

IAEA SAFETY STANDARDS SERIES

Design of
Emergency Power Systems
for Nuclear Power Plants

SAFETY GUIDE

No. NS-G-1.8



IAEA
International Atomic Energy Agency

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Safety Fundamentals (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

www-ns.iaea.org/standards/

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related publications are the **Technical Reports Series**, the **Radiological Assessment Reports Series**, the **INSAG Series**, the **TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series**, the **IAEA Services Series** and the **Computer Manual Series**, and **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. The IAEA also issues reports on radiological accidents and other special publications.

DESIGN OF
EMERGENCY POWER SYSTEMS
FOR NUCLEAR POWER PLANTS

The following States are Members of the International Atomic Energy Agency:

| | | |
|-------------------------------------|---------------------------|--|
| AFGHANISTAN | GUATEMALA | PERU |
| ALBANIA | HAITI | PHILIPPINES |
| ALGERIA | HOLY SEE | POLAND |
| ANGOLA | HONDURAS | PORTUGAL |
| ARGENTINA | HUNGARY | QATAR |
| ARMENIA | ICELAND | REPUBLIC OF MOLDOVA |
| AUSTRALIA | INDIA | ROMANIA |
| AUSTRIA | INDONESIA | RUSSIAN FEDERATION |
| AZERBAIJAN | IRAN, ISLAMIC REPUBLIC OF | SAUDI ARABIA |
| BANGLADESH | IRAQ | SENEGAL |
| BELARUS | IRELAND | SERBIA AND MONTENEGRO |
| BELGIUM | ISRAEL | SEYCHELLES |
| BENIN | ITALY | SIERRA LEONE |
| BOLIVIA | JAMAICA | SINGAPORE |
| BOSNIA AND HERZEGOVINA | JAPAN | SLOVAKIA |
| BOTSWANA | JORDAN | SLOVENIA |
| BRAZIL | KAZAKHSTAN | SOUTH AFRICA |
| BULGARIA | KENYA | SPAIN |
| BURKINA FASO | KOREA, REPUBLIC OF | SRI LANKA |
| CAMEROON | KUWAIT | SUDAN |
| CANADA | KYRGYZSTAN | SWEDEN |
| CENTRAL AFRICAN REPUBLIC | LATVIA | SWITZERLAND |
| CHILE | LEBANON | SYRIAN ARAB REPUBLIC |
| CHINA | LIBERIA | TAJKISTAN |
| COLOMBIA | LIBYAN ARAB JAMAHIRIYA | THAILAND |
| COSTA RICA | LIECHTENSTEIN | THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA |
| CÔTE D'IVOIRE | LITHUANIA | TUNISIA |
| CROATIA | LUXEMBOURG | TURKEY |
| CUBA | MADAGASCAR | UGANDA |
| CYPRUS | MALAYSIA | UKRAINE |
| CZECH REPUBLIC | MALI | UNITED ARAB EMIRATES |
| DEMOCRATIC REPUBLIC OF THE CONGO | MALTA | UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND |
| DENMARK | MARSHALL ISLANDS | UNITED REPUBLIC OF TANZANIA |
| DOMINICAN REPUBLIC | MAURITIUS | UNITED STATES OF AMERICA |
| ECUADOR | MEXICO | URUGUAY |
| EGYPT | MONACO | UZBEKISTAN |
| EL SALVADOR | MONGOLIA | VENEZUELA |
| ERITREA | MOROCCO | VIETNAM |
| ESTONIA | MYANMAR | YEMEN |
| ETHIOPIA | NAMIBIA | ZAMBIA |
| FINLAND | NETHERLANDS | ZIMBABWE |
| FRANCE | NEW ZEALAND | |
| GABON | NICARAGUA | |
| GEORGIA | NIGER | |
| GERMANY | NIGERIA | |
| GHANA | NORWAY | |
| GREECE | PAKISTAN | |
| | PANAMA | |
| | PARAGUAY | |

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

© IAEA, 2004

Permission to reproduce or translate the information contained in this publication may be obtained by writing to the International Atomic Energy Agency, Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria.

Printed by the IAEA in Austria

August 2004
STI/PUB/1188

SAFETY STANDARDS SERIES No. NS-G-1.8

DESIGN OF
EMERGENCY POWER SYSTEMS
FOR NUCLEAR POWER PLANTS
SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2004

IAEA Library Cataloguing in Publication Data

Design of emergency power systems for nuclear power plants : safety guide

— Vienna : International Atomic Energy Agency, 2004.

p. ; 24 cm. — (Safety standards series, ISSN 1020-525X ; no. NS-G-1.8)

STI/PUB/1188

ISBN 92-0-103504-7

Includes bibliographical references.

