failure criterion.

7.30. If the single failure criterion is not met during testing or maintenance activities, the time period during which the equipment is out of service should be evaluated for its significance and its potential impact on the core damage frequency.

7.31. The conditions in which the single failure criterion is not met in the case of maintenance, repair or testing should be consistent with the plant's operational limits and conditions.

7.32. Where compliance with the single failure criterion is not sufficient to meet reliability requirements, additional design features should be provided or modifications should be made to the design to ensure that the system meets the reliability requirements.

Completion of protective action

7.33. The safety power systems and their protective devices and automatic features should be designed so that, once initiated automatically or manually, the intended sequence of protective actions continues until completion.

7.34. Deliberate operator action should be required to return the safety power systems to normal standby conditions.

SAFETY STANDBY AC POWER SOURCES

General

7.35. SSR-2/1 Requirement 68 states that:

> "The emergency power supply at the nuclear power plant shall be capable of supplying the necessary power in anticipated operational occurrences and accident conditions, in the event of the loss of off-site power."

7.36. Standby AC power sources should consist of an electrical power generating unit complete with all auxiliaries and a dedicated separate and independent stored energy supply for both starting and running the prime mover.

7.37. The preferred approach is to have only one standby power source per division, avoiding the necessity of parallel operation of generators.

7.38. If multiple power sources per division are used, it should be demonstrated that this is a reliable configuration.

7.39. The standby power source should have sufficient capacity and capability to start and to continuously supply all loads in its division under the full range of conditions, including allowances for conditions such as:

(a) Loads that might operate at run-out conditions;

(b) Loads that might operate in an overload condition;

(c) Changes in load characteristics due to generator operation at the lower end or upper end of the allowable voltage and frequency ranges;

(d) Engine derating due, for example, to the higher temperature of the intake air, environmental conditions or the fuel temperature;

(e) Future load growth.

7.40. Diesel generators are specified to operate at a fixed voltage and frequency in the emergency mode of operation. In general, the steady state voltage and frequency are maintained within an allowable tolerance of ±2% relative to the specified value. When electric motors are subjected to voltages below their nominal rating, some of the characteristics will change slightly and the power consumption will increase.

7.41. The continuous rating of the standby source prime mover preferably allows 3000 to 4000 hours of continuous operation without major overhaul. A 10–15 % overload capacity for a minimum of two hours in a 24 hour period is typically provided. This provides assurance that the power source can handle the short time loading at the onset of an event when systems of engineered safety features are realigning for injection or cooling system operation and their pumps are operating in run-out conditions or with a higher flow than is assumed in thermohydraulic analyses. The thermohydraulic analyses are normally conservative in such a way that the expected power consumption of motors could be underestimated.

7.42. The capability of motor driven pumps to deliver required flows should be evaluated for generator operation at the lower end of the frequency range.

7.43. A variation in frequency affects the torque developed by motors.

7.44. It should be demonstrated that the standby power source could operate continuously for the required time period set out in the design bases without any stops for maintenance activities.

7.45. The standby AC power source should have an automatic start on loss of preferred power supply to the essential buses.

7.46. The standby AC power source may also have an automatic start on actuation of an emergency signal (without loss of power to the safety bus).

7.47. The times to start the standby AC power source and to connect loads to this source should be consistent with the assumptions on startup time made in the safety analysis.

7.48. On-site sources of fuel and other consumables (such as lubricating oil) should be sufficient to operate the standby power sources until off-site power supply can be restored.

7.49. Off-site sources of fuel and other consumables may be depended on if sources of replenishment are identified and if on-site sources are sufficient for the time required to replenish supplies. In most States, on-site sources are sized for one to two weeks of operation without replenishment from external sources.

7.50. Standby power sources should be independent of electrical power sources and power sources for instrumentation and control systems, other than those sources in their own division.

7.51. Instrumentation and control systems used for the starting, coupling, running and protection of a standby power source should be supplied by batteries within their own division.

7.52. Loss of the DC power source within the same division as the standby power source could lead to unavailability of the standby AC power source, but it would also cause loss of other functions in the division, thus making the standby AC supply in that division inoperable.

7.53. When batteries specifically dedicated to the standby power source are used, they should be subject to adequate surveillance to detect deterioration and failure, to the same extent as for any safety system battery.

7.54. Standby power sources should only be used for the period of time necessary to reconnect to reliable and stable preferred or alternative power supplies.

7.55. The use of standby power sources for peaking generation should not be allowed.

7.56. The safety power system may supply loads of lower safety classification (including loads not important to safety) provided that the independence requirements of this Safety Guide are met.

7.57. Equipment that is not safety classified should be automatically disconnected on an accident signal.

7.58. The isolation devices between a safety power system and equipment of lower safety classification should be part of the safety system.

7.59. The load sequencer should automatically shed all the non-safety loads and should not automatically start non-safety loads.

7.60. The load sequencer should only permit the start of non-safety loads after safety loads have been started and it has been determined that there is enough capacity for start and operation of the non-safety loads.

7.61. Transfer of a safety power system bus from its standby AC source to a preferred power source should require manual action.

7.62. When multiple safety power divisions are transferred from their standby power source to preferred power sources; only one division should be transferred at a time.

7.63. After a safety division is returned to the preferred power source, the associated standby AC power source should be made operable in normal standby conditions before transferring another division to the preferred power source.

Testing

7.64. Means should be provided for the periodic testing of standby power sources during plant operation.

7.65. The design of the test provisions should ensure that the standby power source can continue to perform its safety function during testing.

7.66. Arrangements for testing should neither compromise the independence of safety systems nor introduce the potential for common cause failures.

7.67. Examples of testing that either compromises the independence of safety systems or introduces the potential for common cause failures are the formation of soot in diesels being tested under no-load

conditions, inadequate provision for restoring to normal standby conditions after completion of the test or the introduction of human errors when testing redundant equipment.

Performance criteria (transient and dynamic)

7.68. The variations in voltage and frequency in power supplied from the standby AC power source should be shown to be within the design basis of the connected loads and the prime mover.

7.69. It is expected that voltage and frequency variations will remain within the range for continuous operation. Deviations outside the range during the loading sequence and for short time periods are permitted, provided that the voltage and frequency are restored well before the next load is connected and that the voltage on the motor terminals is sufficient for starting of the loads in each sequential step.

7.70. The performance of the standby power source during sequential loading, with continuous loads that would only occur in accident conditions, is usually determined by a mixture of testing and analyses.

Relay protection of standby power sources

7.71. Trip devices that protect the power supply from a standby power source against immediate catastrophic failure should be in service in all modes of operation of standby power sources.

7.72. Examples of such devices include those that:

- Protect the standby power source from catastrophic failures, such as overspeed protection and generator differential protection;
- Protect the safety power system from catastrophic failures, such as backup overcurrent protection and low impedance to ground fault protection.

7.73. Trip devices that protect the standby power source from non-catastrophic failures should be bypassed when the standby power source is supplying safety loads during emergency operation, but should be in service during normal operation and testing.

7.74. The design should provide for individual testing of each trip function and bypass function.

7.75. All protection trip actuations for the standby power source should be annunciated in the main control room.

Support systems for standby AC power sources

7.76. Support system equipment (e.g. ventilation systems, cooling water pumps and lubrication systems) for redundant division of the standby power sources should be supplied with power from the division it serves in order to preserve the redundancy and independence of the divisions.

