Date: 2012 April 30

IAEA SAFETY STANDARDS

for protecting people and the environment

Draft E

For NUSSC Review

Design of Electric Power Systems for Nuclear Power Plants

DS-430

DRAFT SAFETY GUIDE

New Safety Guide

Supersedes NS-G-1.8

IAEA

International Atomic Energy Agency

TABLE OF CONTENTS

TABLE OF CONTENTS 3

1. INTRODUCTION 7
BACKGROUND 7
OBJECTIVE 7
SCOPE 8
STRUCTURE 8
STYLE 12
RELATIONSHIP TO OTHER STANDARDS 12

2. NUCLEAR PLANT ELECTRICAL POWER SYSTEMS 13
DESCRIPTION OF PLANT ELECTRICAL POWER SYSTEM 13
Off-site power system 13
On-site power system 14
Preferred power supply 14
ROLE OF CODES AND STANDARDS 15
DESIGN CONSIDERATIONS IMPOSED BY NUCLEAR SAFETY 15
DESIGN CONSIDERATIONS IMPOSED BY ELECTRICAL DESIGN CRITERIA 16
Power plant as a generating facility connected to the grid 17
Personnel and equipment safety 17

3. CLASSIFICATION OF ELECTRICAL POWER SYSTEMS 17

4. DESIGN BASES FOR ELECTRICAL POWER SYSTEMS 19

5. GENERAL DESIGN GUIDELINES FOR ELECTRICAL POWER SYSTEMS 22
GENERAL 22
Anticipated electrical events 22
Station blackout 25
DESIGN FOR RELIABILITY 25
General 25
Redundancy 25
Independence 26
Diversity 29
Common cause failures 29
Failure modes 31
Protection coordination 31
Reliability confirmation. 32
RATING 33
Motor loads 33
ELECTRICAL EQUIPMENT AND RACEWAYS 34
General 34
Rating and sizing 34
Installation 34
Separation by voltage classes 35
GROUNDING PRACTICES. 36
General 36
Electrical Safety 36

Functionality ... *36*
LIGHTNING AND SURGE PROTECTION ... 37
EQUIPMENT QUALIFICATION ... 38
General ... *38*
Suitability and correctness ... *39*
Environmental qualification ... *39*
Internal and external hazards ... *40*
Electromagnetic qualification ... *40*
DESIGN TO COPE WITH AGEING ... 42
CONTROL OF ACCESS ... 43
SURVEILLANCE TESTING AND TESTABILITY ... 43
Test Provisions ... *43*
Test program ... *44*
Test procedures ... *45*
MAINTAINABILITY ... 45
PROVISIONS FOR REMOVAL FROM SERVICE FOR TESTING OR MAINTENANCE ... 46
SHARING OF STRUCTURES, SYSTEMS AND COMPONENTS IN MULTI-UNIT PLANTS ... 46
MARKING AND IDENTIFICATION ... 47
CONTAINMENT ELECTRICAL PENETRATIONS ... 47
DISTRIBUTION SYSTEMS ... 48
Capability ... *48*
Protective devices of the main and branch circuits and loads ... *48*
CONTROLS AND MONITORING ... 49
NON-SAFETY CLASSIFIED STANDBY AC POWER SOURCES ... 50

6. DESIGN GUIDELINES FOR PREFERRED POWER SUPPLIES ... 50
GENERAL ... 50
RELIABILITY OF PROTECTION DEVICES AND HIGH VOLTAGE EQUIPMENT ... 51
OFF-SITE POWER SUPPLIES ... 51
AVAILABILITY ... 52
INDEPENDENCE ... 53
SWITCHYARD ... 53
GRID STABILITY AND RELIABILITY ... 53
INTERFACE AND INTERACTION BETWEEN TRANSMISSION SYSTEM OPERATOR AND NUCLEAR POWER PLANT OPERATOR ... 54
RELIABILITY ASSESSMENT OF GRID CONNECTIONS ... 55

7. DESIGN GUIDELINES FOR ELECTRICAL SAFETY POWER SYSTEMS ... 55
GENERAL ... 55
Anticipated electrical events ... *55*
Bus monitoring and switching ... *56*
DESIGN FOR RELIABILITY ... 57
Single failure criterion ... *57*
Completion of protective action ... *59*
SAFETY STANDBY AC POWER SOURCES ... 59
General ... *59*
Testing ... *61*
Performance criteria (transient and dynamic) ... *61*
Relay protection of standby power sources ... *61*

Support systems for standby power sources ... *62*
Fuel for standby power sources ... *62*
DC POWER SYSTEMS ... 62
General ... *62*
Battery ... *63*
Battery charger ... *63*
Uninterruptible AC power system ... *65*
Protection of DC power systems and uninterruptible AC power system ... *65*

8. ALTERNATE AC POWER SUPPLIES ... 66

9. DESIGN CONFIRMATION AND DOCUMENTATION ... 67
MANAGEMENT SYSTEM ... 67
VERIFICATION ... 67
Testing ... *68*
DESIGN DOCUMENTATION ... 69

REFERENCES ... 71

ANNEX I. DEFENCE IN DEPTH IN ELECTRICAL POWER SYSTEMS ... 73
FIRST LEVEL ... 73
Design bases ... *73*
The grid ... *73*
Onsite power systems ... *75*
SECOND LEVEL ... 76
Fault clearing system and protection coordination ... *76*
Power transfer capability ... *76*
House-load operation possibilities ... *77*
THIRD LEVEL ... 77
On-site standby AC power supplies ... *77*
Safety power systems ... *77*
FOURTH LEVEL ... 78
Alternate AC power supply ... *78*

ANNEX II. ELECTRICAL SYSTEM ANALYSES FOR DESIGN VERIFICATION ... 79
LOAD FLOW STUDIES ... 79
SHORT CIRCUIT STUDIES ... 80
ELECTRICAL PROTECTION COORDINATION STUDIES ... 80
LOSS OF VOLTAGE AND DEGRADED VOLTAGE STUDIES ... 81
TRANSIENT STABILITY STUDIES ... 82
LIGHTNING PROTECTION AND SYSTEM GROUNDING STUDIES ... 83
ELECTROMAGNETIC COMPATIBILITY STUDIES ... 84

LIST OF DEFINITIONS ... 85

CONTRIBUTORS TO DRAFTING AND REVIEW ... 87

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide is issued in support of the Safety Requirements publication on Safety of Nuclear Power Plants: Design SSR-2/1, Ref. [1], which establishes the requirements that nuclear power plant must meet to ensure the protection of the public and the environment.

1.2. This Safety Guide provides recommendations on the characteristics that nuclear plant Electrical Power systems, and the processes for developing these systems, should have in order to meet the requirements of Safety Requirements SSR-2/1, Ref. [1]. It reflects international best practices and a consensus that the recommended characteristics (or equivalent) should be achieved in the development of electrical power systems. The Guide does not provide details of implementation processes, development methods, or technology, except as explanation.

1.3. This publication is a revision of a previous Safety Guide issued in 2004 as Safety Guide NS-G-1.8, Ref. [2], Emergency Power Systems at Nuclear Power Plants, and supersedes it. This revision takes into account the developments in the design of Emergency Power Systems in nuclear power plants and expands the scope to include all Electrical Power Systems that provide power to systems Important to Safety.

1.4. NS-G-1.8, Ref. [2] also included guidance on non-electrical systems that provided emergency power. Guidance for such systems is to be located in a new safety guide on Auxiliary Systems.

1.5. Electrical systems that supply power to systems important to safety are essential to the safety of nuclear power plants. These systems include both the onsite and offsite power supply systems. The onsite and offsite systems work together to provide necessary power, in all plant conditions, so that the plant can be maintained in a safe state. Offsite power systems are not plant equipment. They are, nevertheless, essential to the safety of a nuclear power plant and have an important role 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 up to the safety classified electrical power system. It is composed of transmission system, switchyard, main generator and distribution system up to safety classified electrical power system. The portions of the preferred power supply that are part of the offsite power system. (e.g., transmission system and switchyard) are not plant equipment and, therefore, are not part of the safety classification scheme (see Fig. 2). The location of the boundary between the offsite and onsite power supplies will be a plant-specific decision

OBJECTIVE

1.7. The objective of this Safety Guide is to give guidance on the design of Electrical Power Systems to comply with the requirements established in Requirements 41 and 68, paragraphs 6.43–6.45, and the general requirements of Sections 2-5 of SSR-2/1, Ref. [1]. It is intended for the use by those involved in the design, operation, maintenance, modification, assessment, and licensing of nuclear plants, including designers, reviewers, safety assessors, regulators and operators. It might not be practicable to apply some of the recommendations of this Safety Guide to plants that are already in operation or under construction.

SCOPE

1.8. The Safety Guide makes recommendations and provides guidance on the electrical power systems provisions necessary for both new and operating nuclear power plants. It applies to all Electrical Power Systems important to safety[1] in Nuclear Power Plants, including the preferred power supply.

1.9. This guide applies to all types of nuclear power plants. The extent of the electrical power systems import to safety and of safety power systems[2], given by classification of the electrical systems, differs between different designs. The minimum design requirements for electrical systems needed at different voltage levels, for maintaining defence-in-depth and diversity, are outlined in this Guide. In all cases, this guide should be used together with the plant's Safety Report in order to determine the safety significance and importance of different power sources. For example, in plants with passive engineered safety features, the classification of the electrical power systems may be substantially different than shown in figure 2.

1.10. Additional recommendations applicable to electronic devices used in the control and protection of the Plant Electrical Power Systems are given in the safety guide for I&C systems, DS-431, Ref. [3].

1.11. Figures 1, 2 and 3 show example Nuclear Power Plant Electrical Power System to illustrate the scope of this guide and terminology used in this guide. Further explanation is found in the section on definitions and abbreviations.

1.12. This guide is focused on the electrical power systems. Guidance on the specification of loads is outside the scope, but such specifications must align with the design guidelines for the power systems.

1.13. Electrical power for security systems (e.g., fences, surveillance systems, entrance control) is outside the scope of this guide.

STRUCTURE

1.14. Section 1 of this document gives the introduction, scope, and objectives.

1.15. Section 2 introduces the main systems of a typical plant electrical power system and describes the fundamental goals to be met by each system.

1.16. Section 3 describes the application of safety classification to electrical power systems.

1.17. Section 4 outlines the content that should be included in the design bases for electrical power systems.

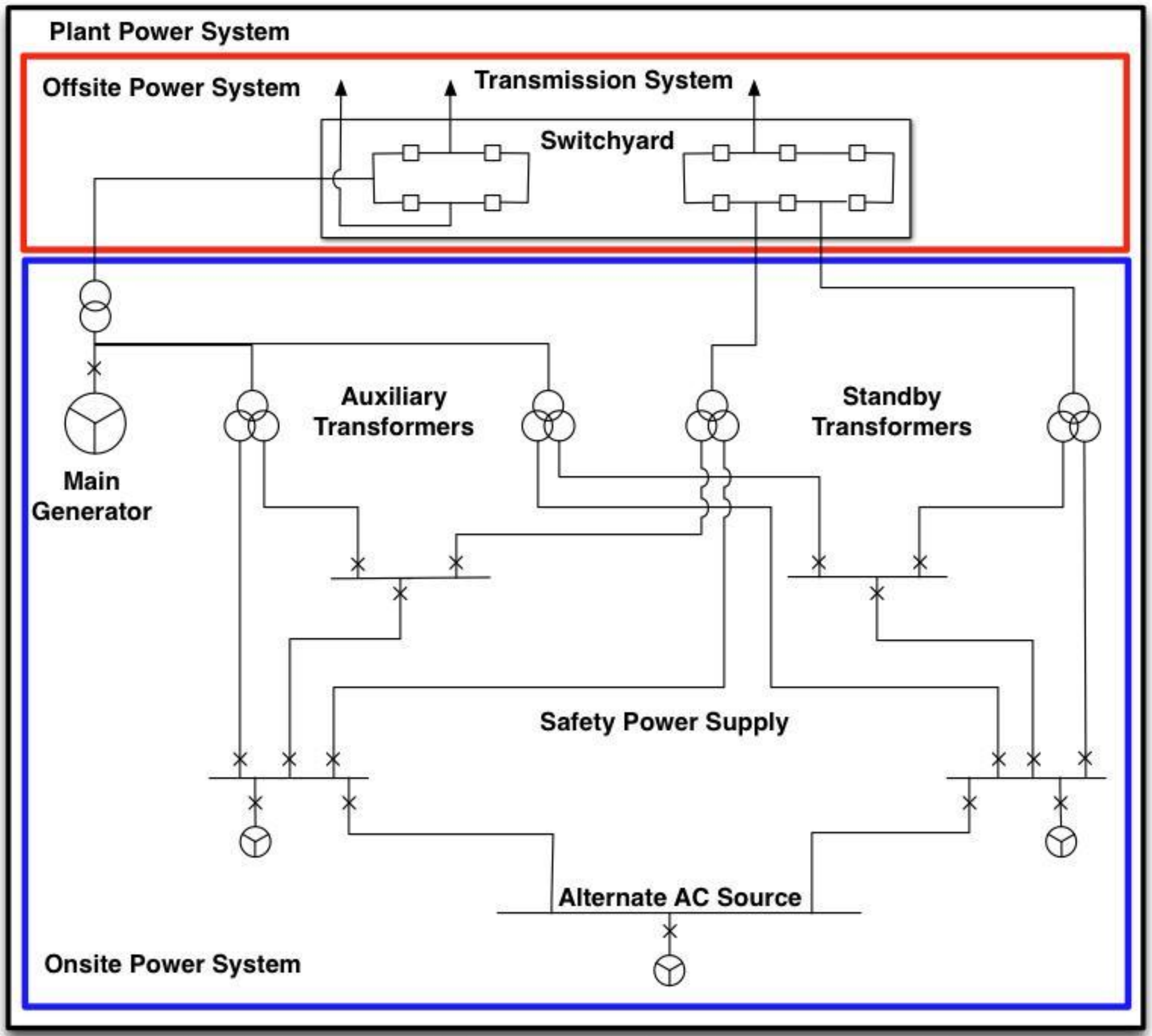
1.18. Section 5 gives general guidance that applies to all electrical power systems. These recommendations are the minimum recommendations for systems that are not covered in sections 6 thru 9. For systems that are covered in sections 6 thru 9 the recommendations of section 5 should be used in conjunction with the specific recommendations.

1.19. Section 6 gives guidance for the preferred power supplies, which 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 sources.