1. Nuclear power plants — Design and construction. 2. Nuclear power plants — Risk assessment. 3. Nuclear engineering — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL

04-00377

FOREWORD

**by Mohamed ElBaradei
Director General**

One of the statutory functions of the IAEA is to establish or adopt standards of safety for the protection of health, life and property in the development and application of nuclear energy for peaceful purposes, and to provide for the application of these standards to its own operations as well as to assisted operations and, at the request of the parties, to operations under any bilateral or multilateral arrangement, or, at the request of a State, to any of that State's activities in the field of nuclear energy.

The following bodies oversee the development of safety standards: the Commission on Safety Standards (CSS); the Nuclear Safety Standards Committee (NUSSC); the Radiation Safety Standards Committee (RASSC); the Transport Safety Standards Committee (TRANSSC); and the Waste Safety Standards Committee (WASSC). Member States are widely represented on these committees.

In order to ensure the broadest international consensus, safety standards are also submitted to all Member States for comment before approval by the IAEA Board of Governors (for Safety Fundamentals and Safety Requirements) or, on behalf of the Director General, by the Publications Committee (for Safety Guides).

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA. Any State wishing to enter into an agreement with the IAEA for its assistance in connection with the siting, design, construction, commissioning, operation or decommissioning of a nuclear facility or any other activities will be required to follow those parts of the safety standards that pertain to the activities to be covered by the agreement. However, it should be recalled that the final decisions and legal responsibilities in any licensing procedures rest with the States.

Although the safety standards establish an essential basis for safety, the incorporation of more detailed requirements, in accordance with national practice, may also be necessary. Moreover, there will generally be special aspects that need to be assessed on a case by case basis.

The physical protection of fissile and radioactive materials and of nuclear power plants as a whole is mentioned where appropriate but is not treated in

detail; obligations of States in this respect should be addressed on the basis of the relevant instruments and publications developed under the auspices of the IAEA. Non-radiological aspects of industrial safety and environmental protection are also not explicitly considered; it is recognized that States should fulfil their international undertakings and obligations in relation to these.

The requirements and recommendations set forth in the IAEA safety standards might not be fully satisfied by some facilities built to earlier standards. Decisions on the way in which the safety standards are applied to such facilities will be taken by individual States.

The attention of States is drawn to the fact that the safety standards of the IAEA, while not legally binding, are developed with the aim of ensuring that the peaceful uses of nuclear energy and of radioactive materials are undertaken in a manner that enables States to meet their obligations under generally accepted principles of international law and rules such as those relating to environmental protection. According to one such general principle, the territory of a State must not be used in such a way as to cause damage in another State. States thus have an obligation of diligence and standard of care.

Civil nuclear activities conducted within the jurisdiction of States are, as any other activities, subject to obligations to which States may subscribe under international conventions, in addition to generally accepted principles of international law. States are expected to adopt within their national legal systems such legislation (including regulations) and other standards and measures as may be necessary to fulfil all of their international obligations effectively.

EDITORIAL NOTE

An appendix, when included, is considered to form an integral part of the standard and to have the same status as the main text. Annexes, footnotes and bibliographies, if included, are used to provide additional information or practical examples that might be helpful to the user.

The safety standards use the form 'shall' in making statements about requirements, responsibilities and obligations. Use of the form 'should' denotes recommendations of a desired option.

The English version of the text is the authoritative version.

CONTENTS

| | | |
|----|--|----|
| 1. | INTRODUCTION | 1 |
| | Background (1.1–1.5)..... | 1 |
| | Objective (1.6) | 2 |
| | Scope (1.7–1.9) | 2 |
| | Structure (1.10–1.11) | 3 |
| 2. | GENERAL DESIGN BASIS FOR EPSs | 3 |
| | General (2.1–2.5) | 3 |
| | Reliability, form and arrangement (2.6–2.8)..... | 5 |
| | Single failure criterion and equipment outages (2.9–2.10) | 6 |
| | Common cause failures (2.11) | 6 |
| | Combinations of events (2.12–2.13)..... | 7 |
| | Station blackout (2.14–2.17) | 7 |
| 3. | GENERAL RECOMMENDATIONS ON DESIGN | 8 |
| | Redundancy (3.1)..... | 8 |
| | Independence (3.2–3.6) | 8 |
| | Diversity (3.7)..... | 9 |
| | Controls and monitoring (3.8–3.12)..... | 9 |
| | Identification (3.13) | 10 |
| | Capacity and capability (3.14) | 11 |
| | Sharing of components in multiunit plants (3.15) | 11 |
| | Operating limits (3.16)..... | 11 |
| | Control of access to the EPSs (3.17) | 12 |
| 4. | RECOMMENDATIONS ON THE DESIGN OF SYSTEMS AND FEATURES (4.1–4.3) | 12 |
| | Design and features of the electrical parts of the EPSs (4.4–4.68)... | 13 |
| | Design and features of the non-electrical equipment in the EPSs (4.69–4.92) | 34 |
| 5. | DESIGN PROVISIONS FOR THE INSPECTION, TESTING AND MAINTENANCE OF THE EPSs (5.1–5.8) | 39 |