7.77. The auxiliary systems and support systems of standby AC power sources should be sized for multiple starts.

7.78. Starting systems typically have the capacity to support at least five starts. In order to support this, it is usually necessary to abort any starting attempt after a specified time to preserve resources.

Fuel for standby AC power sources

7.79. It should be shown that fuel for standby AC power sources can be stored for long periods.

7.80. Fuel oil at a nuclear power plant is stored for extended periods. Some types of fuel are chemically unstable when stored for long periods. Fuel ageing and oxidation can lead to high acid content, high viscosity, and the formation of gums and sediments that clog filters. Degradation in fuel quality could cause a common cause failure of the standby AC power sources.

7.81. Every fuel delivery should be tested to verify that it meets specifications.

7.82. Samples for the testing of fuel will usually be taken on site.

DC POWER SYSTEMS

General

7.83. Each division of a DC safety power system should consist of at least one battery, one battery charger and a distribution system.

7.84. In order to have more flexibility for maintenance, two battery chargers and two parallel batteries are preferred in each division.

7.85. The connected DC loads should be rated for float voltage and equalizing voltage.

7.86. To have sufficient battery capacity the float voltage is higher than the nominal DC bus voltage and the end voltage after discharging is low.

Battery

7.87. Each battery set should, without a battery charger, be capable of meeting all required load demands and conditions (including duty cycles and electrical transients) that occur in the plant states specified in the design basis, with account taken of such factors as design margins, temperature effects, any recent discharge and deterioration with age.

7.88. The limiting case for battery capacity sizing is normally station blackout.

7.89. Ventilation should be provided in battery rooms to maintain the concentrations of combustible gases below prescribed levels.

7.90. If forced ventilation is necessary:

(a) The ventilation system for the battery room should be powered from the same division as the battery in the affected room;

(b) Hydrogen monitoring as a precautionary measure should be considered.

7.91. Batteries should be periodically tested to demonstrate the operability of the system and to detect any degradation.

7.92. Periodic testing will usually be based on recommendations for each type of battery and typically a battery capacity test at an interval of 1 to 5 years, depending upon the condition of the battery, as well as frequent verification of the following as applicable:

- Trickle charge current;
- Electrolyte level of each cell;
- Specific gravity of the electrolyte of a representative cell;
- Voltage of a representative cell;
- Temperature of a representative cell.

7.93. The temperature of the battery rooms should be monitored.

7.94. Battery capacity and battery lifetime are temperature dependent.

7.95. Battery fuses should be monitored.

Battery charger

7.96. Each battery should have its own battery charger.

7.97. Each battery charger should have sufficient capacity to do the following:

(a) To maintain the battery in a fully charged condition during normal operation;

(b) To restore the battery from a fully discharged condition to a minimum charged state within an acceptable period of time while at the same time supplying the highest combined demands of the various steady state loads and accident loads following loss of normal power.

7.98. When a rectifier is used as a power supply for an inverter it should be self-protected.

7.99. The power supply protection to be provided includes: reverse current protection, current limiting features or overload protection, and output undervoltage and overvoltage protection.

7.100. Each battery charger should shield its DC supply from transients on the AC system and should shield its AC supply from transients on the DC system.

7.101. Battery chargers should keep the output voltage within the operating range of the DC voltage under the following circumstances:

(a) When the AC input voltage goes low during clearing of faults on the supply side and returns to a high voltage:

For the clearing of faults on the transmission system close to the plant, the typical duration is 100–250 ms, and when faults happen in the on-site power system the typical duration is up to 100 ms. After a fault on the grid is cleared, the supply voltage will rise to a level determined by

the generator acting as the supply (see Fig. 6.) This voltage sag and swell with short rise time might cause severe overvoltage on the DC side of a battery charger.

An effective way for the battery chargers to keep the output voltage within the operating range of the DC voltage is to shut down automatically, with no time delay, the battery charger on AC undervoltage and to restart when the supply voltage is normal. This could shield the DC power systems (and the uninterruptible AC power systems) from voltage transients induced by grid events.

(b) In loss of load scenarios when the input voltage goes high:

The voltage rise will be determined by the previous active and reactive loading of the generator. The overvoltage will typically be 130–150% (see Fig. 7).

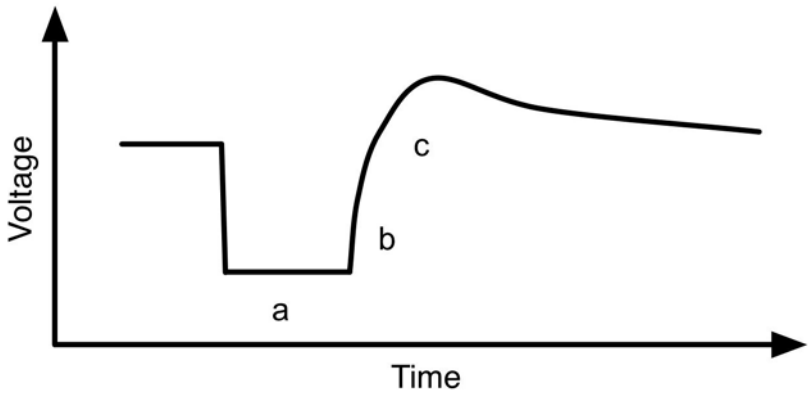


FIG. 6. Typical on-site voltage profile during clearing of a transmission system fault: (a) voltage during fault: (b) rapid voltage rise; (c) voltage swell due to generator excitation and return to normal voltage.

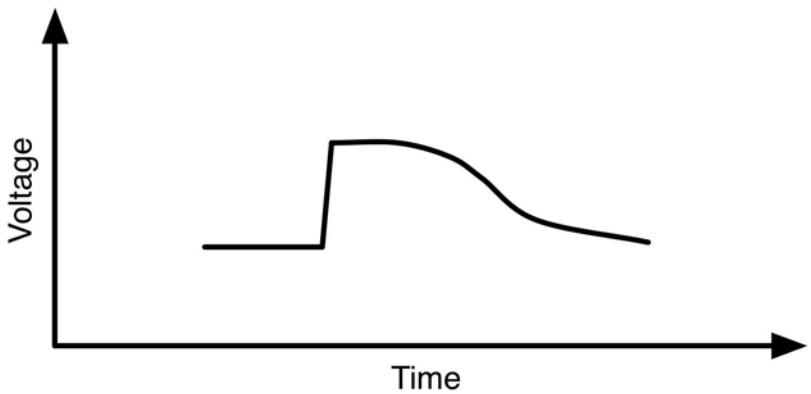


FIG. 7. Typical on-site voltage profile after loss of load (transfer to house load operation).

7.102. Battery chargers should be able to supply the loads without any battery connected.

7.103. The ability to supply DC loads directly from the battery charger is part of the diversity in power supply for DC systems. Operation in this mode is not normally expected.

7.104. Each battery charger should have disconnecting devices in the AC and DC circuits to enable the battery charger to be isolated.

Uninterruptible AC power system

7.105. Uninterruptible AC safety power systems should be provided where necessary to supply loads for equipment important to safety that requires continuous AC power.

7.106. Some plant designs will not need uninterruptible AC power systems. For modern instrumentation and control systems, it is feasible to power all loads requiring continuous power with DC power systems. Such an approach eliminates a source of failure.