---

[1] Power systems important to safety are plant electrical systems that provide power necessary for systems or components important to safety to accomplish their safety functions.– directly or via transformers, switchgear and switchyards. (see fig. 2)

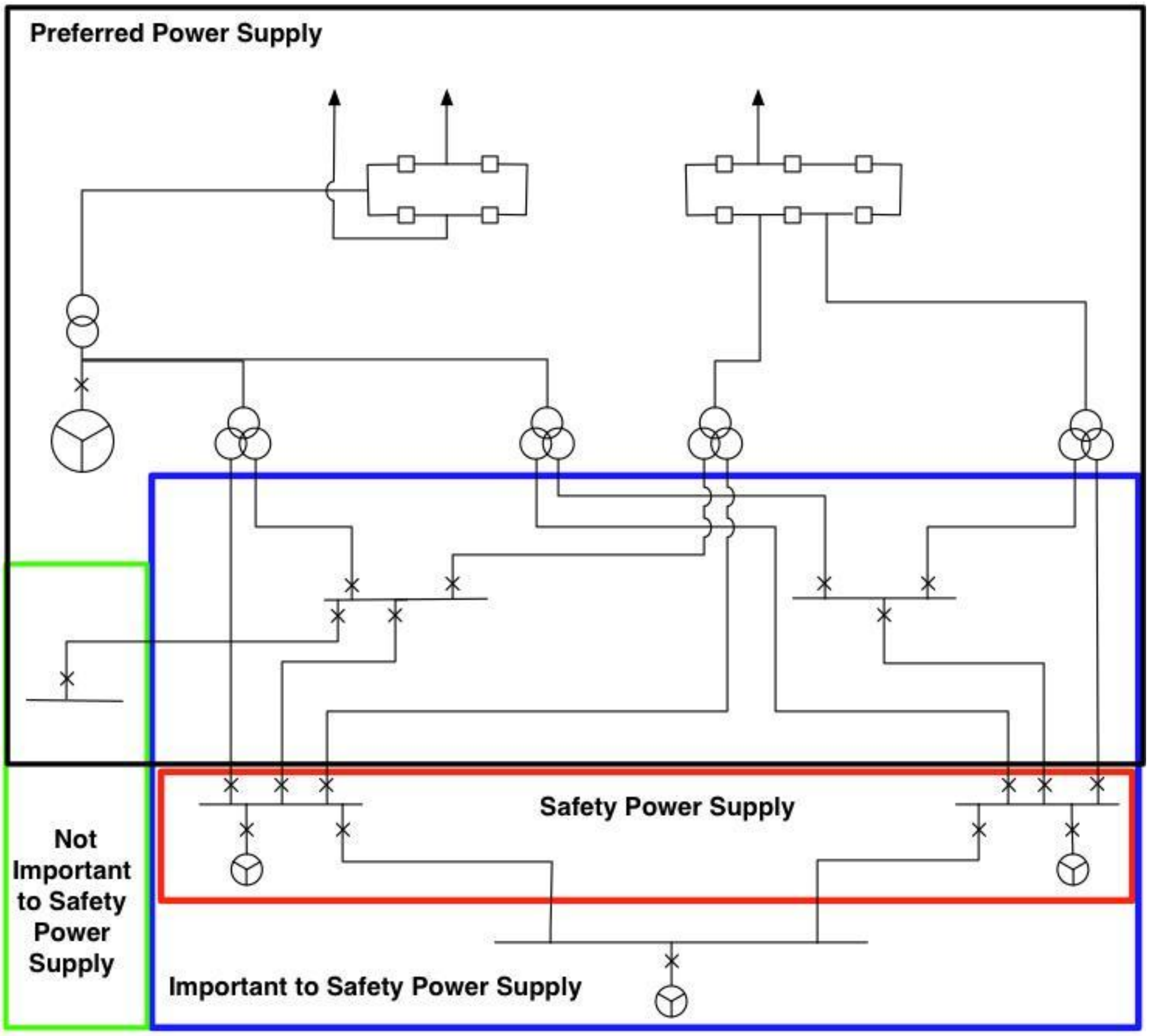
[2] Safety power systems are plant electrical systems that provide power necessary for safety systems or components to ensure safe shutdown of the reactor, residual heat removal from the core, or to limit the consequences of anticipated operational occurrences (AOO) or design basis accidents (DBA).



Note This figure is only an example. Varrious arrangements of buses, loads, generators, and interconnections will meet the requirements of SSR 2/1. Furthermore, many elements of the plant power system, such as buses that are not important to safety, and DC power systems are not shown.

Special purpose, "stand-alone" power supplies, such as separate power for security systems, are not included in the scope of this guide.

FIG. 1. Relationship of the plant power system, the offsite power system and the onsite power system.



Notes This figure is only an example. Various arrangements of buses, loads, generators, and interconnections will meet the requirements of SSR 2/1. Furthermore, many elements of the plant power 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 system that are within the safety classification scheme and the Preferred Power Supply.

The elements of the Preferred Power System 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 the different Member States.

Some plant designs do not require safety standby power sources. All nuclear power plants are expected to have safety DC power supplies.

FIG. 2. Relationship of power supplies important to safety, safety power supplies, and the preferred power supply.

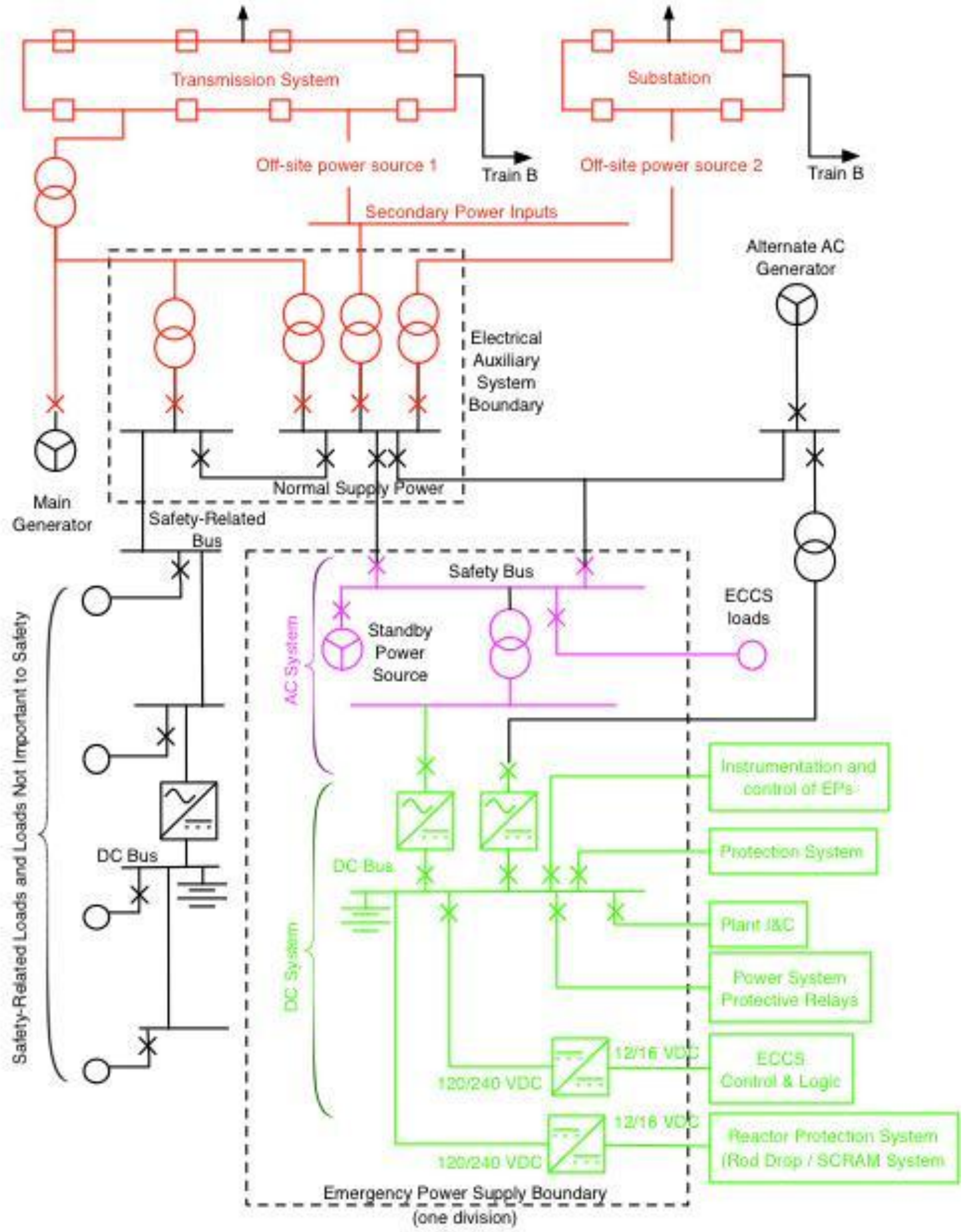


FIG. 3. Schematic representation of the different parts of the plant power supplies discussed in this guide, with their boundaries..(Typical for one train.)

1.20. Section 7 gives guidance that is specific to the design of safety power systems, including safety standby power supplies.

1.21. Section 8 gives guidance that is specific to the design of alternate AC 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 offsite and emergency on-site AC power supplies.

1.22. Section 9 provides recommendations for activities to confirm the adequacy of the electrical power system design 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.

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

1.24. Annex II gives an example of Electrical System Analyses for design verification of the nuclear plant.

STYLE

1.25. This guide uses the term ‘should’ to indicate that it is recommended to take the measures stated or alternative measures. The term ‘may’ is used to indicate measures that are considered acceptable practice, but which are not necessarily recommended. In general this safety guide uses the term ‘power source’ for a device that produces energy (e.g., generator or battery), including the prime mover and supporting items that are part of the device. The term ‘power supply’ is used for a system that provides power to one or more loads. A power supply includes distribution equipment and cabling and may include a power source or power conversion equipment such as inverters or chargers.

1.26. All paragraphs of guidance of this document are of one of three types:

- A quote of, or reference to, requirements from SSR-2/1, Ref. [1] or other IAEA requirements documents. These paragraphs are given in the form of block quotes.
- Recommendations of electrical power system or development process characteristics that should be achieved in order to comply with IAEA requirements. These paragraphs are given in bold text. Each recommendation is given as a separate paragraph.
- Comments that further explain or amplify the recommendations or illustrate ways in which the recommendations might be achieved. These paragraphs are given in normal text.

1.27. The Guide includes illustrative figures, a glossary, a bibliography and annexes. Words are used with the spellings and meanings assigned to them by the Concise Oxford Dictionary. The English text is the authoritative version.

RELATIONSHIP TO OTHER STANDARDS

1.28. This guide is a part of the IAEA Safety Standards series and should be used in conjunction with the other documents in this series. IAEA Safety and Security Standards of particular relevance to the design of NPP electrical power systems are listed below.

- NS-G-1.2, Safety Assessment and Verification for Nuclear Power Plants, Ref. [4];
- DS-431, Design of Instrumentation and Control Systems for Nuclear Power Plants, Ref. [3];
- NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Ref. [5];
- NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants, Ref. [6];
- NS-G-1.7, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, Ref. [7];
- NS-G-1.11, Protection against Internal Hazards other than Fires and Explosions in Nuclear Power Plants, Ref. [8];

- NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Ref. [9];
- NS-G-2.4, The Operating Organization for Nuclear Power Plants, Ref. [10];
- NS-G-2.6, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, Ref. [11];
- NS-G-2.12, Ageing Management for Nuclear Power Plants, Ref. [12];
- NS-G-2.14, Conduct of Operations at Nuclear Power Plants, Ref. [13];
- GS-R-3, The Management System for Facilities and Activities, Ref. [14];
- GS-G-3.1, Application of the Management System for Facilities and Activities, Ref. [15];
- GS-G-3.5, The Management System for Nuclear Installations, Ref. [16].

1.29. This guide has an important relationship with DS-431, Ref. [3], which deals with I&C systems. This guide gives recommendations for power supply, cable systems, and protection from electromagnetic interference that has strong support roles for I&C systems. DS-431, Ref. [3] gives recommendations that apply to the electronic controls and protective elements of the electrical power systems.

2. NUCLEAR PLANT ELECTRICAL POWER SYSTEMS

DESCRIPTION OF PLANT ELECTRICAL POWER SYSTEM

2.1. Figures 1, 2, and 3 show examples of the outline of a nuclear power plant's Electrical Power System to illustrate the scope of this guide. The design of a specific plant's electrical power system will depend upon the grid[3], the design of plant systems, and engineering design decisions that are beyond the scope of this guide. Therefore, Figures 1, 2, and 3 are not to be taken as a recommended design for any specific plant.

2.2. The Safety Power System can be supplied by either the preferred power supplies or the stand-by power sources. Alternate Alternating Current (AAC) supplies can also supply the safety power systems in design extension conditions.[4]

2.3. This 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 paragraphs below explain these terms as they are used in this guide. The use of these terms in a specific plant will depend upon details of the plant design and may differ from the use in this 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 ideally provide AC power to the plant during all modes of operation. It also provides transmission lines for out-going power. (See

[3] The term grid may refer to just the transmission system in a country, or in interconnected countries, or include both the transmission and distribution systems.

[4] Electrical Power Systems can be described in a number of different ways such as: 1) Safety and non-safety when focusing on reactor safety aspects 2) Non-priority, emergency power and battery back-up when focusing on interruption time of the power supply 3) AC and DC when focusing on system properties.

Figure 1.) The border between on-site and off-site power systems is normally in the high voltage breakers closest to the plant.

2.5. The offsite power system performs an essential role in terms of safety in order to supply the onsite power systems with reliable power from multiple off-site generators. The off-site power system is part of the preferred power supply.

2.6. An intrinsically robust grid system provides a highly reliable offsite power source as it rapidly dampens the effects of grid perturbations during normal conditions and minimizes the voltage and frequency deviations in the nuclear plant electrical system.

On-site power system

2.7. The on-site power system is composed of distribution systems and power supplies within the plant. It includes the AC and DC power supplies needed to bring a the plant to a controlled state following anticipated operational occurrences or accident conditions and to maintain it in a controlled state or safe state until off-site sources can be restored. (See Figure 1.) Stand-alone power supplies, for example separate power for security systems, are not included. The on-site power systems are separated into three different categories according to their safety significance. See Figure 2.

2.8. The major components of the On-site Power System include the plant generator, plant transformer, auxiliary transformer, standby transformer and the distribution system feeding unit auxiliaries, service auxiliaries, batteries, rectifiers, inverters/UPSs, cables and standby AC power sources. Portions 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 systems according to the different power requirements of the loads:

- An Alternating Current (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. The loss of the preferred AC power supply to the Electrical Power Systems triggers the startup of a standby electrical power source. In most cases plant safety analyses assume that the standby AC power source will be available for response to design basis accidents.
- A direct current (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. Often separate DC power systems will be provided to support loads of different safety classification.
- A uninterruptible AC power system which 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 include a bypass circuit to allow feeding safety loads directly from safety class AC power systems.

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 safety electrical power systems. The preferred power supply includes portions of both the on-site and off-site systems. See Fig. 2.

2.11. The preferred power supply is composed of the transmission system, switchyard, main generator, transformers and distribution system up to the safety electrical power systems.

ROLE OF CODES AND STANDARDS

2.12. SSR-2/1 Requirement 9 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.

2.13. The offsite power system should satisfy the nuclear safety criteria established in national and international standards, the grid code and electrical design criteria (as imposed by national electrical codes).

2.14. The plant electrical 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 during all modes of plant operation.

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

DESIGN CONSIDERATIONS IMPOSED BY NUCLEAR SAFETY

2.16. The electrical power systems and components at a nuclear power plant:

- Supply electrical power to the plant’s auxiliary systems from external and internal power supplies. The reliable operation of these systems is essential for ensuring plant safety, accident management and the mitigation of the consequences of accidents, and
- Generate electrical power for commercial use,

2.17. The NPP needs high reliability and availability of the transmission network, as grid disturbances can challenge nuclear safety when the NPP acts as a:

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

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

2.19. The electrical power systems, at all voltage levels, are support systems needed for all plant states as well as for reaching and maintaining a safe state and provide defence-in-depth (refer to Annex I for a detailed explanation) in the case of an event requiring plant cool-down. A reliable power supply is critical for maintaining control during anticipated deviations from normal operation as well as to power, control and monitor plant safety functions required to support the barriers that prevent radiological releases during design basis accidents and design extension conditions.

2.20. Special attention must be given during shutdown operation to ensure that adequate electrical power systems are available to maintain the applicable safety specifications when parts of the plant systems are taken out of operation for maintenance or surveillance testing.

2.21. SSR-2/1 requirement 4 and paragraph 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.

2.22. A systematic approach should be followed to identify the electrical power systems, structures and components needed in order that items necessary to fulfil the fundamental safety functions can be powered from electrical supplies with appropriate safety classification and reliability.

2.23. Robust and reliable onsite power systems are essential for supporting the safety functions of the plant.

2.24. Robustness means that the plant equipment has sufficient margins and built in conservatisms such that equipment ratings, capabilities and capacities required to meet intended goals are not easily challenged. Equipment protection setpoints are chosen to accommodate anticipated variations in operation of onsite and offsite power systems. Protective actions are initiated, when needed, in order to preserve the functionality of the Safety Power Systems during normal operation. However, during emergency operation, there is a need to allow for sustained overload or overvoltage conditions. Use of proven design is preferred.

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

2.26. A number of measures can be taken on and off 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.

2.27. Measures should be taken to protect the electrical systems against common cause failures (CCF).

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

2.29. 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 equipment during events, normal or abnormal (see paragraph 5.8), in the electrical systems.

2.30. Electrical systems powering equipment important to safety - directly or via transformers, switchgear and switchyards – are connected to equipment not important to safety that is not required for prevention of abnormal operation or for mitigating the consequences of failures or accident conditions.

DESIGN CONSIDERATIONS IMPOSED BY ELECTRICAL DESIGN CRITERIA

2.31. 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.