7.107. Each division of an uninterruptible AC safety power system should consist of a power supply from a DC safety power system to an inverter, a power supply from the AC bus of the same division and a device for automatically switching between the two supplies.

7.108. Alternatively, the uninterruptible AC safety power supply may be in the form of an uninterruptible power supply with a dedicated battery charger, battery and inverter.

7.109. If an uninterruptible power supply is used, the recommendations and guidance given here for battery chargers and batteries also apply.

7.110. The electrical characteristics and the continuity of the uninterruptible AC power supply should meet the design requirements of the loads to be served by the system.

7.111. The limiting case for capacity is usually station blackout.

7.112. An uninterruptible power supply could withstand a perturbation in its output, such as voltage sag or an interruption to the cycle, provided that such a perturbation does not result in a loss of the required function of the equipment being served by the supply or in any undesired action by the equipment.

7.113. The design of uninterruptible power supplies should be consistent with the characteristics and design requirements of the loads and the interactions between loads connected to the uninterruptible AC power system.

7.114. For example, the design of static inverters should ensure that the voltage harmonics produced by the inverter itself, as well as by any non-sinusoidal loads, do not degrade the functions of the systems being supplied.

Protection of DC power systems and uninterruptible AC power system

7.115. Battery chargers, inverters and motor generator sets are sources of limited short circuit current. This will affect the sensitivity requirements for their protective devices.

7.116. The protection for battery chargers, inverters and motor generator sets should be coordinated with their associated alternative supplies, inverters, static switches, battery chargers, distribution panels, instrumentation panels and racks, and other equipment that they power.

7.117. The DC power systems and uninterruptible AC power system should be provided with undervoltage protection and overvoltage protection.

7.118. Ground detection monitoring should be provided for isolated (ungrounded) DC power systems.

7.119. The ground detection monitoring should give an alarm before the impedance to ground falls below a value at which any malfunction could occur.

7.120. The DC power distribution system should be provided with coordinated protection.

7.121. Coordination for DC power system circuits involves protective devices for the main bus and the protective devices used in branch circuits, in switchgear control circuits, in relay control panels and process control panels, and in battery chargers.

7.122. In performing coordination analysis of DC protective devices, appropriate correction factors or DC trip characteristic curves for protective devices should be used.

7.123. The uninterruptible AC safety power system should be provided with coordinated protection.

7.124. It is preferable that the inverter does not have an overvoltage protection on the DC side.

7.125. Coordination involves the main bus protective devices and the protective devices used in branch circuits.

7.126. The battery charger, the battery and the inverter (or the motor generator set) is a unique functional system because these elements create the ‘power supply chain’ for many uninterruptible loads and there are strong interactions among them. Consequently, properly coordinated protection settings will preserve the safety functions. For example, in the case of overvoltage on the AC supply to the battery charger, the battery charger will limit the transfer of the disturbance to the DC side to a level that would not cause trip of other safety loads — including the uninterruptible power supply itself.

7.127. Uninterruptible AC power systems should be provided with under frequency and over frequency protection.

8. ALTERNATE AC POWER SUPPLIES

8.1. An alternate AC power supply should be provided at or near the nuclear power plant if the plant’s design depends on AC power to bring the plant to a controlled state following loss of off-site power and safety standby power sources.

8.2. Alternate AC power supplies, including necessary connecting points, are provided to protect electrical power systems against the simultaneous failure of off-site and emergency AC power

supplies. This needs AC power sources that are diverse in design and are not susceptible to the events that caused the loss of on-site and off-site power sources.

8.3. The alternate AC power supplies with auxiliaries should be qualified for their intended application.

8.4. Alternate AC power supplies should have sufficient capacity to operate systems necessary for coping with a station blackout for the time required to bring the plant to a controlled state and to maintain it in a controlled state.

8.5. Ensuring that the alternate AC power supplies can cope with station blackout involves ensuring that the alternate supply is sufficient for simultaneous removal of reactor decay heat, ensuring primary circuit integrity and maintaining the reactor subcritical, and for removing decay heat from spent fuel for all units served for a period of time that is sufficient for reliable restoration of other power sources.

8.6. Units that have more than the required redundancy of standby AC power sources may use one of these sources as an alternate AC source, provided that it follows the other recommendations of this section.

8.7. If an alternate AC power source serves more than one unit at a site where safety standby AC power sources are shared between units, the alternate AC power source should have sufficient capacity to operate systems necessary for coping with a station blackout for the time required to bring all units that share the safety AC power sources to a controlled state and to maintain them in a controlled state.

8.8. The alternate AC power source for one unit should not normally be connected to the on-site power system of that unit.

8.9. Support systems that maintain the alternate AC source in readiness may be powered from one or more units, provided that this does not affect the operability of the alternate AC power source.

8.10. There should be a minimum potential for common cause failure of any safety standby AC power source and the alternate AC power source.

8.11. No single point of vulnerability should exist whereby weather related event, another external event or a single failure could disable any of a unit’s safety standby AC power supplies and simultaneously cause the failure of all off-site power supplies and the alternate AC power supplies.

8.12. Provision should be made for connecting the alternate AC power supply to one or all safety power system buses.

8.13. The safety power systems should be fed from the alternate AC power supply only after it has been disconnected from other power supplies.

8.14. Alternate AC power supplies should be capable of supplying the required loads within the time specified in the plant safety analysis and the plant station blackout coping analysis.

8.15. It is preferable that the alternate AC power supplies will be capable of supplying loads as soon as is reasonably practicable. Restoring AC power as soon as possible after a station blackout restores a degree of defence in depth to the electrical power systems, restores safety systems that depend on AC power and restores support systems (e.g. lighting systems and habitability systems) that significantly enhance the ability of the operators to respond to an event.

8.16. The alternate AC power supply may also have the capability to power loads necessary in design extension conditions.

8.17 The plant design should include the necessary features to enable the use of non-permanent power sources which may be available at the site or not.

8.18 Equipment necessary to mitigate the consequences of a core melt accident should be able to be supplied by any of the power sources.

9. CONFIRMATION AND DOCUMENTATION OF THE DESIGN

MANAGEMENT SYSTEM

9.1. The design of electrical power systems important to safety should be conducted within the framework of a management system that meets the requirements of GS-R-3 [15] and follows the recommendations of GS-G-3.1 [16] and GS-G-3.5 [17].

VERIFICATION

9.2. The capacity and capability required of electrical power systems should be determined by analysis and should be verified by tests (see Annex II).

9.3. As part of the design and design verification, the following demonstrations should be performed and each demonstration should be documented in a form suitable for auditing:

(a) Demonstration that the electrical power systems are capable of fulfilling their safety functions as set out in their design bases;

(b) Demonstration that the design requirements for electrical power systems are met;

(c) Demonstration that electrical safety power systems comply with the single failure criterion;

(d) Demonstration that electrical power systems meet design basis reliability requirements;

(e) Demonstration that the operation of protective devices has been adequately coordinated;

(f) Demonstration that adequate measures against station blackout are implemented;

(g) Demonstration that the reliability of off-site circuits credited with supplying safety loads meets and will continue to meet availability requirements after planned changes to transmission systems and generation facilities;

(h) Demonstration that the off-site circuits credited with supplying safety loads will continue to have their required capacity and capability with the occurrence of: the loss of the nuclear power plant; the loss of the largest generating unit; the loss of the largest

transmission circuit or intertie (interconnection permitting passage of current) between two or more electrical utility systems; or loss of the largest load.

(i) Demonstration that each off-site power supply has the capacity and capability to power all electrical loads required to mitigate the consequences of all anticipated operational occurrences and design basis accidents.

9.4. The demonstrations should cover all modes of operation of the nuclear power plant.

9.5. The demonstration of the reliability and availability of the off-site circuits should be performed together with the transmission system operator (see Section 6).

9.6. For all systems important to safety, a systematic assessment should be conducted to confirm that the reliability requirements of the design basis for the systems are achieved in the design.

9.7. This confirmation by systematic assessment for all systems important to safety may be based on a balance of application of deterministic criteria and use of quantitative reliability analysis in which design features such as, for example, redundancy testability, failure modes and rigour of qualification are considered.

9.8. The use of software or complex multi-element logic modules could cause difficulties in the confirmation of reliability and sensitivity to common cause failures. The confirmation of reliability may therefore depend on assurances of freedom from error in the design and implementation process. Reference [2] provides recommendations and guidance on this subject.

9.9. Test facilities that are part of the safety system should be considered in determining the availability of systems.

9.10. Analytical tools used in the design and analysis of electrical power systems should be qualified and the validity of the mathematical models should be justified on the basis of experimental data or operating experience.

9.11. The analyses recommend in paras 9.2–9.10 are part of the plant safety assessment. GSR Part 4 [18] establishes requirements on safety assessment.

Testing

9.12. Provisions should be made in the design to ensure that the following test programmes can be conducted without jeopardizing the safety of the plant during testing:

(a) A pre-operational test programme to demonstrate operation in all system modes (e.g. operational states and emergency conditions) to the extent practicable, to prove that the design requirements have been met and to establish that each division is independent of other divisions.

(b) A test programme during operation that provides adequate assurance of the readiness of the systems to function upon demand.

(c) Periodic test procedures to demonstrate the continuing operability of the system and to detect and identify any degradation of the system or degradation of components within the system.

9.13. General recommendations on measures for verifying the adequacy of the design are provided in GS-G-3.5 [17] paras 5.114–5.134.

9.14. A major consideration in pre-operational test programmes for electrical power systems in nuclear power plants is to confirm, before entering into operation and after major modifications, the independence of the divisions of the safety power systems. Usually this involves testing to verify that all on-site power systems and their load groups can successfully operate and are in no way affected by the partial or complete failure of any other power source in other divisions.

DESIGN DOCUMENTATION

9.15. Documentation of the electrical power systems should include the documentation of:

(a) Design bases;

(b) A description of the overall power supply system including:

1. Details of how the nuclear power plant is connected to the grid;
2. An explanation of the degree of redundancy of the electrical safety power system;
3. Identification of interfaces with the auxiliary systems;

(c) A description of the separation criteria for installing equipment, cables and raceways, including wiring and components inside panels;

(d) One-line diagrams, functional control diagrams, schematic diagrams, connection diagrams, panel wiring diagrams and descriptions of systems;

(e) Layout plans for the on-site electrical power system together with the arrangements of equipment and associated support systems;

(f) Layout plans of cable routes, including trays, ducts and conduits, throughout the plant and identification of redundant divisions and cables and their routing;

(g) Raceway schedules showing cables contained in each raceway segment and the fill percentage of each segment;

(h) Circuit schedules identifying for each field cable its connection points, cable type and routing through the raceway system;

(i) An electrical load analysis showing the inventory of electrical loads and for electrical safety power systems showing a time dependent loading from which the capabilities of the necessary components of the power systems are calculated;

(j) Operating procedures and maintenance manuals for electrical power systems and equipment;

(k) Periodic testing and maintenance requirements for electrical power systems and equipment;

(l) Documentation of acceptance tests and commissioning tests for electrical power systems and equipment;

(m) Quality management records;

(n) Analysis of voltage and frequency transients, short circuit calculations and voltage drop calculations:

1. From the grid during power operation;
2. From the on-site electrical distribution system;
3. From the grid during shutdown;
4. From the main generator.

(o) Studies of steady state load and voltage profile studies that show the voltages throughout the power system for various modes of plant operation (and generator load to power factor), including design basis events, under normal conditions and under conditions of degradation in voltage;

(p) Transient load and voltage studies that show the profile of the loads that are sequentially applied to the preferred power supplies and standby power supplies in various modes of plant operation;

(q) A bus transfer study that analyses the effects of voltage, phase angle and frequency, and the effects of motor reacceleration on buses and motors before, during and immediately after automatic bus transfers;

(r) Short circuit studies to determine the maximum and minimum fault currents throughout the power system for various modes of plant operation, including design basis events, for use in analysing the fault clearing capability of the electrical equipment;

(s) Studies of coordination of protective devices and studies of equipment protection that show proper set point selection in all of the protection schemes;

(t) Analysis of fuel storage capacities for standby power sources;

(u) Analysis of the consequences of partial or total loss of power supplies;

(v) Equipment qualification plans, analyses and test reports;

(w) Specifications for electrical power components.

REFERENCES

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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series, IAEA, Vienna (in preparation). [[DS431]]

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 13 (INFCIRC/225/Revision 5), Vienna (2011).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series, IAEA, Vienna (in preparation). [[DS367]]

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards Other than Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.11, IAEA, Vienna (2004).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.12, IAEA, Vienna (2009).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, The Operating Organization for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.4, IAEA, Vienna (2002).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.6, IAEA, Vienna (2001).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Conduct of Operations at Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.14, IAEA, Vienna (2008).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Electric Grid Reliability and Interface with Nuclear Power Plants, D-NG-T-3.8, Vienna (2012).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Application for the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, Safety Standards GS-G-3.5, IAEA, Vienna (2009).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4, IAEA, Vienna (2009).

[19] Nuclear Energy Agency, Defence in Depth in Electrical Systems and Grid Interaction, Final DIDELSYS Task Group Report, NEA/CSNI/R (2009)10, Paris (2009).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, IAEA, Vienna (2007).

ANNEX I
DEFENCE IN DEPTH IN ELECTRICAL POWER SYSTEMS

I-1. Nuclear power plants rely on electrical power for various safety functions and the reliability of the power supplies are important for the safety of the plant. Owing to the design of electrical power systems, all parts of the systems are normally connected regardless of their safety classification.

I-2. The electrical power systems are support systems necessary for all levels of defence in depth. It is essential that the plant have a reliable power supply to control anticipated deviations from normal operation as well as to power, control and monitor the plant during events of all types that challenge the barriers against radioactive releases and also in design extension conditions.

I-3. Any electrical event or disturbance that happens in the electrical power systems has to be handled in such a manner that the safety functions of the power plant can be fulfilled.

I-4. Operating experience shows that loss of transmission systems or failures in the on-site power systems could jeopardize the safety of the plant, as described in Ref. [19].

I-5. Many overlapping system characteristics that are provided to obtain reliable and robust electrical power systems form the different levels of defence in depth. These system characteristics cover grid systems and on-site systems, both important to safety and not important to safety. Even though more stringent criteria are applied to safety power systems and more verification is necessary, the entire on-site and off-site power systems contribute to the reliability and robustness of safety power systems.