2.32. Design should consider transient and quasi-stationary variations of voltage and frequency that affect the electrical systems and components of the nuclear power plant.

2.33. The protection scheme of 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.

2.34. During emergency activation, equipment protection may be reduced to the essential set in order to give priority to the safety action.

Power plant as a generating facility connected to the grid

2.35. In accordance with national legislation, national grid codes or bilateral agreements between each transmission system operator[5] and each power generating facility, a power generating facility should be designed in such a way that it supports highly reliable grid system operation.

2.36. High grid reliability is essential for safe and reliable electrical power supply in a nuclear power plant.

2.37. It is important that grid codes recognize the specific features and design requirements of Nuclear Power Plants.

Personnel and equipment safety

2.38. Electrical installations should be designed and erected in such a way that they do not carry a risk of injury or damage to persons or property due to high temperatures, arcing or mechanical stress caused by rated current, overcurrent, or any internal mechanical stresses to the equipment.

2.39. Electrical installations should be designed and erected in such a way that they can withstand voltages that can be expected to occur in the installation.

3. CLASSIFICATION OF ELECTRICAL POWER SYSTEMS

3.1. SSR-2/1 Requirement 22 and paragraphs 5.34, 5.35 and 5.36 state that:

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

[5] The transmission system operator (TSO) is the organization that transmits electrical power from generation plants to regional or local electricity distribution operators.

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.

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

3.2. Member States use different classification schemes. This guide does not recommend any specific scheme.

3.3. For the purposes of this guide the following classification scheme is used to grade recommendations according to safety significance.

3.4. All plant Electrical Power System functions, systems, and components fit into one of two safety categories: important to safety or not important to safety.

3.5. Items important to safety include:

- Those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public;
- Those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions;
- Those features that are provided to mitigate the consequences of malfunction or failure of structures, systems and components.

3.6. Functions, systems, and components important to safety are further categorized as either safety or safety-related.

3.7. Safety functions, systems, and components are those provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences (AOO) or design basis accidents (DBA).

3.8. Safety-related items are items important to safety that are not part of a safety system.

3.9. The classification scheme described above can be mapped to most of the Member States classification systems currently in use. The safety-related or safety categories may be further subdivided.

3.10. Figure 4 illustrates the relationship between these safety categories.

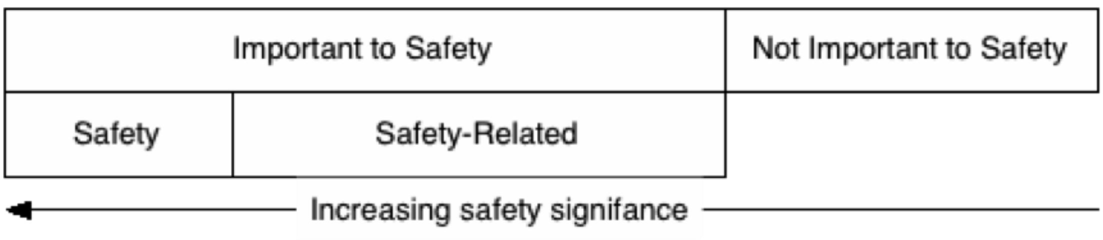


FIG. 4. Relationship between Safety Categories for plant equipment used in this Guide

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

4. DESIGN BASES FOR ELECTRICAL POWER SYSTEMS

4.1. SSR-2/1 Requirement 14 and paragraph 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. Requirements 15 to 19 of SSR-2/1, Ref. [1] elaborate on specific topics that must be considered in the development of system design bases.

4.3. A set of design bases should be specified and used to design the nuclear power plant electrical power system.

4.4. During normal operation the safety systems are generally powered from systems not classified as safety or interconnected with non-safety systems. In order to have a reliable safety system power supply, design bases need to be established for all electrical systems in the nuclear power plant.

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

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

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

4.8. Transients to be considered include external events such as anticipated grid events and grid perturbations leading to degraded or overvoltage conditions, internal events such as short circuits and large load starting or tripping, onsite power system voltage and frequency variations during load sequencing and switching operations in the electrical supply systems. If the design of the onsite power system requires transfer of station auxiliaries from one power source to another (for example, main generator to offsite power source) then the consequences of the transfer scheme must be evaluated on plant shutdown equipment.

4.9. The design bases should cover all modes of operation and take into account all possible events that could impact the electrical system in the nuclear power plant.

4.10. Events to be considered include symmetrical and asymmetrical faults, large motor starts, momentary perturbations in the grid system such as switching surges or lightning strikes, and loss of transmission system elements.

4.11. The design bases should be confirmed when major replacements and major modifications of the electrical power system (on-site or off-site) are implemented and a cumulative evaluation performed periodically, e.g., as part of Periodic Safety Reviews.

4.12. 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 100% power with maximum auxiliary loading, plant shutdown from 100% power, and safe shutdown following a trip and a design basis accident.

b. Voltage and frequency range for continuous operation;

This range defines the input for motors for pumps and valve actuators used in the accident analyses (safety analyses) of the plant.

c. Capacity requirements;

The equipment credited in the accident analyses normally defines capacity. Capacity, from an electrical point, 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 for heavy and light load conditions
- Frequency variation in normal operation
- Float voltage for DC systems

Transient conditions include, for example:

- Switching surges
- Lightning surges
- Voltage sags and swell in conjunction with clearing of faults on the on-site electrical system or the off-site grid
- Voltage and frequency variations and transients when the grid (and main generator) is affected by faults

e. Variables, such as system voltage and frequency, to be monitored;

This includes variables needed for accident and post-accident monitoring.

f. Actuation conditions for operating standby electrical power sources;

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,
- Natural phenomena,

h. Identification of all loads indicating safety classification and electrical characteristics;

This includes motor input power at run-out when applicable. It is necessary to update this element of the design basis after every modification of loads.

i. Required performance characteristics of all components;

j. Requirements for maintaining and testing;

Including test acceptance criteria.

k. Protective schemes and coordination of protection;

Protective schemes must 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, and
- 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.

System and component reliability and unavailability limits may be specified using probabilistic criteria, deterministic criteria (e.g., compliance with 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 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, starting load as well as, in certain member 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 must 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 that should be permitted to shutdown or disconnect safety power sources.

For example, the need to protect equipment from catastrophic failures.

5. GENERAL DESIGN GUIDELINES FOR ELECTRICAL POWER SYSTEMS

GENERAL

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

Anticipated electrical events

5.2. The design of the power systems in the plant should consider all possible events that could occur in the electrical systems associated with the plant (see fig 5). These events can cause symmetrical and asymmetrical perturbations in the plant and can be initiated:

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

5.3. The impact of such events on all the onsite electrical power systems (AC and DC) (see Figure 6) should be evaluated and confirmed that the allowable voltage and frequency requirements are not exceeded and the protection system is adequate.

5.4. Events on the onsite power systems to be considered include, but not limited to,

- Switching and lightning surges
- Voltage swells caused by loss-of-load scenarios
- Voltage sags caused by motor starts and electrical faults off-site and on-site
- Voltage interruptions caused by electrical faults off-site during shut-down operation;
- Voltage interruptions caused by on-site faults;
- Frequency deviations caused by turbine speed variations;
- Transmission system faults cleared by first step or backup protection;
    - With generator connected to the grid after the event,
    - Out-of-step events, or
    - Voltage and frequency variations and transients at house load operation;
- Deviating grid voltage and frequency;
- Faults in the on-site power system (all voltage levels) cleared by first step or backup protection;
- Main generator excitation malfunctions (high and low excitation);
- Open conductors; and
- Solar activity and geomagnetic induced currents.

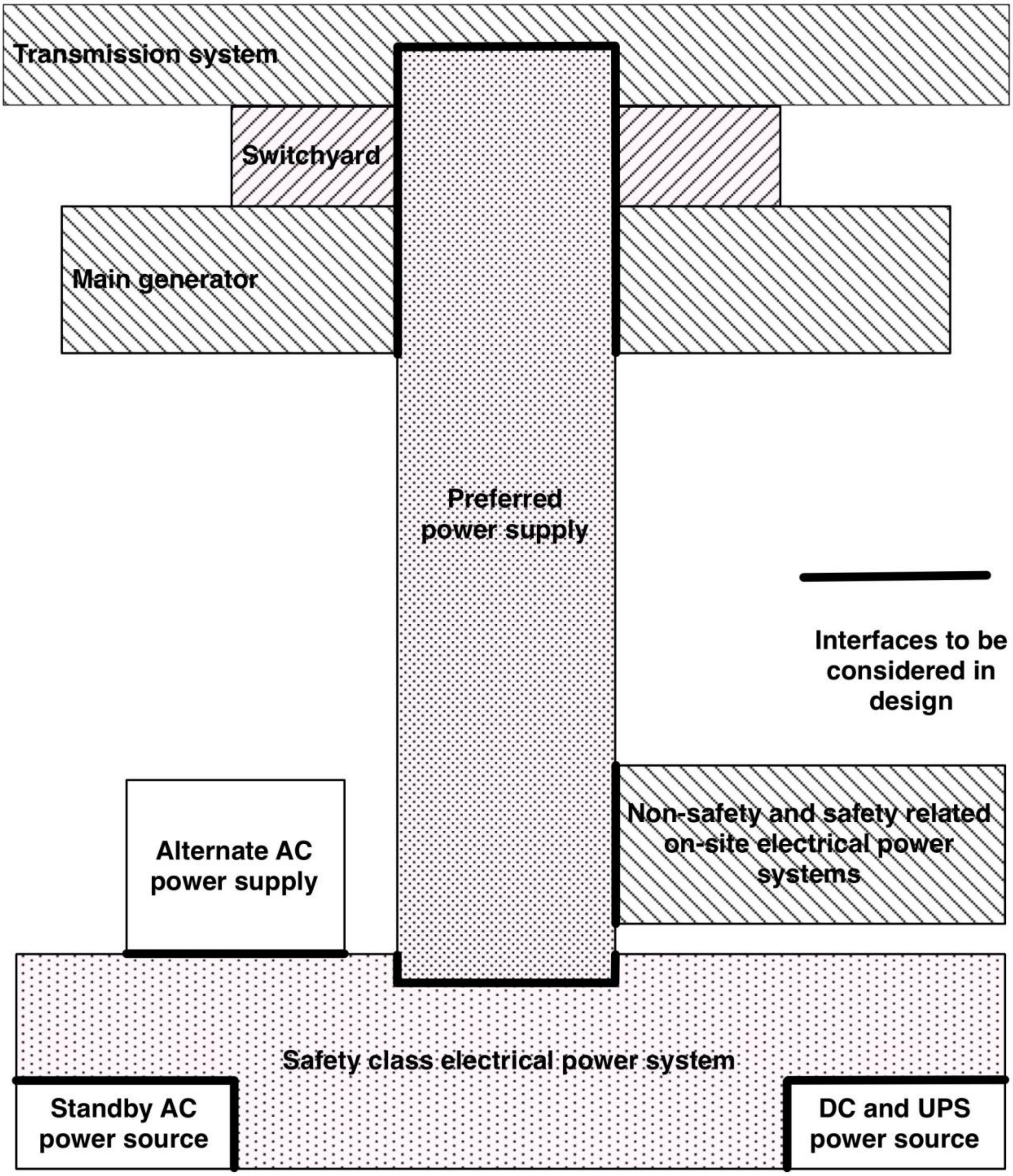


FIG. 5. Relationship between the Preferred Power Supply and Other Elements of the Electrical Power System

5.4. Events on the onsite power systems to be considered include, but not limited to,

- Switching and lightning surges
- Voltage swells caused by loss-of-load scenarios
- Voltage sags caused by motor starts and electrical faults off-site and on-site
- Voltage interruptions caused by electrical faults off-site during shut-down operation;
- Voltage interruptions caused by on-site faults;
- Frequency deviations caused by turbine speed variations;
- Transmission system faults cleared by first step or backup protection;

    - With generator connected to the grid after the event,
    - Out-of-step events, or
    - Voltage and frequency variations and transients at house load operation;
- Deviating grid voltage and frequency;
- Faults in the on-site power system (all voltage levels) cleared by first step or backup protection;
- Main generator excitation malfunctions (high and low excitation);
- Open conductors; and
- Solar activity and geomagnetic induced currents.

5.5. Examples of variations and transients on the buses to be considered include:

- Voltage ranges, maximum and minimum, for heavy and light load conditions;
- Frequency variation;
- Voltage and frequency transient response;
- Voltage regulation limits;

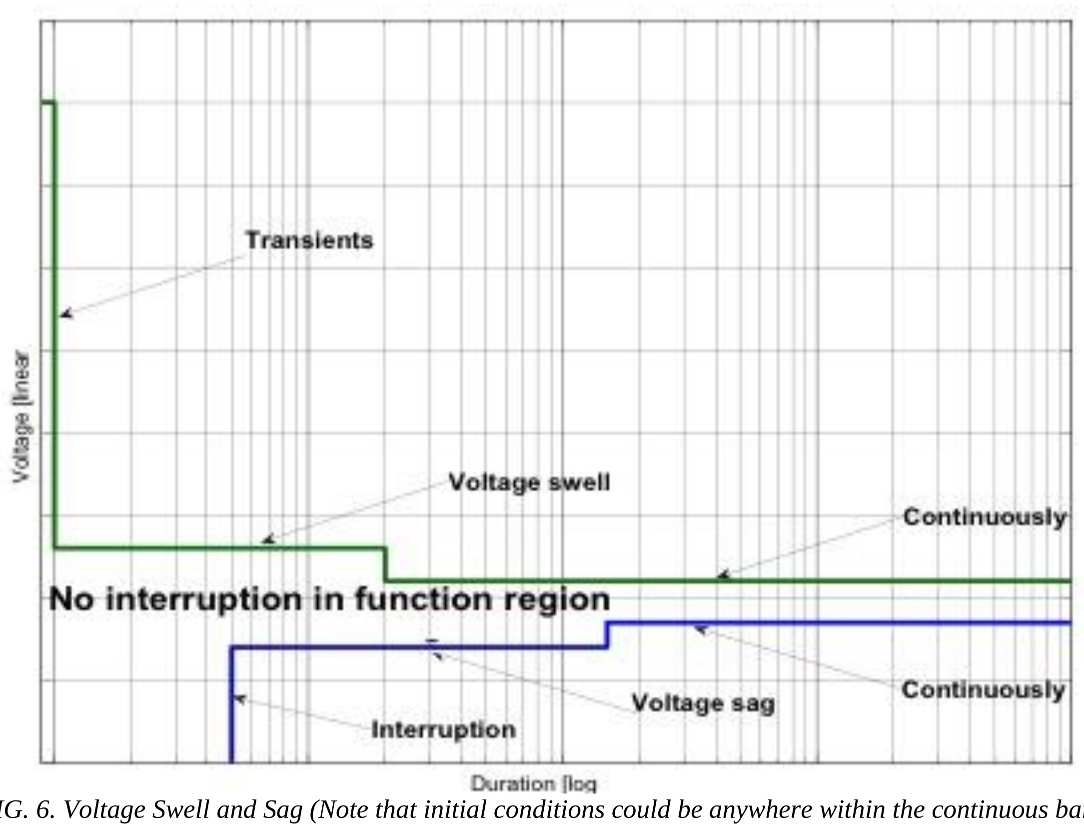


FIG. 6. Voltage Swell and Sag (Note that initial conditions could be anywhere within the continuous band)

5.6. The grid transient system stability analyses should demonstrate that the plant could ride through and remain connected to the grid for perturbations that do not result in generator falling out of step.

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

Station blackout

5.8. International operational experience has shown that on-site and off-site AC power supplies can be simultaneously lost. Such an event is called “station blackout” (SBO). The term station blackout 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 onsite and offsite power sources.

5.9. 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 source that is diverse in design and protected from elements that can degrade the normal power sources.

5.10. The plant’s capability to maintain fundamental safety functions and to remove decay heat from spent fuel should be analysed for the period that the plant is in a blackout condition.

5.11. The capability of the DC systems required to provide critical reactor coolant system parameters and power lighting and communication systems during the blackout should be evaluated for adequacy.

5.12. Critical breakers should have the capability for manual operation in the event that control power is lost.

5.13. The plant should have a diverse power supply unit (Alternate AC source) that is independent of the electrical power supply units provided for use during Operational States and Design Basis Accidents.