I-6. Support features for the electrical power systems are control and monitoring, part of the main control room and supplementary control room complex, and procedures for operation of power systems in all plant states and electrical events.

I-7. Table I-1 summarizes the features of the electrical power systems that support the levels of defence in depth as stated in SSR-2/1 [1].

FIRST LEVEL OF DEFENCE IN DEPTH

Design bases

I-8. The design bases for the on-site electrical power systems are the fundamental basis for reliability and robustness. The design bases account for the continuous operating ranges of voltage and frequency, all possible events that could cause transient, dynamic or continuous variations of these, and internal and external hazards that jeopardize the availability of the power supply to the plant. As a nuclear power plant is a power generating facility, the voltage and frequency excursions that arise from different events will be different from those caused by conventional industrial events. Figure I-1 shows an example of voltage variations and frequency variations that will affect the on-site power systems in a nuclear power generating unit during anticipated operational occurrences.

I-9. Incomplete design bases, resulting in equipment not qualified for the intended function, cannot be rectified by redundancy or diversity.

TABLE I-1. SUPPORT OF THE ELECTRICAL POWER SUPPLY FOR THE DEFENCE IN DEPTH OF THE PLANT

Levels of defence in depth	Objective [SSR 2/1]	Essential means [SSR 2/1]	Applied to plant electrical power systems	Guidance in this Safety Guide Section
1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Comprehensive design bases, robust and reliable grid, robust and reliable on-site power systems	4 Design bases 5 General design guidelines 6 Design guidelines for preferred power supplies
2	Control of abnormal operation and detection of failures	Control systems, limiting systems and protection systems and other surveillance features	Robust and reliable fault clearing system and coordination of protection, power supply transfer capability, house-load operation possibilities	5 Design for reliability 6 Design guidelines for preferred power supplies
3	Control of accidents within the design basis	Engineered safety features and accident procedures	Robust and reliable safety power systems, robust and reliable on-site standby AC power supplies	7 Design guidelines for electrical safety power systems
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of design extension conditions	Complementary measures and accident management	Robust and reliable alternate AC power supply	7 Design guidelines for electrical safety power systems 8 Alternate AC power supplies
5	Mitigation of radiological consequences of significant radioactive releases	Off-site emergency response	(Not covered in this Safety Guide)	

The grid

I-10. The grid is part of the preferred power supply for the nuclear power plant and the safety power systems. During power operation, the power supply to the plant is normally provided from the generator, which will dampen variations arising from the grid.

I-11. The grid has to provide stable off-site power; that is, it needs to be capable of withstanding load variations and anticipated operational occurrences on the transmission system without exceeding the specified voltage limits and frequency limits. More information on the integration of nuclear power plants and the grid is provided in Ref. [14].

On-site power systems

I-12. The on-site power systems are linked together and an electrical event on a non-safety bus will in most cases also affect the safety power systems. A reliable on-site 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 (environmental and electrical) of equipment as well as equipment specifications based on the plant design bases also contribute. Good housekeeping will lessen the risk of faults and a proper understanding of load behaviour will minimize the risk for overload of rotating equipment.

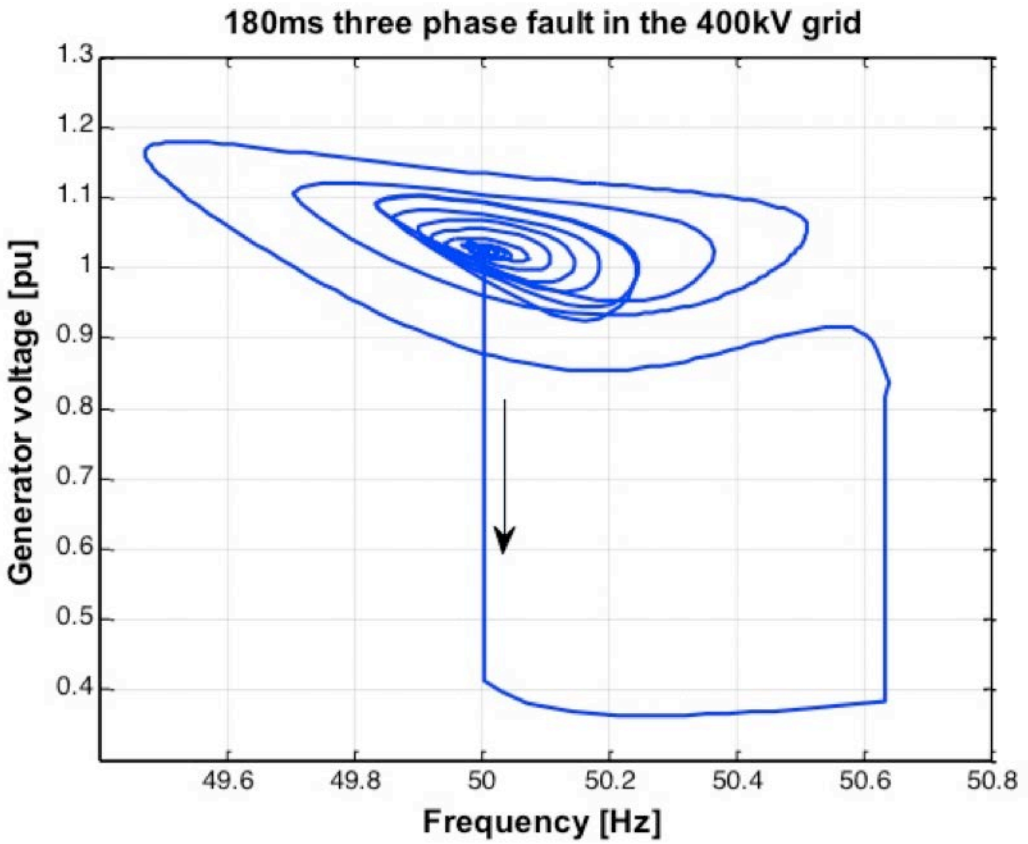


FIG. I-1. Example of variations in on-site generator voltage (y-axis) and in frequency (x-axis) during clearing of a fault on the transmission system.

I-13. The deterministic analyses to design and verify the reliable and robust on-site system are part of the safety justification for the nuclear power plant.

I-14. The robustness and reliability of the on-site power systems need to be analysed for all plant configurations, including those where part of the electrical power system may be taken out of service, such as refuelling outages.

I-15. The possibility of common cause failures cannot be ruled out, as in normal operation redundant divisions of the safety power system are connected to a common preferred power supply. Preventive measures such as diversity in power supplies (normally a built-in feature by design) are essential.

I-16. Maintenance programmes and procedures aim for the highest standards, not only for safety systems but for all parts of the on-site electrical power systems. Surveillance testing or performance testing is one way of following any degradation of equipment.

I-17. Plant modifications usually have an impact on the electrical power systems. Changes in loads and load behaviour have to be evaluated. This includes changes in control systems as such changes might affect battery loading.

I-18. Power supplies for lighting and telecommunication play an important role in coping with operational disturbances and events, although they are not generally classified as important to safety.

SECOND LEVEL OF DEFENCE IN DEPTH

Fault clearing system and coordination of protection

I-19. In order to minimize the effects of any faults in the electrical power systems, coordination of protection and fault clearing systems are provided that will disconnect only the faulted equipment. Backup features are also provided for the event that a primary protection feature or a fault clearing device fails.