DESIGN FOR RELIABILITY

General

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

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

5.15. In the design of Electrical 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, fail-safe design, and selection of high quality equipment, are typically used to provide the specified reliability of safety functions.

Redundancy

5.16. Electrical systems important to safety should be redundant to the degree needed to meet design basis reliability requirements.

5.17. 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 needed. Taken alone, redundancy increases the reliability of safety actions, but it also increases the probability of spurious operation.

5.18. Coincidence of redundant signals (voting logic) or a rejection scheme for spurious signals that is based on comparisons of the redundant signals is commonly used to obtain an appropriate balance of reliability and freedom from spurious operation.

5.19. Safety electrical systems should have redundancy also to the degree necessary to ensure that the system will continue to comply with the single failure criterion when equipment is removed from service for planned surveillance testing or maintenance at the time the associated safety functions are required.

5.20. Operating experience indicates that additional redundancy within a train or division provides operational flexibility and increased availability. The availability of spare components such as an uninterruptible power supply, or battery charger, might preclude operating restrictions in the event of a failure or maintenance related outage of these critical components.

Independence

5.21. 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.

5.22. 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.

5.23. SSR-2/1 Paragraph 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.

5.24. Independence is provided to prevent a failure or 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, or common errors in design, manufacture, operations, or maintenance.

5.25. Safety items should be independent of the effects of the design basis accidents to which they must respond.

5.26. 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 design basis event that requires these functions.

5.27. Redundant portions of safety groups should be independent from each other to ensure that the safety group can perform its safety functions during and following any design basis event that requires these functions.

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

5.29. The functional failure of the support features of safety systems should not compromise the independence between redundant portions of safety systems or between safety systems and systems of lower safety classification.

5.30. For example, a safety system support feature such as room ventilation ought to be assigned to the same division as the safety system it is supporting in order to prevent the loss of mechanical function in one division causing a loss of electrical system function in another division.

5.31. Means for providing independence include physical separation, electrical isolation, independence from the effects of communications errors, equipment qualification, and diversity. Generally a combination of these methods must be applied to achieve independence goals.

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

5.33. Measures used to provide isolation from various physical effects, electrical faults, and communications errors do not necessarily need to be in the same physical device or at the same location in a circuit. Isolation functions for a single effect may also be shared by more than one device.

5.34. The adequacy of design features provided to meet the independence recommendations should be justified.

Physical separation

5.35. Physical separation:

- Protects against common cause failure due to the effects of internal hazards. Internal hazards of concern include: fire, missiles, steam jets, pipe whip, chemical explosions, flooding, failure of adjacent equipment.
- Might protect against common cause failure due to common normal, abnormal, or accident environments, the effects of design basis accidents, or the effects of external hazards. Environmental, seismic, and electromagnetic qualification might also 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., tornado, or tsunami).
- Reduces the likelihood of inadvertent errors during operation or maintenance on redundant equipment.

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

5.37. NS-G-1.11, Ref. [8] gives guidance on protection against the failure of mechanical equipment.

5.38. Safety systems should be physically separated from systems of lower safety classification.

5.39. Redundant portions of safety groups should be physically separated from each other.

5.40. It is important to carefully consider the adequacy of physical separation provided in areas of convergence for redundant equipment or wiring. Examples of areas where physical separation is often problematic include:

- Near the reactor vessel,
- Containment penetrations,
- Motor control centres,
- Switchgear areas,
- Cable spreading rooms,

- Equipment rooms,
- The main and other control rooms, and
- The plant process computer.

Electrical isolation

5.41. 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 pick-up, short circuits, open circuits, grounding, or application of the maximum credible voltage (alternating or direct current).

5.42. In general, non-safety loads should not be powered by safety electrical power systems.

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

5.44. Non-safety loads should preferably be disconnected from the safety electrical power systems when supply is transferred to safety standby AC power sources.

5.45. Non-safety loads that remain connected should be analysed for worst-case fault and catastrophic failure modes.

5.46. Non-safety loads that remain connected during postulated accident conditions should be included in power system loading analyses.

5.47. Fault current and failure mode evaluation should demonstrate minimal or no impact on associated safety systems.

5.48. An example of a preferred isolation device is a 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. This type of design feature precludes adverse impact (such as short circuit current) on the safety power supplies.

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

5.50. Connections between redundant divisions may be made during shutdown after a safety assessment confirms the following:

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

5.51. These interconnections could also be used in Station Blackout conditions.

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

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

Associated circuits

5.54. When it is impractical to provide adequate physical 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. Physically separated from other components.in the same manner as the circuits of the safety division with which it is associated.

Diversity

5.55. Safety power systems should be supplied from diverse power supplies.

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

5.57. 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 and in house-load scenarios will supply power;
- The Standby power source, which will supply the safety power systems on loss of off-site power; or
- Alternate AC power source during SBO conditions.

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

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

5.60. Where the design basis requires diversity for software based devices of an electrical power system, the guidance of DS-431, Ref. [3], should be followed.

5.61. Diversity of power supply sources for specific loads, e.g., I&C systems, might often improve the availability of the overall system.

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

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

Common cause failures

5.64. 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.

5.65. 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.

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

5.67. The use of principles of independence helps to ensure that the overall unavailability of the system is not determined by common cause failures. However, the possibility of other common cause failures occurring that might affect the principles of diversity and independence needs to be considered.

5.68. As the nuclear power plant is connected to 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 common cause failure possibilities will decrease. If the redundant safety power systems are fed from independent connections to the grid the common cause failure possibilities will also decrease.

5.69. Operating experience of events related to voltage transients, both on 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 for common cause failures. A ”no interruption” concept is desirable, realized as a series of design means to minimize the impact from transients (see Figure 6).

5.70. Due to the voltage, frequency and phase angle excursions that can occur in a generating facility, operating experience from industrial applications is of limited value when screening for common cause failure vulnerability.

5.71. The primary protections 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 built in features or by relay protection; and
- Verified capability not to transmit voltage and frequency excursions to buses fed from rectifiers and inverters.

5.72. After an event that ends in a loss of offsite power and if the safety power systems is not fed from the main generator(s), the standby power sources will supply the safety power systems. When the safety power systems as a result are divided into different divisions, one single electrical event cannot challenge redundant divisions. However 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.

5.73. The primary protection against common cause failures for the standby power sources is:

- Comprehensive design bases and guidelines that identify all possible events that could challenge the standby power sources control, start and operation;
- 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; and

- Proper redundancy of control circuits and equipment to ensure reliability in starting, endurance in operation and prevent unnecessary tripping.

5.74. In order to handle common cause failure risks for soft-ware based devices, the design of these items should follow the design principles for I&C equipment given in DS-431, Ref. [3].

Failure modes

5.75. 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.

5.76. The failure modes of electrical components important to safety should be known, evaluated, and documented.

5.77. Knowing the failure modes of components is important in applying the fail-safe concept to systems important to safety.

5.78. Failures of electrical components important to safety should be detectable by periodic testing or revealed by alarm or anomalous indication.

5.79. It is preferred that failures be self-revealing except when such a design might result in an unsafe state or cause a spurious actuation of safety systems.

Protection coordination

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

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

5.82. 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 degrade or fail.

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

5.84. 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 electrical system disturbances, equipment damage, and potential personnel and property hazards;

b. Monitoring the connected preferred power supply with provisions to automatically or manually initiate transfer to alternate supply;

The alternate supplies in this case may be different offsite supplies or standby AC power supplies. Fast bus transfers using state of the art 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 protection control power; and

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

5.85. A protection scheme that disconnects only faulted equipment will include the following characteristics.

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

5.86. The design of the protection devices of electrical power systems and components of nuclear facilities needs to consider also national safety standards that apply to the safety of electrical equipment and electrical installations, as well as other electrical safety regulations issued by electrical safety authorities

5.87. The protection scheme should take into consideration reacceleration currents after voltage sags and interruptions or bus transfer.

5.88. The bus voltage-monitoring scheme must be set to comply with voltage dips during reacceleration.

5.89. The design of protection devices should consider both symmetrical and asymmetrical faults.

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

5.91. Provision of means (part of modern digital relay protection) to capture transients during events is desirable in order to support verification of performed analysis and protection coordination.

Reliability confirmation.

5.92. For all systems important to safety a systematic assessment should be conducted to confirm that the design achieves the reliability requirements of system design bases.

5.93. This demonstration may be based on a balance of application of deterministic criteria and quantitative reliability analysis that considers design features such as, for example, redundancy, testability, failure modes, and rigor of qualification.

5.94. The use of software or complex multi-element logic modules might create difficulty in justification of reliability and sensitivity to common cause failures. The reliability confirmation may therefore depend on assurances of freedom from error in the design and implementation process. DS-431, Ref. [3] guide provides further discussion and guidance on this topic.

5.95. Test facilities that are part of the safety system must be considered when determining system availability.

RATING

5.96. All equipment used in the electrical systems in the plant should have sufficient margin in operating parameters when compared to their nominal rating.

5.97. Analyses to confirm the design margins should be performed, using conservative assumptions and qualified methods.

5.98. The adequacy of the margin in equipment rating should be confirmed regularly; at least in conjunction with major component replacements, plant modifications, and Periodic Safety Reviews.

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

Motor loads

General

5.100. Motors for items important to safety should be designed with pullout torque high enough to permit starting with degraded voltage, as defined by the design bases of the electrical system.

5.101. Motors and other devices for items important to safety connected to the power system must withstand the overvoltage that could result from different events in a power generating facility.

5.102. Thermo-hydraulic safety analyses verify a minimum required flow based on conservative assumptions. The actual flow, and motor load, will normally be greater if automatic flow control is not present. The loads used for motor rating and design of components in safety power systems as well as settings for overload protective devices must consider this higher load. In certain applications run-out torque must also be considered.

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

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

Design for overload operation

5.105. The need for the electrical power system to support operation of loads in overload conditions should be taken into account at the design stage.

5.106. Electrical systems, including cables, should be designed to permit needed overload operation without exceeding their rating.

5.107. It might be necessary in some situations to operate the 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. In such instances it is necessary to design the equipment to withstand the expected temporary overload conditions.

5.108. For example, the set points of circuit protective devices may be set higher than the levels that protect the equipment from damage due to continuous overloads. Cables must be protected against overload in accordance with their continuous current-carrying capability.

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

5.110. The continued operation of safety system equipment under overloaded conditions with the consequent risk of its damage need not form part of the safety justification for design basis accidents, although it is to be recognized that unforeseen circumstances might arise.

5.111. Loading above continuous rating should be indicated in the control room.

5.112. 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 needed in the particular situation.

ELECTRICAL EQUIPMENT AND RACEWAYS

General

5.113. Electrical equipment is defined here as switchgear, motor control centres, transformers and cable systems.

5.114. Electrical equipment should be selected, rated, and qualified for their service and environmental conditions.

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

5.116. Aspects of fire protection are considered in NS-G-1.7, Ref. [7].

Rating and sizing

5.117. 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.

5.118. Electrical equipment should be sized to:

a. Carry safely the currents of the main circuits and branch circuits required under voltage variations;

b. Meet the demands of the loads without exceeding rated temperature;

c. Withstand short circuits (e.g. fault current during the specified fault-clearing time), and

d. Withstand peak currents without exceeding mechanical strength.

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

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

Installation

5.120. Buses, raceway (i.e., tray or conduit), and their supports should be designed to withstand, with an appropriate margin, the mechanical loads, imposed by the cables and their associated fittings.

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

5.122. 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.

5.123. Generally the design ensure that cables, that are part of safety systems, are routed or protected so that neither fire nor failure of mechanical equipment can affect more than justified in the safety analysis report (normally one division of any safety group). Failure of mechanical equipment includes the 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 NS-G-1.11, Ref. [8].

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

5.125. Common practice is to permanently identify raceways and cables at each end and at regular intervals (except for cables in closed raceways). Raceway identification also normally includes cable voltage class.

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

5.127. In general, the use of cable splices should be prohibited in raceway.

5.128. Cable splices may be used for connections between field cables and equipment provided that they are qualified for the service. Such termination techniques may be needed for safety cables and equipment in containment to protect against high leakage currents that might be caused by exposure to environments created by accident conditions.

Separation by voltage classes

5.129. At least three voltage classes of cables should be identified for the purpose of physically separating cables within a division:

a. **Instrumentation and control cables;**

b. **Low voltage power cables (1 kV or less); and**

c. **Medium voltage power cables (20 kV or less).**

5.130. High voltage power cables are not commonly used in on-site power systems. If they are used, their separation from other cables needs to be considered.

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

5.132. Separation for electromagnetic purposes is in addition to separation for reasons of divisional independence. Cable routing must satisfy both sets of criteria.

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

5.134. Grounded metallic conduit represents an acceptable separation barrier.

GROUNDING PRACTICES.

General

5.135. Grounding serves both to assure electrical safety and electrical power system/I&C functionality. Detailed design guidelines for grounding are available in national and international standards.

5.136. In any generating station there are generally four conceptually identifiable, but not necessarily physically distinct, grounding systems: personnel safety, lightning, electrical power system and I&C system - including signal grounding.

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

5.138. The ground resistance value should take into consideration:

a. Fault current capacity of equipment, and

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

5.139. International standards describe a number of solutions for I&C grounding. Typically, generating stations use one of two approaches for I&C grounding: single-point grounding or multiple-point grounding. The selected solution is design specific and needs to be justified and coordinated with the overall EMC design provisions.

Electrical Safety

5.140. Overall grounding should be designed installed and maintained to effectively protect people, buildings and equipment as well as electrical power and I&C systems against damage.

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

5.142. If frames are not connected to ground, additional provisions for assuring personnel safety should be made.

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

Functionality

5.144. Medium and low voltage AC electrical power systems should preferably be high impedance grounded.

5.145. High impedance grounding limits fault current and allows continued operation of the affected equipment.

5.146. Other grounding solutions such as solid grounded or insulated system may be used when justified.

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

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

5.149. Protective schemes may trip equipment on multiple faults.

LIGHTNING AND SURGE PROTECTION

5.150. Provision should be made that a lightning strike will not prevent the power and I&C systems from fulfilling their required safety function.

5.151. The systems for achieving this may rely on external or internal protection. Typically a combination of both methods will be needed.

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

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

5.154. 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.

5.155. External lightning protection should be grounded in order to conduct the lightning current to ground outside the building.

5.156. The internal protection grounding should be connected to the rest of the lightning grounding in such a way it prevents high transferred potentials from injuring personnel or damaging equipment.

5.157. 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.

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

5.159. 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 plant power distribution systems.

5.160. 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 impact the plant safety and non-safety power systems

5.161. Power systems for control and monitoring should not be distributed outside a plant in order to minimize the risk for disturbances due to induction or other influence.

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

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

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

5.165. 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 unwanted electrical noise may be needed for reliable operation of equipment sensitive to electrical noise in the power system

EQUIPMENT QUALIFICATION

General

5.166. 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.

5.167. Electrical systems and components important to safety should be qualified for their intended function during their service life.

5.168. The qualification should provide confidence commensurate with the system or component safety classification.

5.169. The qualification program(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, and

d. Electromagnetic qualification.

5.170. Qualification should be based upon an appropriate combination of methods, including for example:

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

b. Reliability demonstration;

c. Past experience in similar applications;

Where operating experience is used to support equipment qualification it must be shown to.be relevant to the proposed application and environment of the target application.

d. Type testing;

e. Testing of supplied equipment; or

f. Analysis to extrapolate test results or operating experience under pertinent conditions.

5.171. It is generally not necessary to apply all of the methods mentioned. The specific combination of methods will depend upon 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 during engineering and manufacturing.

5.172. Analysis that is part of the evidence of equipment qualification should include a justification of the methods, theories and assumptions used.

5.173. 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.

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

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

Suitability and correctness

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

5.177. 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.

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

Environmental qualification

5.179. In this guide environmental qualification is qualification for temperature, pressure, humidity, chemical exposure, radiation, submergence, and ageing mechanisms that might affect the proper functioning of components under those conditions.

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

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

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

Components exposed only to mild environments

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

Components exposed to harsh environments

5.184. Environmental qualification of safety classified electrical power system components whose environmental service conditions during accidents are at any time significantly more severe than the conditions during normal operations (harsh environments) 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.

5.185. The worst credible case for combinations of environmental service conditions must be addressed. If it is necessary to separately test for different environmental conditions (e.g., separate tests for radiation and temperature effects) the sequence in which these tests are conducted must be justified as one that appropriately simulates the degradation caused by the combined environments.

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

5.187. The design life of the plant might be considerably longer than the qualified life of devices.

5.188. It is common practice to apply the most rigorous environmental qualification methods only to safety components.

5.189. Environmental qualification of safety components that must operate in harsh environments should include type testing.

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

Internal and external hazards

5.191. Electrical power systems and components should be protected against the effects of fire and explosion in accordance with the guidance of NS-G-1.7, Ref. [7].

5.192. Electrical power systems and components should be protected against the effects of other internal hazards in accordance with the guidance of NS-G-1.11 Ref. [8].

5.193. 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. [6].

5.194. 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.-[5].

Electromagnetic qualification

5.195. The undisturbed operation of electrical and electronic systems and components depends upon the electromagnetic compatibility (EMC) of components intended for the same operating environment, i.e. a component’s capability to withstand more disturbances than caused by the components around it.

5.196. Significant sources of electromagnetic interference (EMI) include, for example, fault current clearance by switchgear or circuit breaker or fuse operation, electric fields caused by radio transmitters, natural sources such as lightning strike, and other man-made sources internal or external to the plant.

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

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

- Suppression of electromagnetic noise at the source;
- Separation and isolation of instrument and control signal cables from power cables;
- Shielding of equipment and cables from external magnetic and electromagnetic sources;
- Filtering noise before it can couple to sensitive electronic circuits;
- Neutralization, or isolation of electronic equipment from, ground potential differences; and

- Proper grounding of electrical equipment, raceway, cabinets, components, and cables.

5.199. Practices for installation and maintenance must ensure that these provisions are appropriately implemented and maintained.

5.200. Detailed EMC requirements should be determined for all electrical systems and components and their compliance with the requirements demonstrated.

5.201. International EMC standards on industrial environments may serve as the basis for the requirements provided that they are supplemented, where necessary, to cover the EMC environments of generating power plant components, which might be more demanding. Determining the EMC requirements includes considering the exposure of components to possible repetitive rapid (e.g. switching off of inductive loads and ringing of relays) and high energy (e.g. various switching transients and lightning) transients in their operating environment.

5.202. Establishing the EMC environment of electrical systems and components at each nuclear power plant unit, involves unit-specific analyses based on which the adequacy of each electrical component's EMC requirements is evaluated.

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

5.204. The types of electromagnetic interference, to be considered in the design of electrical systems and components include:

- Emission of and immunity to radiated radio frequency disturbances;
- Emission via cables of and immunity to conducted radio frequency disturbances;
- Electrostatic discharge (ESD);
- Switching 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.

5.205. In the vicinity of certain sensitive equipment it may be necessary to establish exclusions zones where operation of wireless devices and other portable EMI sources (e.g., welders) is not permitted.

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

5.207. Any electrical or electronic equipment in the plant will contribute to the electromagnetic environment that must be withstood by I&C systems important to safety. Therefore, the need to apply limits to electromagnetic emissions applies to all plant equipment, not just equipment important to safety.

5.208. Emission limits placed on individual components should be below the EMI operating envelope by an amount that is sufficient to ensure that no single item makes a significant contribution to the EMI hazard.

5.209. The equipment qualification program should show that electromagnetic emissions of all plant equipment are within the defined limits.

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

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

5.212. DS-431, Ref. [3] gives additional recommendations for electromagnetic compatibility of the electronic elements of the electrical power system.

DESIGN TO COPE WITH AGEING

5.213. 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.

5.214. SSR-2/1 Paragraph 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.

5.215. SSR-2/1 Paragraph 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.

5.216. The qualified service life of electrical and electronics systems and components might be considerably less than plant life.

5.217. Ageing mechanisms that could significantly affect electrical components, and means for following the effects of these mechanisms, should be identified during design.

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

5.219. Ageing is most commonly due to heat, and radiation exposure. Nevertheless, the possibility that other phenomena (e.g., mechanical vibration or chemical degradation) might be relevant to a specific component must be considered.

5.220. Maintenance and surveillance programs should include activities to identify any trend towards degradation (ageing) that could result in the loss of operability of equipment.

5.221. Examples of monitoring techniques include:

- Equipment testing (of plant components or components subject to ageing representative of plant components);
- Visual inspections; and
- Analysis of operating experience.

5.222. Examples of means to address ageing impacts include:

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

5.223. The qualified life of safety components that must perform their safety function in harsh environments should be determined.

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

5.225. On-going qualification might show that the qualified life of a component is validated or is indicated to be different than the expected lifetime. Information from on-going qualification may be used to increase or decrease the qualified life of a component.

5.226. NS-G-2.12, Ref. [12] gives additional guidance on ageing management including the interface between equipment qualification and the ageing management program.

CONTROL OF ACCESS

5.227. 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.

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

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

5.230. Areas of particular concern are access to set-point adjustments and calibration adjustments, because of their important to preventing degraded system performance due to potential errors in operation or maintenance.

5.231. IAEA Nuclear Security Series No. 4 Ref. [17], and 13 Ref. [18] give guidance on security for nuclear power plants and the coordination of nuclear safety and security.

5.232. DS-431, Ref. [3] gives additional recommendations for access control and security of computer-based applications used in electrical power systems.

SURVEILLANCE TESTING AND TESTABILITY

Test Provisions

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

5.234. Design of test provisions must be coordinated with the design of the operational test program in order that availability requirements of the systems and components are fulfilled. This includes establishing test frequencies that take into consideration failure rates of components. It is envisaged that certain tests could only be performed during refuelling outages.

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

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

5.237. Periodic tests during plant operation will normally be needed to achieve the reliability required of safety systems; however it is sometimes desirable to avoid conducting tests during operation if they put at risk safe plant operation.

5.238. The capability for testing and calibration during power operation is not necessary if doing so would adversely affect the safety or operability of the plant.

5.239. 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 affected is acceptable, and**
- **b. The capability for testing during shutdown.**

Test program

5.240. The design of systems important to safety should include identification of a testing program that supports implementation of the guidance given in NS-G-2.2, Ref. [9]; NS-G-2.4, Ref. [10], NS-G-2.6, Ref. [11]; and NS-G-2.14, Ref. [13].

5.241. A test program will normally include:

- A description of program 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 required documentation and reports;
- Periodic review of program effectiveness;
- The individual test procedures that will be used to control the conduct of tests.

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

5.243. Implementation of the test program should provide:

- **a. Objective information on system or component status;**
- **b. Assessment of component degradation;**
- **c. Data on trends to assist in detecting degradation; and**
- **d. Indications of incipient failure within the system.**

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

5.245. The test program for electronic components of electrical power systems, including electronic protective devices, should also meet applicable parts of guidance in the DS-431, Ref. [3].

Test procedures

5.246. Procedures for periodic test of systems important to safety should:

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 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 actual, or simulated, operating conditions present 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; and

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

5.247. 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 minimize risks to maintenance personnel.

5.248. 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.

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

- Avoiding locating equipment in areas where conditions of extreme temperature, or humidity are normal.

- Avoiding locating equipment in areas where there is a risk of high radiation levels.
- Design that takes account of human capabilities and limitations in performing the required maintenance activities.
- Leaving sufficient room around the equipment to ensure that the maintenance staff can perform their tasks under normal working conditions.

5.250. All systems and components should have maintenance plans.

PROVISIONS FOR REMOVAL FROM SERVICE FOR TESTING OR MAINTENANCE

5.251. If 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 maintenance system is not possible without deliberate manual intervention.

5.252. The design should ensure that the system couldn't unknowingly be left in a test or maintenance configuration.

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

5.254. In safety systems it is important that design features ensure that, during periodic tests of part of a safety system, the parts remaining in service can perform the required safety task.

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

5.256. For frequently bypassed items these indications should be automatic.

5.257. NS-G-2.6, Ref. [11] provides guidance for returning systems and equipment to service after testing and maintenance.

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

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

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

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

5.260. Electrical power systems or components important to safety should not be shared between reactor units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cool-down of the remaining units.

5.261. Any demonstration that sharing of systems or components between units does not increase the likelihood or consequences of an accident should consider 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.

5.262. In applying the single-failure criterion to units with shared systems the analysis should show the following conditions are met regarding the units sharing systems or components:

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

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

5.263. It is not necessary to show that conditions a) and b) can be simultaneously met.

MARKING AND IDENTIFICATION

5.264. SSR-2/1 Paragraph 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.

5.265. A consistent and coherent method of naming and identifying all electric power components should be determined and followed throughout the design, installation and operation phases of the plant.

5.266. The method of naming and identifying electrical power components should not require frequent reference to drawings, manuals, or other reference material.

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

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

5.269. Coherent and easily understood naming and identification of systems and components is important for engineering, maintenance, and construction staff as well as for use to label the controls, displays, and indications. For example, it reduces the likelihood of inadvertently performing maintenance, tests, repair or calibration on an incorrect channel.

5.270. 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, modules and embedded computer software.

CONTAINMENT ELECTRICAL PENETRATIONS

5.271. All containment electrical penetration assemblies should be classified as safety.

5.272. Electrical penetrations are elements of accomplishing the containment safety function and will always be safety classified. Structural integrity functions include the ability to withstand rated and fault currents without the penetration leak rate exceeding 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 upon the penetration. .

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

5.274. 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 a 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 during all plant states without exceeding allowable conductor temperatures, degrading the assembly pressure boundaries;

d. To safely carry short circuits over the period of time required for the protective device to clear a fault currents, accounting for credible voltage variations; and

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

5.275. The setting of the protection devices should consider the continuous current ratings and capabilities of the electrical penetrations.

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

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

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

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

DISTRIBUTION SYSTEMS

Capability

5.280. Each distribution system should have sufficient capacity and capability to:

a. Supply the required loads under all required operating conditions;

b. Withstand the maximum credible overcurrent under electrical fault conditions;

c. Withstand transient conditions without damage to, or adverse effects on, any of its components; and

d. Switch power supplies and loads as demanded.

Protective devices of the main and branch circuits and loads

5.281. All main and branch circuits should be protected against overloads and short circuits and be supervised for ground faults and protected when applicable.

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

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

5.284. The co-ordination 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.

5.285. The function of the protective devices is to minimize equipment damage and any 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.

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

CONTROLS AND MONITORING

5.287. Sufficient instrumentation and control equipment should be provided in the main control room to monitor and control the onsite and offsite power systems.

5.288. The human machine interface (HMI) for electrical power systems should comply with the HMI recommendations of DS-431, Ref. [3].

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

- **a. Breaker positions (safety power system, power sources and large loads);**
- **b. Busbar voltage and current; and**
- **c. Standby power source voltage, current and frequency.**

5.290. Indication of bypasses and equipment taken out of service should be provided.

5.291. Procedures should exist for operation of the power systems during all plant states and electrical events.

5.292. 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 safety functions that are assigned to that location.

5.293. 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.

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

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

5.296. In order to substantiate a claim 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 judgements 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; and**
- **e. The communication links between operators carrying out the actions are adequate to ensure the correct performance of these actions.**

5.297. Means should also be provided to manually initiate safety actions at system level and at component levels. Manual initiation of safety action provides a form of defence in depth for abnormal situations and supports long-term post accident operation.

5.298. 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 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; and

g. Manual switching to facilitate testing, maintenance and repair during normal operation or shutdown;

5.299. Automatic load sequencers should work correctly irrespective of the actual sequence of demand, i.e., the loss of offsite power and an accident signal can occur in any sequence.

NON-SAFETY CLASSIFIED STANDBY AC POWER SOURCES

5.300. Some designs have standby AC power sources that are not safety classified. The general guidance for safety standby AC power sources applies, but the degree of equipment qualification, design confirmation and documentation is according to principles for safety-related or non-safety components.

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

5.302. 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 NPP with power during startup, shutdown and during emergency situations in a stable and continuous way.

6.3. The preferred power supply to the safety power systems is from the grid. During 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 NPP in a stable and continuous way.

6.5. This applies also after anticipated grid events when the plant stays 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 CCF caused by events on the grid, switchyard or main generator, it might be investigated if the different divisions of the NPP Electrical Power Systems could be connected to different preferred power supplies without significantly increased risk for undue trips and other disturbances.

RELIABILITY OF PROTECTION 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 contribute to a reliable preferred power supply.

6.8. Events to be considered in the design of the grid connection and 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, and
- Events such as winding-to-winding faults in transformers and loss of one phase of the grid connection.

OFF-SITE POWER SUPPLIES

6.9. Offsite power should be supplied by two or more physically independent offsite supplies designed and located in order to minimize, to the extent practical, the likelihood of their simultaneous failure.

6.10. 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 itself.

6.11. In areas with high risk of pollution increased insulator length may be needed to ensure that insulator contamination is not a threat of common cause failure of both offsite supplies.

6.12. Nuclear power plants with a single transmission line might have a higher forced outage rate owing to line tripping. This is particularly important 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 limits unless the plant is designed to withstand the effects of the forced outages or that measures are taken to reduce the number of forced outages, possibly by adding additional transmission lines and greater level of protection.

6.13. A single transmission line for each offsite power supply may be acceptable if this achieves the technical safety objectives as defined in SSR-2/1, Ref. [1].

6.14. A single offsite power supply might be acceptable for some reactor designs (usually with passive engineered safety features) if it is shown in the safety analyses report that it is sufficient with one offsite power connection.

6.15. Each plant’s off-site power supplies should have the capacity and capability to power all plant electrical loads under all plant conditions.

6.16. Attention must be paid to the fact that voltage levels on the grid might be different when the plant is shutdown.

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

6.18. The offsite power supplies provided to meet this recommendation may be shared among two or more plants or units, or they may have separately dedicated circuits.

6.19. For multi unit sites, a single offsite power supply may be acceptable for some reactor designs if it is shown in the safety analyses report that it is sufficient with one offsite power connection.

6.20. Where offsite supplies are shared between multiple units the ability to disconnect a unit should not affect the availability of offsite supply to any other units.

AVAILABILITY

6.21. It is preferable if at least one offsite power circuit is directly connected to each division of the safety power systems without intervening connections to non-safety buses. See figures 1, 2, and 5 for examples.

6.22. A minimum of one offsite circuit should be designed to be automatically available to provide power to its associated safety divisions within a few seconds following a design basis accident to meet the accident analysis requirements.

6.23. A second offsite circuit should be designed to be available within a short time period.

6.24. Preferably the second circuit would also be available within a few seconds following a design basis accident.

6.25. The transfer scheme of the auxiliary loads needs to be evaluated as a part of the safety requirements of the design.

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

6.27. Switching between two live circuits is not performed without risk and the transfer capability is only to be used when actually needed. It is preferred to energize from the second circuit after loss of voltage from the primary circuit. Interlocks between breakers may be used to preclude paralleling circuits that may result in adverse voltage or current conditions on common buses.

6.28. The design of the transfer sequence should consider variations in voltage and inrush currents during the transfer.

6.29. The more reliable power supply should be selected for use during normal plant operation.

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

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

6.32. 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 generator power output to levels sufficient to meet the electrical power needs of the disconnected plant (the house load) without tripping the steam supply or the turbo generator. This transfer to house load operation will result in frequency and voltage excursions before stable operation is achieved.

6.33. A generator circuit breaker may be used as a means to immediately power the onsite AC power systems from the offsite circuits following a main generator trip. Generator load break switches can be used as for this purpose, but the switchover will not be immediate.

INDEPENDENCE

6.34. Two offsite circuits should be designed and located to minimize, to the extent practical, the likelihood of their simultaneous failure under all plant conditions and design basis environmental conditions.

6.35. Examples of events that could cause simultaneous failure of both offsite circuits include:

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

SWITCHYARD

6.36. The physical design of the switchyard should minimize the possibility that a single equipment failure will cause the failure of offsite circuits that are credited with supplying safety loads.

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

6.38. The switchyard control power should be unique to the switchyard and not be fed from the NPP safety control power supplies.

6.39. Control circuits to outdoor switchyards should be equipped with overvoltage protection when entering the plant and be isolated from the control circuits inside the plant.

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

6.41. Protective systems should minimize the probability of failure of both offsite circuits that are credited with supplying safety loads.