I-20. Since battery chargers, inverters and motor generator sets are generally sources of limited short circuit current, coordination of protective devices and available fault current receives special attention.

I-21. Coordination of protection is designed to work properly both during power operation and during shutdown conditions.

Power transfer capability

I-22. Off-site power is normally supplied by at least two physically independent off-site circuits designed and located to minimize, to the extent practicable, the likelihood of their simultaneous failure. For some reactor designs (usually designs with passive safety features) it might be shown in the safety analyses report that one off-site power connection is sufficient.

I-23. One of these connections is designed to be available within a few cycles following a loss of coolant accident to ensure that core cooling, containment integrity and other vital safety functions are maintained.

I-24. The transfer to the other off-site circuit is normally automatic but provisions are made to initiate the transfer either manually or automatically. Studies are performed to analyse the impact of voltage, phase angle and frequency on buses and motors before, during and immediately after a bus is transferred. Also, reacceleration of motors has to be considered in the study.

I-25. The supply of uninterruptible AC power systems will also involve provisions to transfer the electrical power supply from one source to another.

Possibilities for house load operation

I-26. Some plants are designed to have the capability to withstand load rejection without undergoing a reactor trip or a turbogenerator trip, so as to continue to supply the house load.

I-27. The transfer to house load is complex owing to reactivity feedback and control of the power decrease. Experience shows that if the initial transient can be accommodated, operation can be continued for several hours; this adds diversity to power supplies for the plant.

I-28. To achieve house load operation, circuit breakers are necessary to separate the plant generator from the grid. This arrangement provides continuous power, either from the plant's turbogenerator or from the grid, in all conditions except those in which faults occur between the circuit breakers or in which there are coincident faults in the plant generator and in the grid.

THIRD LEVEL OF DEFENCE IN DEPTH

On-site standby AC power supplies

I-29. The safety systems of a nuclear power plant normally operate from the preferred power supply (i.e. the grid or the main generator) or from the on-site standby AC power supply.

I-30. The operability of the standby AC supplies has to be regularly verified. Testing of the starting capability of the standby AC power source is usually designed in such a manner that the test does not have negative effects on the long term availability of the power source.

I-31. Verification of the starting capability and the loading capability of the standby AC power sources usually has to be a combination of tests and analysis to capture design basis events.

I-32. Loads other than safety system loads may derive their electrical power from the safety power system. These loads are not automatically started after a loss of off-site power as they could affect the availability of the safety loads. The non-safety loads may only be started after it has been determined that there is enough capacity and capability for their starting and operation.

I-33. If an external hazard could jeopardize the first and second level of defence in depth in electrical power systems (e.g. grid connections and house load), the on-site standby AC power supplies have to be protected against such a hazard. Proper precautions will be based on the criteria considered in NS-G-1.5 [8] and NS-G-1.6 [7].

Safety power systems

I-34. The safety power systems that supply different loads are of utmost importance for the capability of the nuclear power plant to withstand a wide range of initiating events that could challenge the barriers to the release of radioactive material from the plant.

I-35. Events on the electrical power systems with origins from preferred power supplies can cause common cause failures on all divisions. Adequate countermeasures are therefore essential during design, construction, and operation. After loss of preferred power supplies, when the standby AC power sources supply one division each, the risk for common cause failures from electrical events is negligible as there are no common parts (although the starting sequence of the standby source is sensitive to common cause failure). Experience shows that incomplete design bases are the dominating contributor to common cause failure, in which case diversity of components does not lessen the risk.

I-36. Common cause failure for identical components can be screened out if:

- They perform different functions (one breaker in one system has to close, one breaker in the other system has to open); or
- They have different modes of operation (one of two parallel rectifiers is in operation, the other is switched off).

Common cause failure due to electrical events is not postulated for passive equipment such as bus bars, cables and transformers.

I-37. The DC systems are essential for the reliability of the safety power systems, as well as for the reliability of any other on-site or off-site power system. A rule is not to transmit any disturbances on the preferred power supply, with origin off the site or from the generator as a result of an off-site disturbance, to the DC power systems and consequently to the uninterruptible AC power systems. This is expected to be part of the design bases and can be achieved by means of design or protective devices.

I-38. In order to withstand the risks of common cause failure for electronic protective devices, the same design criteria are used as for instrumentation and control equipment [2].

I-39. Part of the equipment specifications for electrical loads will be the operating range of voltage and frequency for the electrical power systems, but knowledge of electrical transients and their impacts on the loads is also essential. Understanding of the mechanical load is necessary in order to determine the load range and power consumption for different modes of operation. This will give the proper sizing of standby power sources and the proper setting of protective devices.

Alternate AC power supply

I-40. The dependence on electrical power for safety functions in a nuclear power plant implies that also station blackout scenarios have to be considered. Consideration of station blackout involves determining the time period for which a plant can withstand the loss of all AC power and making provisions to connect an alternate AC power supply to the plant before the end of that period.

I-41. Precautions are necessary to ensure that this alternate AC power supply is available and accessible to withstand external hazards and that it can be connected to the plant within the given time period after an earthquake or a tsunami or during flooding or a storm, for example.

I-42. The alternate AC power source has to be as independent as possible of the other power sources from which the safety power systems can be supplied.

REFERENCES TO ANNEX I

[I-1] NUCLEAR ENERGY AGENCY, Defence in Depth in Electrical Systems and Grid Interaction, Final DIDELSYS Task Group Report, NEA/CSNI/R (2009)10, Paris (2009).

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

[I-3] INTERNATIONAL ATOMIC ENERGY AGENCY, Electric Grid Reliability and Interface with Nuclear Power Plants, D-NG-T-3.8, Vienna (2012).

[I-4] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003).

[I-5] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).

[I-6] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series, IAEA, Vienna (in preparation). [[DS431]]

ANNEX II
ANALYSES OF ELECTRICAL POWER SYSTEMS FOR VERIFICATION OF DESIGN

II-1. Analytical studies are made to demonstrate design margins and the robustness of the electrical power systems in a nuclear power plant. The analyses and design capabilities have to be verified and validated by testing or from operating experience. Annex II describes some of the key elements of electrical power system design that are normally performed as part of the power system analyses. The need for analyses applies to both AC systems and DC systems, but many of the specific topics mentioned apply only to AC systems.

STUDIES OF LOAD FLOW

II-2. Load flow analysis is an important part of power system studies since it evaluates the network in its normal operating conditions and in emergency operating conditions, and establishes the bounding limits. Load flow studies are performed using computer software that simulates actual steady state operating conditions for power systems, enabling the evaluation of bus voltage amplitude and load angle, active and reactive power flow, and losses. Conducting a load flow study using multiple scenarios helps to ensure that the power system is adequately designed to satisfy performance criteria. Specifically, load flow studies are commonly used to investigate the following:

- Component or circuit loading;
- Bus voltage amplitude and load angle;
- Active and reactive power flow;
- Power system losses;
- Proper transformer tap settings;
- Bounding limits for system operation;
- Bus transfer schemes;
- Optimization of circuit usage;
- Practical voltage profiles for postulated conditions;
- Equipment specification guidelines.