6.42. Design features suggested for consideration include:

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

GRID STABILITY AND RELIABILITY

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

6.44. It is important that the grid have enough running inertia in order to make certain that loss of a big generating unit, a trip of the nuclear power plant or busbar faults in the grid do not jeopardize the grid stability.

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

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

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

6.47. The NPP operator and transmission system operator should identify and establish the equipment interface and communication interface requirements for the purpose of ensuring nuclear plant safe operation and shutdown.

6.48. In many countries the energy market is going toward liberalization with splitting of the Electrical system and establishment of Production Companies, Transmission Companies and Distribution Companies.

6.49. It needs to be taken into account that operation of Nuclear power plants requires particular coordination between Transmission System Operator and nuclear power plant operator. This cooperation is based on the common goal to assure nuclear safety and electrical system security (the former prevailing upon the latter). Therefore, it is important to established precise a channel of communications, operative procedures and preferred corridors to supply energy to the nuclear power plant during shutdowns or accident conditions. Operating experience feedback also plays an important role in the communication between the nuclear power plant and transmission system operator. One or more transmission system operators can supply the nuclear power plant.

6.50. There is a need for close cooperation between the Transmission System Operator and the Nuclear Power Plant operator in maintenance planning and outage planning.

6.51. The nuclear power plant operator should identify and establish the equipment interface and communication interface agreements including maintenance requirements with the switchyard or transmission system operators for the purpose of ensuring nuclear plant safe operation and shutdown.

6.52. Experience has shown that a formal agreement between Nuclear power plant operator and transmission system operator on coordination of planning, including definition of responsibilities, is beneficial.

6.53. It is important that the Nuclear Power Plant Operator notify the Transmission System Operator regarding outages, modifications and maintenance activities as well as any changes to the plant design, configuration, operations, limits, electrical protection systems, or capabilities that would impact the ability of the Transmission System Operator to meet the current requirements.

6.54. It is also important that the Transmission System Operator notify the Nuclear Power Plant operator regarding outages, modifications and maintenance activities that could impact 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.

6.55. The Nuclear Power Plant operator 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.

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

6.57. The Nuclear Power Plant operator 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.

6.58. The Nuclear Power Plant operator should ensure that the licensing and design requirements of the plant are understood by the transmission system operator in order to prevent challenges to nuclear safety as a result of transmission system disturbances, transients, or operating conditions.

6.59. 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 and electrical protection equipment) in the Nuclear Power Plant switchyard, and the transmission circuits that connect to it, is maintained to a higher standard, or is tested or inspected more frequently, than other grid equipment.

6.60. Note that structures, systems, and components of preferred power supply (e.g., switchyard or grid) that are not under the direct control of the plant operator and the nuclear regulator, are nevertheless site characteristics required to maintain plant safety.

6.61. The preferred power characteristics that are essential to plant safety, including compliance with the recommendations of this guide, should be documented in the plant safety analysis and ensured by the licensee.

RELIABILITY ASSESSMENT OF GRID CONNECTIONS

6.62. To ensure that the Nuclear Power Plant has adequate electrical power (voltage and frequency) from the grid, analyses should be performed on a regular basis.

6.63. Factors to be considered in these analyses include loss of generation by the nuclear plant, any other critical generation source, or loss of power from a transmission system element, the failure rate of protection devices and transmission system breakers and other equipment.

6.64. D-NG-T-3.8, Ref. [20] gives additional background on integration of Nuclear Power Plants and the power grid.

7. DESIGN GUIDELINES FOR ELECTRICAL SAFETY POWER SYSTEMS

GENERAL

7.1. The variations of voltage and frequency in the Nuclear Power Plant's electrical power system during 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 voltage and frequency variations and transients on the safety-classified buses that could result from events on the preferred power supply or in any of the onsite electrical power systems, and to confirm the adequacy of the protection scheme.

7.3. Examples of events to consider are given in chapter 5.

7.4. Standby power supplies used for onsite power systems will have voltage and frequency variations during load sequencing. The magnitude of these variations might impact equipment that is starting, already sequenced or operating. Therefore, it is important to evaluate the effects of voltage and frequency variations.

7.5. It is important that the analyses consider all modes of operation and both symmetrical and asymmetrical events. An event could challenge different components in the electrical systems, depending on rise time, fault time, amplitude or asymmetry.

Bus monitoring and switching

7.6. Degradation of the preferred power supply of each safety power system bus (i.e. overvoltage, undervoltage, overfrequency, and underfrequency) should be detected on the buses of the safety AC power systems.

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

7.8. After a bus is disconnected from a degraded preferred power supply, the bus should be automatically connected directly to alternative sources in the order given below.

- **a. The alternative off-site power source,**
- **b. The standby power source for that division of the safety power system,**

7.9. A time delay may be associated with the disconnection to allow the system to ride through minor disturbances. The time delay must be supported by the assumptions in the accident analyses.

7.10. It is preferred that two breakers be provided to disconnect each preferred power supply feed to a safety system bus. See, for example, Figure 3.

7.11. If automatic connection to the alternative preferred power source is not used, it must be shown that this is in accordance with the safety criteria of the plant.

7.12. 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 for the plant.

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

7.14. Bus voltage and frequency monitoring schemes for protection against degraded voltage, degraded frequency, or loss of voltage should meet the following criteria.

- **a. Bus voltage and frequency should be detected directly from the safety system buses to which the standby sources are to be connected.**
- **b. Voltage or frequency degradation should be alarmed in the MCR.**
- **c. Voltage or frequency degradation below acceptable limits should automatically disconnect the affected supply from the safety buses.**

  Two levels of voltage protection with different time delays are needed: one level to detect loss of offsite power at the safety buses; and a second level for degraded voltage.

d. On sensing unacceptable high voltage on a preferred power supply, the affected preferred power supply should be automatically disconnected from the safety system buses.

1. **The setpoint and time delay should be coordinated with the overvoltage capability of connected equipment.**
2. **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 nor prevent correct operation of the 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 for test and calibration during power operation should be provided.

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

7.15. Voltage monitoring, used only for alarms, does not have to meet the guidance of paragraph 7.14.

7.16. The undervoltage and time delay setpoints for degraded voltage protection should be determined from an analysis of the voltage requirements of the safety loads at all onsite system distribution levels.

7.17. Improper voltage protection logic can cause adverse effects on the safety systems and equipment such as spurious shedding of safety loads from the standby diesel generators and spurious separation of safety systems from offsite power due to normal motor starting transients.

DESIGN FOR RELIABILITY

Single failure criterion

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

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

7.19. SSR-2/1 Paragraph 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.

7.20. SSR-2/1 Paragraph 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.

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

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

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

a. Any single detectable failure within the safety system;

b. All failures caused by the single failure;

c. All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety function; and

d. The removal from service or bypassed of safety channels for testing or maintenance that is allowed by plant operating limits and conditions.

7.24. Single failures include hardware failures, individual operator errors, and any failures caused by a single failure, including all cascading failures expected to result from the single failure. Both operator errors of commission (taking an incorrect action) and omission (failing to take a necessary action) are to be considered.

7.25. Common-cause failures to be considered include cascading failures and failures expected to be caused by a postulated initiating event. Other common-cause failures do not need to be part of the analysis. Examples of such excluded common-cause failures include failures of components due to:

- Environmental conditions for which they have been qualified,
- Design deficiencies,
- Manufacturing errors,
- Installation errors,
- Maintenance errors, and
- Operator errors.

7.26. Design qualification, diversity, personnel training, human factors engineering, and effective operating, maintenance, and surveillance procedures are expected to afford protection from such common-cause failures.

7.27. Non-compliance with the single failure criterion should be exceptional and 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 discounted.

7.29. Reliability analysis, probabilistic assessment, operating experience, engineering judgment or a combination of these may be used to establish a basis from 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 significance and potential impact on core damage frequency.

7.31. The situations in which the single failure criterion is not met in the case of maintenance, repair or testing need to be consistent with plant operating limits and conditions.

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

Completion of protective action

7.33. The safety power systems and its 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 stand-by 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 power sources should consist of an electrical generating unit complete with all auxiliaries and 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. If multiple power sources are used per division it must be demonstrated that this is a reliable configuration.

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

7.39. 7.40a. At the design stage margin to account for future load growth is needed in the capacity specifications.

7.40. When standby AC power source capacity is calculated, margins must account for loads that might operate at run-out conditions and for loads that might operate in an overload condition.

7.41. Diesel Generators are specified to operate at a fixed voltage and frequency during the emergency mode of operation. In general, the steady state voltage and frequency is maintained within an allowable tolerance of ± 2% relative to the specified value. When electric motors are subjected to voltages, below the nameplate rating, some of the characteristics will change slightly and current consumption will increase. A variation in frequency affects the torque developed by motors. The capability of motor driven pumps to deliver required flows must be evaluated for the generator operation at lower end of frequency. Similarly, the change in load characteristics due to generator operation at the lower or upper end of the allowable voltage and frequency range must be evaluated for impact on generator overall loading capability.

7.42. Any equipment derating, due for example, to higher temperature in in-take air, environmental conditions or fuel temperature, must be considered.

7.43. 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 is typically provided. This provides assurance that the power source can handle the short-time loading at the onset of an event when accident mitigating fluid systems are realigning for injection or cooling system operation and pumps are operating at run out conditions or with higher flow than assumed in thermo hydraulic analyses. The thermo hydraulic analyses are normally conservative in such a way that the expected power consumption of motors might be underestimated.

7.44. It should be demonstrated that the stand-by 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 upon loss of preferred power supply to the essential buses.

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

7.47. The time to start the standby AC power source and connect loads to this source must be consistent with the startup time assumptions of the safety analysis.

7.48. Onsite sources of fuel and other consumables (such as lube oil) should be sufficient to operate the standby power sources until offsite power supply can be restored.

7.49. Off-site sources of fuel and other consumables may be depended upon if sources of replenishment are identified and on-site sources of are sufficient for the time required to replenish supplies. In most member states onsite sources are sized for 1 to 2 weeks of operation without replenishment from external sources.

7.50. I&C used for the starting, coupling, running and protection of a standby power source should be supplied by batteries within its own division.

7.51. The loss of the DC power source within the same division as the standby power source could lead to the unavailability of the standby AC power source, but it would also cause loss of other functions in the division, making the standby AC supply in that division not required.

7.52. When using batteries specifically dedicated to the standby power source, they must be subject to the adequate surveillance as any safety system battery. Use of station batteries for control power is preferred because it is more likely that failure of station batteries will be detected.

7.53. Standby power sources should be independent of electrical power sources outside its own division.

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

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

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

7.57. Equipment that is not safety classified either should be automatically disconnected on an accident signal or be connected to the safety power system by means of isolation devices.

7.58. The isolation devices between a safety power system and non-safety classified loads 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 start of non-safety loads after safety loads are started and it is determined that there is enough capacity for start and operation of the non-safety load.

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 stand-by AC power source should be made operable in normal stand-by 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 are the formation of soot in diesels being tested under no-load conditions, inadequate provisions for restoring to normal stand-by conditions after completion of the test or introducing 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 is permitted, if voltage and frequency is restored well before the next load is connected and if the voltage on motor terminals are 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 only exist during accident conditions, must normally be 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 failures should be in service during all modes of standby power source operation.

7.72. Examples of such devices include those that protect the:

- Standby power source from catastrophic failure, such as over speed and generator differential protection,
- Safety power system from catastrophic failures, such as backup overcurrent and low impedance 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 individually testing each trip 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 power sources

7.76. Support system equipment (e.g. ventilation, cooling water pumps and lubrication) 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. Redundancy of support systems might add to the reliability of the standby power source. If multiple circuits are used, surveillance testing must verify that all circuits are available and operable.

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

7.79. Starting systems typically have the capacity to support at least 5 starts. In order to support this, it is normally necessary to abort any starting attempt after a specified time in order to preserve resources.

Fuel for standby power sources

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

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

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

7.83. Normally samples for testing of fuel will be taken on site.

DC POWER SYSTEMS

General

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

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

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

7.87. 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

7.88. Each battery set should, without battery charger, be capable of meeting all required load demands and conditions (including duty cycles and electrical transients) occurring 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.

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

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

7.91. If forced ventilation is needed:

a. The battery room ventilation system should be powered from the same division as the battery in the affected room; and

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

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

7.93. Periodic testing will usually be based on recommendations for each type of battery and typically a battery capacity test on an interval of 1 to 5 years, depending upon battery condition, 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, and
- Temperature of a representative cell.

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

7.95. Battery capacity and lifetime is temperature dependent.

7.96. Battery fuses should be monitored.

Battery charger

7.97. Each battery should have its own battery charger.

7.98. Each battery charger should have sufficient capacity to:

a. Maintain the battery in a fully charged condition during normal operation;

b. 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 and accident loads following loss of normal power.

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

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

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

7.102. Battery chargers should keep the output voltage within the operating range of DC voltage:

a. When the AC input voltage goes low during fault clearing on the supply side and returns to a high voltage.

When clearing faults on the transmission system close to the plant, typical duration is 100 – 250 ms., and when faults happen in the onsite 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 supply. (See Figure 7.) This voltage sag and swell with short rise time might cause severe overvoltage on the DC side of a battery charger.

An effective way is to automatically, with no time delay, shut down the battery charger on AC undervoltage and restart when the supply voltage is normal. This might shield the DC (and uninterruptible AC) power systems from voltage transients induced from 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 figure 8)

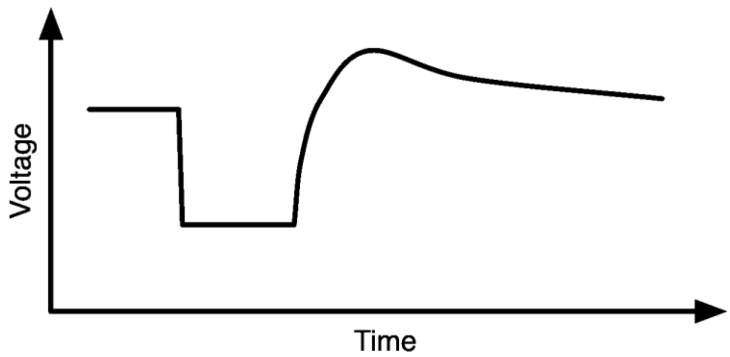


FIG. 7. Typical on-site voltage profile during clearing of transmission system fault, a. Voltage during fault, b. Rapid voltage rise, c. Voltage swell due to generator excitation and return to normal voltage

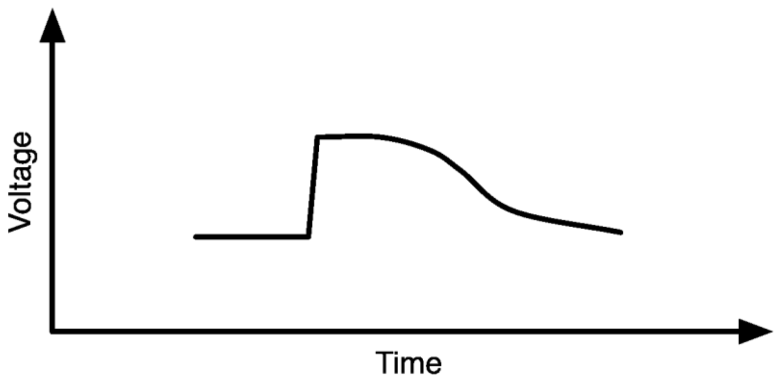


FIG. 8. Typical on-site voltage profile after loss-of-load (conversion to house-load operation)

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

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

7.105. 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

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

7.107. Some plant designs will not need uninterruptible AC power systems. With modern I&C systems it is feasible to power all loads requiring continuous power with DC. Such an approach eliminates a source of failure.

7.108. 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.

7.109. Alternatively the uninterruptible AC safety power supply could be in the form of an uninterruptible power supply (UPS) with dedicated battery charger, battery and inverter.

7.110. If a UPS is used, the guidance given here for battery chargers and batteries also applies.

7.111. 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.

7.112. The limiting case for capacity is normally station blackout.

7.113. An uninterruptible power supply might experience 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.

7.114. Special consideration should be given to the characteristics and design requirements of the loads and the interactions between loads connected to the uninterruptible AC system.

7.115. For example, the design of static inverters must 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

7.116. Battery chargers, inverters and motor generator sets are sources of limited short-circuit current therefore, special attention needs to be given to coordinating protective device sensitivity and system available fault current. Coordination must include the protective devices in the alternate supply, inverters, static switches, battery chargers, distribution panels, instrumentation panels and racks, and other equipment powered from the system.

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

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

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

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

7.121. Coordination for DC power system circuits involves main bus protective devices and the protective devices used in branch circuits, in switchgear control circuits, in relay 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 protection devices need to be used.

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

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

7.125. The battery charger, the battery, and the inverter (or motor-generator set) is a functional unique system because these elements create the "power supply chain" for many uninterruptible loads and have strong interactions among them. Consequently, protection settings must preserve the safety functions. For example, in case of overvoltage on the AC supply to the battery charger, the battery charger must 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.

7.126. Uninterruptible AC power systems should be provided with underfrequency and overfrequency protection.

8. ALTERNATE AC POWER SUPPLIES

8.1. An alternate AC power supply should be provided at or near the plant if the plant's design depends upon AC power for safe response to postulated initiating events.

8.2. Alternate AC power supplies are intended to provide a power supply whose failure simultaneously with the external power transmission grid connections, and due to the same cause, is unlikely. This involves also providing auxiliary systems for the alternate AC power supply and external grid connections, e.g. auxiliary power supplies and automatic switching systems, that are as independent as possible of offsite power and other on-site power supplies.

8.3. The alternate AC power supplies with auxiliaries should be qualified for its 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 and 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, maintaining the reactor sub-critical, and for removing decay heat from spent fuel for all served units 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 for an AAC source, provided that it meets the other criteria 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, and maintain them in a controlled state.

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

8.9. Support systems that maintain the AAC source in readiness may be powered from one or more units, providing it 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 supply.

8.11. No single point of vulnerability should exist whereby a weather-related event, external event, or single active failure could disable any of a unit's safety standby AC power supply and simultaneously fail all offsite power supplies and the alternate AC power supplies.

8.12. Provisions 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 supply only after it has been disconnected from other power supplies.

8.14. The alternate AC power supply may also have the capability to power certain loads needed from defence in depth aspects.

8.15. 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.

8.16. Preferable 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 and habitability systems) that significantly enhance the operators' ability to respond to an event.

9. DESIGN CONFIRMATION AND DOCUMENTATION

MANAGEMENT SYSTEM

9.1. The design of electrical systems important to safety should be conducted within the framework of an overall management system that meets the requirements of GS-R-2, Ref. [14] and follow the recommendations of GS-G-3.1, Ref. [15], and GS-G-3.5, Ref. [16].

VERIFICATION

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

9.3. As part of the design and design verification, the following should be performed and 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 electrical power systems design requirements are met;

c. Demonstration that electrical safety power systems comply with the single failure criteria;

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

e. Demonstration that operation of protective devices have been adequately coordinated;

f. Demonstration that adequate mitigating 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 and generation facilities;

h. Demonstration that the offsite circuits credited with supplying safety loads will continue to have their required capacity and capability in the presence of: loss of the nuclear plant, loss of the largest generating unit, loss of the largest transmission circuit or intertie, or loss of the largest load.

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

9.5. The demonstration of the off-site circuits' reliability and availability must be performed together with the transmission system operator. (Refer to chapter 6.)

9.6. For all systems important to safety a systematic assessment should be conducted to confirm that the design achieves the reliability requirements of the system design basis.

9.7. This demonstration may be based on a balance of application of deterministic criteria and quantitative reliability analysis that considers design features such as, for example, redundancy, testability, failure modes, and rigor of qualification.

9.8. The use of software or complex multi-element logic modules might provide difficulties in justification of reliability and sensitivity to common cause failures. The reliability may therefore depend on assurances of freedom from error in the design and implementation process.

9.9. Test facilities that are part of the safety system must be considered when determining system availability.

9.10. Analytical tools used in design and analysis of electrical 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 by paragraph 9.2-9.10 are part of the plant safety assessment. NS-G-1.2, Ref. [4] provides additional guidance on safety assessment.

Testing

9.12. Provisions should be made in the design to ensure that the following test programs can be implemented without endangering the safety of the plant during testing:

a. A pre-operational test program to demonstrate the operational and emergency modes 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 program 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 components within the system.

9.13. General recommendations on measures for verifying the adequacy of the design are given in GS-G-3.5, Ref. [16] paragraphs 5.114 to 5.134.

9.14. A major consideration of pre-operational test programs for electrical power systems is to confirm, before entering into operation, and after major modifications, the independence between divisions of the safety power systems. Normally this involves testing to verify that all on-site power systems and their load groups can successfully operate and is 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:

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 test and maintenance requirements for electrical power systems and equipment;

l. Documentation of acceptance and commissioning tests for electrical power systems and equipment;

m. Quality assurance 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, and

4. From the main generator.

o. Steady-state load and voltage profile studies that show the voltages throughout the power system for various modes of plant operation (and generator load/ power factor), including design basis events, at the time of normal and degraded voltage conditions.

p. Transient load and voltage studies that show the profile of the loads that are sequentially applied to the preferred and standby power supplies during various modes of plant operation.

q. A power system study that examines loading and voltages in the DC power systems supplying alternating current and direct current systems during various modes of plant operation.

r. A bus transfer study that analyses the impact of voltage, phase angle, frequency, and the effect of motor reacceleration on buses and motors before, during, and immediately after automatic bus transfers.

s. 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, to be used to analyse the fault clearing capability of the electrical equipment.

t. Protective device coordination and equipment protection studies that show proper setpoint selection in all of the protective schemes;

u. Analysis of fuel storage capacities for standby power sources;

v. Analysis of the consequences of partial or total loss of power supplies;

w. Equipment qualification plans, analyses, and test reports, and

x. 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 Electric Power Systems of Nuclear Power Plants, Safety Guide Series NS-G-1.8, IAEA, Vienna (2004).

[3] International Atomic Energy Agency, Design of Instrumentation and Control Systems for Nuclear Power Plants, Safety Standard Series No. DS-431, IAEA, Vienna (Draft 03 August 2011).

[4] International Atomic Energy Agency, Safety Assessment and Verification for Nuclear Power Plants, Safety Guide Series No. NS-G-1.2, IAEA, Vienna (2001).

[5] International Atomic Energy Agency, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Guide Series No. NS-G-1.5, IAEA, Vienna (2003).

[6] International Atomic Energy Agency, Seismic Design and Qualification for Nuclear Power Plants, Safety Guide Series No. NS-G-1.6, IAEA, Vienna (2003).

[7] International Atomic Energy Agency, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, Safety Guide Series No. NS-G-1.7, IAEA, Vienna (2004).

[8] International Atomic Energy Agency, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, Safety Guide Series No. NS-G-1.11, IAEA, Vienna (2004).

[9] International Atomic Energy Agency, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Safety Guide Series No. NS-G-2.2, IAEA, Vienna (2000).

[10] International Atomic Energy Agency, The Operating Organization for Nuclear Power Plants, Safety Guide Series No. NS-G-2.4, IAEA, Vienna (2002).

[11] International Atomic Energy Agency, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, Safety Guide Series No. NS-G-2.6, IAEA, Vienna (2001).

[12] International Atomic Energy Agency, Ageing Management for Nuclear Power Plants, Safety Guide Series No. NS-G-2.12, IAEA, Vienna (2009).

[13] International Atomic Energy Agency, Conduct of Operations at Nuclear Power Plants, Safety Guide Series No. NS-G-2.14, IAEA, Vienna (2008).

[14] International Atomic Energy Agency, The Management System for Facilities and Activities, Safety Requirements No. GS-R-3, IAEA, Vienna (2006).

[15] International Atomic Energy Agency Safety Guide, Application for the Management System for Facilities and Activities, Safety Guides Series No. GS-G-3.1, IAEA, Vienna (2006).

[16] International Atomic Energy Agency, The Management System for Nuclear Installations, Safety Guide Safety Guide GS-G-3.5, IAEA, Vienna (2009).

[17] International Atomic Energy Agency, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, Nuclear Security Series No. 4, IAEA, Vienna (2007).

[18] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), Nuclear Security Series No. 13, IAEA, Vienna (2007).

[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, Electric Grid Reliability and Interface with Nuclear Power Plants, D-NG-T-3.8, Vienna (in publication).

[21] International Atomic Energy Agency, 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. Due 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 needed 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 all types of events challenging the barriers against radiological releases and also during design extension conditions.

I-3. Any electrical event or disturbance that happens in the electrical systems must be handled in such a manner that the safety functions of the power plant can be carried out.

I-4. Operating experience shows that loss of transmission systems or failures in the on-site power systems could degrade the safety of the plant as described in.Ref.[19].

I-5. The system characteristics needed to accomplish reliable and robust electrical systems supplying the safety functions must be multiple and overlapping, forming the different levels of a defence-in-depth concept. They must cover grid 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 needed, the complete on-site and off-site power systems contribute to the reliability and robustness.

I-6. Support features for the electrical power systems are control and monitoring, part of the main and supplementary control room complex, and procedures for operation of the power systems during all plant states and electrical events.

I-7. Table I-1 summarizes the electrical power system features that support the levels of defence in depth defined in SSR-2/1.

FIRST LEVEL

Design bases

I-8. The design bases for the on-site electrical systems are the fundamental base for reliability and robustness. The bases account for the continuous operating range of voltage and frequency, all possible events that could cause transient, dynamic or continuous variations of them, and internal and external hazards that threaten the availability of power supply to the plant. As a nuclear power plant is a generating facility, the voltage and frequency excursions that will arise from different events will be different from normal industrial events. Figure I-1 gives an example of voltage and frequency variations that will affect the on-site power systems in a generating unit during an anticipated operating event.

I-9. Incomplete design bases, resulting in equipment not qualified for the intended function, cannot be solved by redundancy or diversity.

The grid

I-10. The grid is part of the preferred power supply for the plant and the safety power systems. During power operation, the power supply to the plant is normally from the generator, which will dampen variations from the grid.

TABLE I-1. ELECTRICAL POWER SUPPLY SUPPORT FOR THE PLANT DEFENCE IN DEPTH CONCEPT

Levels of defence in depth	Objective (From INSAG-12)	Essential means (From INSAG-12)	Applied to plant electrical power systems	Guidance in Safety Guide chapter
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, limiting, and protection systems and other surveillance features	Robust and reliable fault clearing system and protection coordination, 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 releases of radioactive materials	Off-site emergency response	Not part of this guide	

I-11. The grid should provide stable off-site power; that is, it should be capable of withstanding load variations and anticipated events on the transmission system without exceeding the specified voltage and frequency limits. More aspects on integration of nuclear power plants and the grid are given in D-NG-T-3.8, Ref. [20].

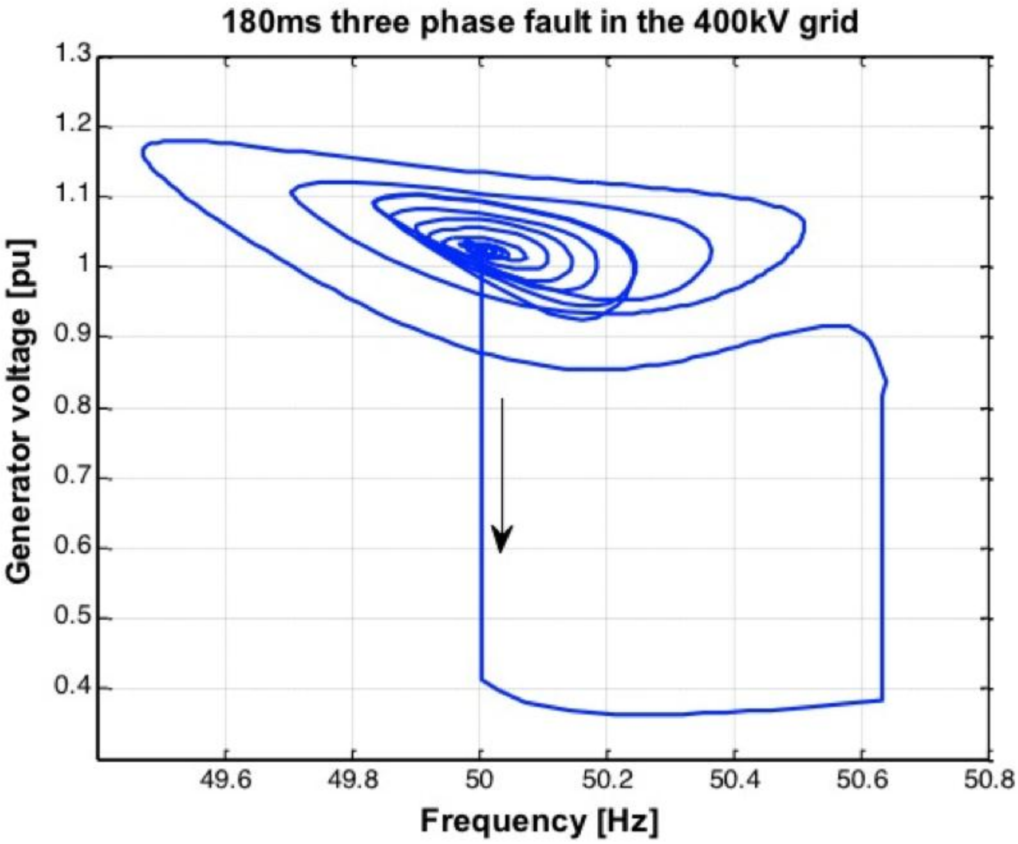


FIG. I-1. Example of on-site voltage (y-axis) and frequency (x-axis) variations during fault clearing on the transmission system

I-12. The reliability of the grid calls for close cooperation between the power plant operator and the transmission system operator. Grid availability is essential as part of the licensing base for the nuclear plant and especially when the plant is shut down, attention must be given to the predicted and actual voltage variations in the grid supply..The grid is normally designed to cope with a loss of a transmission line without any reduction of capabilities. Such a loss could affect the power plant and provisions should be taken to minimize such incidents close to the plant. Agreements on maintenance programs and procedures should exist between the plant and the transmission system operator.

I-13. Modification to the grid might have an impact on the nuclear plant and vice versa. Any such modifications should be communicated and evaluated.

I-14. It is preferred that multiple transmission lines connect the power plant to the grid.

Onsite power systems

I-15. The onsite 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 onsite power system implies an installation with low possibility of failure of loads and other equipment. The substantial part of this is covered by national electrical codes, but qualification of equipment (environmental and electrical) as well as equipment specifications based on design bases contribute. Good housekeeping will lessen the risks for faults and a proper understanding of load behaviour will minimize the risk for overload of rotating equipment.

I-16. The deterministic analyses to design and verify the reliable and robust on-site system are part of the safety justification for the nuclear plant.

I-17. The onsite power systems' robustness and reliability needs to be analyzed for the different configurations of the onsite power systems during refuelling outages, when part of the electrical supply is taken out of service.

I-18. The possibility of common cause failures should not be ruled out, as during 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-19. Maintenance programs and procedures should aim for the highest standards, not only for safety systems but also for all parts of the on-site power. Surveillance testing or performance testing is one way of following any degradation of equipment.

I-20. Plant modifications usually have an impact on the electrical power systems. Changes in load behaviour must be evaluated. Also changes in control systems have an impact on battery loading and must be tracked and evaluated.

I-21. 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

Fault clearing system and protection coordination

I-22. In order to minimize the effect of any faults in the electrical power systems there is a need for protection coordination and a fault-clearing system that will only disconnect the faulted equipment. If the primary protection or fault-clearing device fails, there should be adequate backup.

I-23. Since battery chargers, inverters, and motor generator sets are generally sources of limited short-circuit current, special attention should be given to coordinating protective device sensitivity and system available fault current.

I-24. Protection coordination must work properly both during power operation and during shut down conditions.

Power transfer capability

I-25. Offsite power should be supplied by two physically independent offsite circuits designed and located in order to minimize, to the extent practical, 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 only one offsite power connection is sufficient.

I-26. One of these connections should be designed to be available within a few cycles following a loss-of-coolant accident to assure that core cooling, containment integrity, and other vital safety functions are maintained.

I-27. The transfer to the other offsite circuit should be automatic and should be initiated manually or automatically. A study must be performed that analyses the impact of voltage, phase angle, and frequency on buses and motors before, during, and immediately after a bus transfers. Also reacceleration of motors should be considered in the study.