II-3. The following general criteria for design are typically considered acceptable when used in power flow studies:

- Steady state voltage drop at all buses to be within +/-5% of the nominal rating for all operating conditions considered;
- Transient state voltage variation > 5% may be acceptable when sequencing loads;

– Electrical circuits are not overloaded for any postulated operating condition;

– Reactive power flows (generation, import and export) are within the specified limits for all operating conditions;

- In specified contingency conditions, the power quality is not degraded.
- Harmonic content is within set limits.

II-4. The following study cases are specifically considered in power flow studies:

– Extreme operating conditions of maximum and minimum loading conditions to check the adequacy of the on-site and off-site power sources, in normal operation and in plant shutdown mode.

– Contingency conditions such as outage of lines, transformers and generators for the off-site power supply coupled with minimum and maximum loading of plant auxiliary systems, including equipment required to mitigate the radiologial consequences of an incident.

– Optimization of plant operating parameters such as transformer taps, generator excitation limits, reactive power compensations and cable sizing.

– Large motor starts: the starting current of most AC motors when starting them directly on line at full rated voltage is several times larger than normal full load current. Excessive starting current results in a drop in the terminal voltage and may result in failure of the motor in starting due to low starting torques, unnecessary operation of undervoltage relays or stalling of other running motors connected to the network. Motor starting studies can help in the selection of the best method of starting, the proper motor design and the proper system design for minimizing the impact of the motor starting. This study may have to be re-evaluated after the replacement of motors, depending on motor characteristics.

STUDIES OF SHORT CIRCUITS

II-5. Short circuit calculations provide currents and voltages on a power system in fault conditions. This information is required to design an adequate protective relaying system; to determine the interrupting requirements for circuit breakers at each voltage level under maximum fault current levels; and to verify timely fault clearance with enough available fault current to operate protective relaying by protective devices. The combination of timely fault isolation and coordination of protection provide for stable operation of the electrical power system of the nuclear power plant. Fault contributions from all operating sources at any given time have to be considered. Nuclear power plants have large motors that can provide a significant contribution to the available fault current in the plant power system. The short circuit calculations have to be confirmed when major replacements and major modifications of the electrical power system (on-site or off-site) are made and a cumulative evaluation has to be performed periodically.

II-6. Fault conditions can be balanced or unbalanced shunt faults or series (open conductor) faults. Faults may be caused either by short circuits to ground or between live conductors, or by broken conductors in one or more phases.

II-7. Fault studies have to be updated when major replacements and major modifications of the electrical power system (on-site or off-site) are made, and a cumulative evaluation has to be performed periodically (e.g. as a part of a periodic safety review).

STUDIES OF COORDINATION OF ELECTRICAL PROTECTION

II-8. A short circuit study and/or a coordination study establishes the magnitude of currents flowing throughout the power system at various time intervals after a fault occurs and evaluates the size and settings of a system's protective devices, such as relays, fuses and circuit breakers, and of the circuits that they protect. The goal is to provide power transformers, switchgear, motor control centres, distribution panels and other electrical equipment with the required protection. The study is also useful in selecting appropriate types, ampere ratings and device settings to ensure selective and rapid interruption of circuits under overload conditions and short circuit conditions so as to minimize the isolation of essential equipment.

II-9. Protective relays are designed to rapidly actuate equipment that is used to isolate the faulted part of the system so as to prevent damage to equipment and, with minimum disruption to the system, to ensure the continuity of power supply to unaffected parts of the power systems. When relays designed to protect specific equipment such as containment penetrations are postulated to fail, or primary zones do not operate to clear the fault in their primary protection zone, backup relays have to isolate the fault, after providing sufficient time for the operation of the protective relays for the primary zone. The protective relays also have to discriminate between faulted conditions, normal operating conditions and conditions of abnormal operation and have to function for the specific protection for which they are designed. Relay coordination calculations consider the operating characteristics of the relays, normal operating and withstand characteristics of plant equipment and determine the optimum relay settings to achieve high reliability of the electrical systems.

II-10. Protective systems have to provide protection against 'thermal withstand' limits, motor stalling, negative sequence and direct current withstand limits, protection against abnormal frequencies, and protection against unbalance operating conditions as applicable to various plant components and operating situations. Protection coordination also includes measuring principles.

II-11. Typical studies of protective relays cover:

- Overload phase relays;
- Overcurrent phase fault relays;
- Ground fault relays;
- Coordination with maximum load current;

– Coordination with fuse characteristics;

– Coordination with maximum motor starting current and time;

– Coordination with transformer in-rush current;

– Coordination with reacceleration currents;

– Coordination with primary back-up pairs;

– Coordination with ‘thermal withstand’ capabilities;

– Coordination with safe stall limits for motors.

II-12. Ground fault protection requires unique consideration since the magnitudes of fault currents depend on the method of grounding the system: solidly grounded systems or low impedance grounded systems may have high levels of ground fault currents. These high levels typically require fast tripping to remove the fault from the system. Ground overcurrent and directional overcurrent relays are the typical solution for protection against ground faults for such systems. Detection of high impedance ground faults is difficult as special relays are necessary to measure the ground fault current combined with the unbalance current generated by line phasing and configuration and load unbalance.

STUDIES OF LOSS OF VOLTAGE AND DEGRADED VOLTAGE

II-13. In addition to protection schemes discussed above, safety equipment at nuclear power plants is protected from a complete loss of preferred power (loss of voltage relay) to the safety buses and also from sustained degraded voltage conditions on the preferred power supply which could lead to malfunctioning or could cause damage to safety significant equipment.

II-14. Equipment that is considered important to safety has to be protected against two types of low voltage event:

– Equipment important to safety has to be protected against a loss of voltage event that implies a sudden sharp voltage drop in the grid system. Typically a nominal delay is allowed for relay actuation to separate on-site buses from the grid if the voltage does not recover to the normal operating band. Loss of voltage will also result in an automatic start signal to the on-site standby power sources.

- Equipment important to safety also has to be protected against degraded voltage that involves sustained low voltage conditions for several seconds and subsequent recovery to normal operating band. If the off-site power system does not recover to nominal operating conditions, it is preferable to separate from the source.

The degraded voltage condition occurs in transmission systems that are overloaded due to generation deficiency caused by loss of a generating unit, unexpected system loads, loss of a transmission element or system faults. This protective scheme requires additional plant specific considerations. General approach is outlined below:

– The voltage drop and/or load flow studies done for evaluating the off-site power and the on-site power system interface use the minimum expected voltage at the plant–grid interface

node, demonstrating an adequate voltage for the starting and running of plant components in normal conditions, anticipated operational occurrences and accident conditions.

– The selection of voltage and time delay set points are determined from an analysis of the operating voltage requirements of the safety significant loads at all on-site system distribution levels.

– The time delay is selected on the basis of the following conditions:

- The allowable time delay, including a margin that does not exceed the maximum time delay that is assumed in the accident analyses;
- The time delay has to override the effect of expected short duration grid disturbances, preserving the availability of the off-site power supplies;
- The time duration of conditions of degradation in voltage at all levels of the distribution system that will not result in failure of safety systems or components.

II-15. A typical scheme for degraded voltage relay involves two separate time delay relays to deal with the following conditions:

- The duration of the first time delay is sufficient to establish the existence of sustained degraded voltage condition (i.e. something longer than a transient due to a motor starting). Following this delay, an alarm in the control room alerts the control room operators to the degraded condition. The subsequent occurrence of an accident signal immediately separates the safety distribution system from the off-site power system.