I-28. There should also be a power transfer capability for the supply of uninterruptible AC power systems.

House-load operation possibilities

I-29. During design of the plant, consideration should be given to the capability to withstand load rejection with runback without undergoing a reactor trip or a turbogenerator trip, in order to continue to supply house loads.

I-30. The transfer to house load is complex, due to reactivity feedback and control of the power decrease. Experience shows that if the initial transient can be handled, operation can keep on for several hours. It adds diversity to power supplies for the plant.

I-31. To achieve house load operation, there must be circuit breakers that 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 where faults occur between the circuit breakers or where there are coincident faults in the plant generator and the grid.

THIRD LEVEL

On-site standby AC power supplies

I-32. The safety systems of the nuclear power plant should be capable of operating from the preferred power supply (i.e. grid or main generator), from the on-site standby AC power supply, or from the alternate AC supply.

I-33. The operability of the standby AC supplies needs to be verified regularly. Starting capability should be tested in such a manner that the test does not have negative effects on the long-term availability of the power source. As an example, diesel engines may be slow-started with limited fuel injection during the majority of surveillance testing.

I-34. Verification of starting and loading capability of the standby AC sources normally has to be a combination of tests and analytical methods to capture design bases events.

I-35. Loads other than safety system loads may derive their power from the safety power system. The loading sequence, after a loss of offsite power, should not automatically start these loads as they might affect the availability of the safety loads. The non-safety loads should only be started after it is determined that there is enough capacity and capability for start and operation.

I-35a. If an external hazard might jeopardize the first and second level of the defence in depth in electrical power systems (e.g. grid connections and house load), the on-site standby AC power supplies must be protected against this hazard. Proper precautions should be based on the principles described in NS-G-1.5 and NS-G-1.6.

Safety power systems

I-36. The safety power systems that supply different loads is of utmost importance for the possibility of the nuclear power plant to handle a wide spectrum of initiating events that could challenge the barriers of the plant.

I-37. Events on the electrical power systems with origin from preferred power supplies can cause common cause failures on all divisions. Hence during design, construction, and operation adequate countermeasures are essential. After loss of preferred power supplies, when the standby AC sources supply one division each, the risk for common cause failures (CCF) from electrical events is negligible as there are no common parts (although the starting sequence of the standby source is sensitive to

CCF). Experience shows that incomplete design bases are the dominating contributor to CCF, in which case component diversity does not lessen the risk.

I-38. CCF 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),
- They have different modes of operation (one of two parallel rectifiers is in operation, the other is switched off), or

CCF due to electrical events is not postulated for passive equipment like busbars, cables and transformers.

I-39. The DC systems are essential for the reliability of the safety power systems, as well as any other onsite or offsite power system. A governing principle should be not to transmit any disturbances on the preferred power supply, with origin offsite or from the generator as a result of an offsite disturbance, to the DC power systems and consequently to the uninterruptible AC power systems. This should be part of the design bases and can be achieved by design or protection devices.

I-40. In order to handle CCF risks for protection devices the same design principles as for I&C equipment should be used, refer to DS-431, Ref. [3].

I-41. Part of the equipment specifications for electrical loads will be the operating range of voltage and frequency for the electrical systems, but knowledge of electrical transients and their impact on the loads is as essential. Understanding of the mechanical load characteristics is needed 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 setting of protective devices.

FOURTH LEVEL

Alternate AC power supply

I-42. The dependence on electrical power for safety functions in a nuclear power plant implies that also station blackout scenarios need to be considered. The time during which a plant can cope with a loss of all AC power sources must be determined. Before this time has elapsed, it should be possible to connect an alternate AC power supply to the plant.

I-42a. Precaution should be taken to ensure that this supply is available and accessible to cope with external hazards and can be connected to the plant within the given time after e.g. earthquake, tsunami or during e.g. flooding, storm.

I-43. This supply should be as independent as possible from the other power sources that can supply the safety power system.

I-44. In multi-unit plants, connections between units can serve the same purpose if only one unit is subject to station blackout.

ANNEX II. ELECTRICAL SYSTEM ANALYSES FOR DESIGN VERIFICATION

II-1. Analytical studies should adequately demonstrate design margins and robustness of the Electrical Power System in a nuclear plant. The analyses and design capabilities should be verified and validated by test or operating experience. This Annex describes some of the key elements of electrical system design that should be performed as part of the power system analyses. The need for analyses applies to both AC and DC systems, but many of the specific topics mentioned apply only to AC systems.

LOAD FLOW STUDIES

II-2. Load flow analysis is an important part of power system calculations since it evaluates the network performance in its normal and emergency operating conditions and establishes the bounding limits for limiting conditions. Load flow studies are performed using computer software that simulates actual steady-state power system operating conditions, enabling the evaluation of bus voltage amplitude and load angle, real and reactive power flow, and losses. Conducting a load flow study using multiple scenarios helps ensure that the power system is adequately designed to satisfy performance criteria. Specifically, load flow studies are commonly used to investigate:

- Component or circuit loading,
- Bus voltage amplitude and load angle,
- Real and reactive power flow,
- Power system losses,
- Proper transformer tap settings,
- Limiting conditions for system operation,
- Bus transfer schemes,
- Optimize circuit usage,
- Practical voltage profiles for postulated conditions, and
- 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 load.
- Electrical circuits should not be overloaded for any postulated operating condition.
- Reactive power flows (generation, import and export) should be within specified limits for all operating conditions.
- During specified contingency conditions, the power quality should not be degraded.
- Harmonic content should be 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 onsite and offsite power sources, during normal operation and plant shutdown.
- Contingency conditions such as outage of lines, transformers and generators for the off-site source coupled with minimum and maximum loading of plant auxiliary system including equipment required to mitigate consequences of an accident.
- Optimize 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 is several times larger than normal full load current when starting them directly on line at full rated voltage. Excessive starting current results in drop in terminal voltage and may result in failure of motor starting due to low starting torques, unnecessary operation of under voltage relays or stalling of other running motors connected to the network. Motor starting studies can help in the selection of best method of starting, the proper motor design, and the proper system design for minimizing the impact of the motor starting. This study might have to be re-evaluated after replacement of motors, depending on motor characteristics.

SHORT CIRCUIT STUDIES

II-5. Short circuit calculations provide currents and voltages on a power system during fault conditions. This information is required to design an adequate protective relaying system and to determine interrupting requirements for circuit breakers at each voltage level and verify stability of system operation. Fault contributions from all operating sources at any given time should be considered. Nuclear power plants have large motors that can provide a significant contribution to the available fault current in the plant auxiliary system. The short circuit calculations should be confirmed when major replacements and major modifications of the electrical power system (onsite or offsite) are implemented and a cumulative evaluation performed periodically.

II-6. Fault conditions can be balanced or un-balanced shunt faults or series (open conductor) faults. Faults may be caused by either short-circuits to ground or between live conductors, or may be caused by broken conductors in one or more phases.

ELECTRICAL PROTECTION COORDINATION STUDIES

II-7. A Short Circuit / 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 the circuits they protect. The goal is to provide power transformers, switchgear, motor control centres, distribution panel boards and other electrical equipment with the required protection. The study also assists with selecting appropriate types, ampere ratings and device settings to ensure selective and rapid interruption of circuits under overload and short circuit conditions to minimize isolation of essential equipment.

II-8. Protective relays should be designed to rapidly actuate equipment used to isolate the faulted portion of the system to prevent equipment damage and with minimum system disruption to ensure continuity of power to unaffected portions 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 and clear the fault in their primary protection zone, backup relays must be able to isolate the fault, after providing sufficient time for the operation of the primary zone relays. The relays must also be able to discriminate between faulted conditions, normal operating conditions and abnormal operating conditions and function for the specific protection for which they are designed. Relay coordination calculations should consider the operating characteristics of the relays, normal operating and withstand characteristics of plant equipment and must determine the optimum relay settings to achieve high reliability of the electrical systems.

II-9. Protective system must also be designed 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-10. Typical protective relays studies include:

- 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 inrush current,
- Coordination with reacceleration currents,
- Coordination with primary-back up pairs,
- Coordination with thermal withstand capabilities, and
- Coordination with safe stall limits for motors.

II-11. Ground fault protection requires unique consideration as fault current magnitudes depend on the system grounding method - solidly 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 ground fault protection solution for such systems. High-impedance ground fault detection is difficult as special relays are needed to measure the ground fault current combined with the unbalance current generated by line phasing and configuration and load unbalance.

LOSS OF VOLTAGE AND DEGRADED VOLTAGE STUDIES

II-12. In addition to protection schemes discussed above, safety equipment at nuclear plants should be 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 can lead to malfunction or damage safety significant equipment.

II-13. Equipment that is considered important to safety, should be protected from two types of low voltage issues:

- Loss of voltage event which implies a sudden sharp voltage drop in the grid system. Typically a nominal delay is allowed for relay actuation to separate onsite busses from the grid if voltage does not recover to normal operating band. Loss of voltage should provide an automatic start signal to the on-site stand-by power sources.
- Degraded voltage event that postulates sustained low voltage conditions for several seconds and subsequent recovery to normal operating band. If the offsite 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. A general philosophy is outlined below:
- The voltage drop/load flow studies done for evaluating offsite power/onsite power system interface should use minimum expected voltage at the plant/grid interface node, demonstrating adequate voltage for starting and running of plant components during normal, abnormal and accident conditions.
- The selection of voltage and time delay setpoints should be determined from an analysis of the operating voltage requirements of the safety significant loads at all onsite system distribution levels.
- The time delay selected shall be based on the following conditions:
- The allowable time delay, including margin should not exceed the maximum time delay that is assumed in the accident analyses;
- The time delay should override the effect of expected short duration grid disturbances, preserving availability of the offsite power source(s): and
- The allowable time duration of a degraded voltage condition at all distribution system levels should not result in failure of safety systems or components.

II-14. A typical scheme for degraded voltage relay involves two separate time delay relays to deal with the following conditions:

- The first time delay should be of a duration that establishes the existence of a sustained degraded voltage condition (i.e., something longer than a motor starting transient). Following this delay, an alarm in the control room should alert the operator to the degraded condition. The subsequent occurrence of an accident signal should immediately separate the safety distribution system from the offsite power system.
- The second time delay should be of a limited duration such that the permanently connected safety loads will not be damaged. Following this delay, if adequate voltages have not been restored, the safety distribution system should be automatically separated from the offsite power system.

TRANSIENT STABILITY STUDIES

II-15. By nature, a power system is continually experiencing disturbances. These may be include loss of production, short-circuits caused by lightning or other fault conditions, sudden large load changes, or a combination of such events. These disturbances may lead to a change in the configuration of the power system. Transient stability study of a power system is needed to determine whether the system will remain stable or not after such major disturbances. The assumed critical fault clearing time (CFCT)[6] with a given off-site power system configuration should be examined with various fault conditions. This CFCT might be specified and described in the Plant’s Safety Analysis Report. The recovery of a power system subjected to a severe large disturbance is of importance to reliable and safe operation of a nuclear plant. Typically the system must be designed and operated in such a way that a specified number of credible contingencies do not result in failure of quality and continuity of power supply to the loads. This requires accurate calculation of the system dynamic behaviour, which

[6] Critical fault clearing time is the maximum fault duration for which a system remains stable.

includes the electro-mechanical dynamic characteristics of the rotating machines, generator controls, reactive power compensators, loads, protective systems and other controls..The degree of the system stability is an important factor in establishing the operating characteristics of the grid system in the vicinity of the nuclear plant. Grid perturbations that lead to loss of synchronism of the power system require separation of the disturbance in a rapid manner to avoid equipment damage or loss of system stability.

II-16. Parameters that can affect transient stability include:

- Synchronous machine parameters,
- Generator step-up transformer impedance,
- Inertia of turbo-generator,
- Transmission Line parameters,
- Circuit breaker and relay characteristics,
- System layout,
- Excitation system, power system stabilizer and generator governor characteristics,
- System grounding, and
- System Controls such as auto reclosing of circuit breakers, single pole switching, load shedding and system inertia.

II-17. Typically, transient stability analysis involves:

- Modelling generators in accordance to their steady state, transient, and sub-transient parameters,
- Simulating transient behaviour for three-phase or line-to-ground faults,
- Modelling motor and motor load torque, slip, current and acceleration curves,
- Simulating generator and motor start-ups,
- Modelling trip/close of circuit breakers, open/close of switches, and actions of relays based on the settings, and
- Plotting generator and motor speed, current, voltage, and power curves after postulated disturbances.

II-18. Breaker operating characteristics, synchronous machine behaviour and system interconnections can be optimized using computer based transient stability analysis.

LIGHTNING PROTECTION AND SYSTEM GROUNDING STUDIES

II-19. 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 to its peak in a few millionths of a second. This energy must be returned to ground very quickly through a low impedance path to preclude equipment damage and injury of personnel.

II-20. Most external systems for lightning protection consist of an air terminal, down conductor and grounding terminal including a network of lightning rods metal conductors, and ground electrodes connected to station ground mat to provide a low resistance path to ground for potential lightning strikes. The internal system for lightning protection will include lightning equi-potential bonding, electrical insulation of the external system and a surge protective device.

II-21. In any generating station there are generally four conceptually identifiable, but not necessarily physically distinct, grounding systems: personnel safety, lightning, electrical system and I&C - including signal grounding. All grounding systems should be finally tied to the one grounding grid.

II-22. Typically, international standards recommend that the grounding electrode resistance of large electrical substations should be 1 Ohm or less.

II-23. Factors that affect lightning protection schemes include:

- Plant ground mat design,
- Soil resistivity, and
- Lightning rod design (copper clad, coated, other noble materials, size and depth, etc.)

II-24. A well-designed station grounding system is essential for protection of power plant equipment from ground faults and lightning strikes.

ELECTROMAGNETIC COMPATIBILITY STUDIES

II-25. International EMC standards on industrial environments may serve as the basis for the requirements provided that they are supplemented, where necessary, to cover the EMC environments of generating power plant components, which might be more demanding. Results of such a study would be the emission level envelope with frequency spectrum and the susceptibility level envelope with frequency spectrum

LIST OF DEFINITIONS

The following definitions are not given in the IAEA Safety Glossary [21].

Alternate AC power source. Dedicated power source that could be used as 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.

Preferred power supply. The power supply from the transmission system up to the safety classified electrical power system. It is composed of transmission system, switchyard, main generator and distribution system up to safety classified electrical power system. Some portions of the preferred power supply are not part of the safety classification scheme.

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 stably maintained for long time.

Station blackout (SBO). Plant condition defined as the complete loss of all AC power from offsite and onsite power sources. DC power and uninterruptible AC power is present as long as batteries can supply the loads. Alternate AC power can be available.

CONTRIBUTORS TO DRAFTING AND REVIEW

Auvinen, K.	Forsmark NPP, Sweden
Diaz, E.	Comision Nacional de Energia Atomico, Argentina
Dubois, A.	IRSN, France
Fredlund, L.	Ringhals AB, Sweden
Frey, W.	GRS, Germany
Giannelli, I-A.	ENEL Engineering and Research Division - ATN, Italy
Givaudan, B.	EDF, France
Goodney, D.	Constellation Energy, USA
Johnson, G.	International Atomic Energy Agency
Jordan, R.	Westinghouse Electric Company, USA
Kim, B-Y	Korea Institute of Nuclear Safety, Republic of Korea
Knutsson, M.	Ringhals AB, Sweden
Krastev, E.	Kozloduy NPP, Bulgaria
Lamell, P.	Forsmark NPP, Sweden
Lindner, L.	ISTec, Germany
Lochthofen, A.	GRS, Germany
Matharu, G.	US Nuclear Regulatory Commission, USA
Mathew, R.	US Nuclear Regulatory Commission, USA
Mauhin, B.	Tractebel Engineering GDF Suez, Belgium
Meiss, S.	BfS, Germany
Padin. C.	Comision Nacional de Energia Atomico, Argentina
Rogers, A.	Private Consultant, Canada
Sarwar, T.	Pakistan Atomic Energy Commission, Pakistan
Schnuerer, G.	ISTec, Germany
Sobott, O.	AREVA, Germany
Yonezawa, T.	Mitsubishi Heavy Industries, Japan
Zhu, O-P.	Korea Institute of Nuclear Safety, Republic of Korea