– The duration of the second time delay is selected to be less than the duration of a sustained that would damage the permanently connected safety loads. Following this delay, if adequate voltages have not been restored, the safety distribution system is automatically or manually (by operator action) separated from the off-site power system.

STUDIES OF STABILITY TO TRANSIENTS

II-16. By its nature, an electrical power system is continually experiencing disturbances. These disturbances may include loss of production, short circuits caused by lightning or other fault conditions, sudden large load changes, or a combination of such events. Such disturbances may lead to a change in the configuration of the power system. Studies of the stability of a power system to transients are necessary to determine whether the system will remain stable or not after such major disturbances. The assumed critical fault clearing time[3] with a given configuration of the off-site power system will be different for various fault conditions. This critical fault clearing time may be specified and described in the safety analysis report for the nuclear power plant. The recovery of a power system subjected to a severe large disturbance is of importance to the reliable and safe operation of a plant. Typically the system has to be designed and operated in such a way that a specified number of

[3] The 'critical fault clearing time' is the maximum fault duration for which a system remains stable.

credible contingencies do not result in failure of the quality and continuity of the power supply to the loads. This requires accurate calculation of the dynamic behaviour of the system, which includes the electromechanical dynamic characteristics of the rotating machines, generator controls, reactive power compensators, loads, protective systems and other controls. The degree of stability of the system is an important factor in establishing the operating characteristics of the grid system in the vicinity of the nuclear power plant. Grid perturbations that lead to a loss of synchronism of the power system require the separation of the disturbance in a rapid manner to avoid damage to equipment or loss of stability of the system.

II-17. Parameters that can affect stability to transients include:

- Synchronous machine parameters;
- Impedance of the generator step-up transformer;
- Inertia of the turbogenerator;
- Transmission line parameters;
- Circuit breaker and relay characteristics;
- System layout;
- Excitation system, power system stabilizer and generator governor characteristics;
- System grounding;
- System controls such as auto-reclosing of circuit breakers, single pole switching, load shedding and system inertia.

II-18. Typically, analysis of stability to transients involves:

- Modelling generators in accordance with their steady state, transient and sub-transient parameters;
- Simulating transient behaviour for three phase faults or line to ground faults;
- Modelling motor and motor load torque, slip, current and acceleration curves;
- Simulating generator startups and motor startups;
- Modelling trip and close of circuit breakers, open and close of switches, and actions of relays based on the settings;
- Plotting generator and motor speed, current, voltage and power curves after postulated disturbances.

II-19. Breaker operating characteristics, synchronous machine behaviour and system interconnections can be optimized using computer based transient stability analysis.

STUDIES OF LIGHTNING PROTECTION SYSTEMS AND SYSTEM GROUNDING

II-20. A lightning protection system is a system designed to protect a structure from damage due to lightning strikes by intercepting such strikes and safely passing their extremely high voltage currents to ground. The voltage from a lightning strike rises very rapidly, typically rising to its peak in a few millionths of a second. The energy from a lightning strike has to be returned to ground very quickly through a low impedance path to prevent equipment damage and injury of personnel.

II-21. Most external systems for lightning protection consist of an air terminal, a down conductor and a grounding terminal, including a network of lightning rods, metal conductors and ground electrodes connected to the plant ground mat to provide a low resistance path to ground for lightning strikes. The internal system for lightning protection will include lightning equipotential bonding, electrical insulation of the external system and a surge protection device.

II-22. In any power generating plant there are generally four conceptually identifiable different, but not necessarily physically distinct, grounding systems: for personnel safety, lightning grounding, electrical power systems and instrumentation and control systems — including signal grounding. All grounding systems are tied to one grounding grid.

II-23. Typically, international standards recommend that the resistance of the grounding electrode of large electrical substations should be 1 Ohm or less.

II-24. Factors that affect lightning protection include:

- The design of the plant ground mat;
- The soil resistivity;
- The design of the lightning rod (e.g. whether copper clad, coated, of other noble materials, of what size and depth).

II-25. A well designed plant grounding system is essential for the protection of power plant equipment from ground faults and lightning strikes.

STUDIES OF ELECTROMAGNETIC COMPATIBILITY

II-26. There are international standards for electromagnetic compatibility in industrial environmental conditions. Such international standards may serve as the basis for the requirements for electromagnetic compatibility in a nuclear power plant. Such standards would have to be supplemented, where necessary, to cover requirements for electromagnetic compatibility in the environmental conditions of the components of a generating nuclear power plant, which may be more demanding. The results of such a study would include the emission level envelope with a frequency spectrum and the susceptibility level envelope with a frequency spectrum.

DEFINITIONS

The following definitions are not taken from the IAEA Safety Glossary[4].

alternate AC power source. A power source reserved for the use for the power supply to the plant during total loss of all non-battery power in the safety power systems (station blackout) and other design extension conditions.

controlled state. Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state. (From SSR 2/1[5].)

preferred power supply. The power supply from the transmission system to the safety classified electrical power system, comprising transmission system, switchyard, main generator, distribution system and safety classified electrical power system.

ⓘ Some portions of the preferred power supply are not part of the safety classification.

safe state. Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time. (From SSR 2/1[5].)

station blackout. Plant condition with complete loss of all AC power from off-site sources, from the main generator and from standby AC power sources important to safety to the essential and nonessential switchgear buses. DC power supplies and uninterruptible AC power supplies may be available as long as batteries can supply the loads. Alternate AC power supplies are available.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, IAEA, Vienna (2007).

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

CONTRIBUTORS TO DRAFTING AND REVIEW

Auvinen, K.	Forsmark nuclear power plant, Sweden
Diaz, E.	Comisión Nacional de Energía Atómica, Argentina
Dubois, A.	Institut de radioprotection et de sûreté nucléaire, France
Fredlund, L.	Ringhals AB, Sweden
Frey, W.	Gesellschaft für Anlagen- und Reaktorsicherheit, Germany
Giannelli, I.-A.	ENEL Engineering and Research Division — ATN, Italy
Givaudan, B.	EDF, France
Goodney, D.	Constellation Energy, United States of America
Johnson, G.	International Atomic Energy Agency
Jordan, R.	Westinghouse Electric Company, United States of America
Kiger, C.	Analysis and Measurement Services Corporation, United States of America
Kim, B.-Y.	Korea Institute of Nuclear Safety, Republic of Korea
Knutsson, M.	Ringhals AB, Sweden
Krastev, E.	Kozloduy nuclear power plant, Bulgaria
Lamell, P.	Forsmark nuclear power plant, Sweden
Lindner, L.	ISTec, Germany
Lochthofen, A.	Gesellschaft für Anlagen- und Reaktorsicherheit, Germany
Matharu, G.	United States Nuclear Regulatory Commission, United States of America
Mathew, R.	United States Nuclear Regulatory Commission, United States of America
Mauhin, B.	Tractebel Engineering GDF Suez, Belgium
Meiss, S.	Bundesamt für Strahlenschutz, Germany
Padin, C.	Comisión Nacional de Energía Atómica, Argentina
Rogers, A.	Private consultant, Canada
Sarwar, T.	Pakistan Atomic Energy Commission, Pakistan
Schnuerer, G.	ISTec, Germany
Sobott, O.	AREVA, Germany
Yonezawa, T.	Energis, Japan