| | | |
|----|---|----|
| 6. | CONFIRMATION OF THE DESIGN | 42 |
| | Quality assurance (6.1–6.2)..... | 42 |
| | Qualification (6.3–6.9)..... | 42 |
| | Verification of design (6.10–6.11) | 44 |
| | Documentation (6.12) | 44 |
| | APPENDIX: GUIDANCE ON ON-SITE AND OFF-SITE POWER .. | 46 |
| | REFERENCES | 51 |
| | GLOSSARY | 53 |
| | CONTRIBUTORS TO DRAFTING AND REVIEW | 57 |
| | BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS.. | 59 |

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide was prepared under the IAEA programme for establishing safety standards for nuclear power plants. The basic requirements for the design of safety systems for nuclear power plants are provided in the Safety Requirements publication, Safety Standards Series No. NS-R-1, Safety of Nuclear Power Plants: Design [1], which it supplements. This Safety Guide describes how the requirements should be met in the design of emergency power systems (EPSs) for nuclear power plants.

1.2. This publication is a revision of a previous Safety Guide issued in 1991 as Safety Series No. 50-SG-D7 (Rev. 1), Emergency Power Systems at Nuclear Power Plants, and supersedes it. The revision takes account of developments in the design of EPSs in nuclear power plants since the earlier Safety Guide was published in 1991 and includes recommendations and guidance on non-electrical power sources.

1.3. Many systems in nuclear power plants require power in order to perform their safety functions, both in operational states and during or after accident conditions. This power may be derived from electricity, compressed gas, steam, direct drives (e.g. diesel engines that directly drive pumps) or other sources. Depending on the design of the systems, such power supplies may be used separately or in combination.

1.4. EPSs that supply electrical and non-electrical power to systems important to safety are of fundamental importance to the safety of nuclear power plants. The purpose of the EPSs is to provide the plant with the necessary power in all relevant conditions within the design basis so that the plant can be maintained in a safe state after postulated initiating events, in particular during the loss of off-site (grid) power. The EPSs may also be effective for certain severe accident conditions.

1.5. EPSs are integral parts of the safety systems and serve as support features for safety systems for the purpose of supplying and distributing power to those systems and to other designated items important to safety.

To perform the safety functions that are required for different postulated initiating events, safety systems are provided in various forms and arrangements and with various combinations of redundancy and diversity. A lack of adequate power supplies, with systems consequently unable to perform their necessary safety functions, might lead to radioactive releases that exceed authorized limits.

OBJECTIVE

1.6. The objective of this Safety Guide is to elaborate on the requirements for ensuring the reliability of the EPSs as established in paras 6.88–6.89 of Ref. [1]. It is intended for the use of those involved in the design, operation, assessment and licensing of EPSs, including designers, safety assessors, regulators and operators. The Safety Guide makes recommendations and gives guidance on the provisions necessary for both new and operating nuclear power plants to meet the requirements relating to the functions of EPSs.

SCOPE

1.7. This Safety Guide applies to nuclear power plants for which the total power supply comprises a normal power supply (the power supplied either from the transmission network of the electrical grid or from the plant generator) and an emergency power supply (which may be electrical or a combination of electrical and non-electrical).

1.8. The Safety Guide provides general recommendations and guidance for all types of EPS — electrical and non-electrical — and specific guidance on the safety requirements for design and the features of the electrical and non-electrical parts of the emergency power supplies. The recommendations and guidance are focused on the power supplies necessary to power loads important to safety.

1.9. This Safety Guide also provides guidance on power supplies to loads not important to safety that may be powered by EPSs.

STRUCTURE

1.10. Section 2 deals with the general design basis for the plant and also deals with the loss of all alternating current (AC) power supplies (station blackout)¹ as a combination of events that could lead to severe core damage. Section 3 provides general recommendations on design; detailed recommendations on design are made in Section 4. Recommendations specific to the electrical parts of the EPSs are given in paras 4.4–4.68 and those specific to the non-electrical parts (which are essentially the non-electrical power sources) are dealt with in paras 4.69–4.92. Section 5 specifies the design provisions for inspection, testing and maintenance. Section 6 deals with quality assurance, qualification, design verification and documentation.

1.11. The Appendix provides general guidance and discusses considerations relating to the electrical grid², configurations, transmission lines, on-site electric and non-electric power supplies and alternative power sources used to provide the power supply to the EPSs with a high level of reliability.

2. GENERAL DESIGN BASIS FOR EPSs

GENERAL

2.1. It is required that the EPSs be able to supply the necessary power in any operational state or in the case of a design basis accident, and that it be possible to test their functional capability (Ref. [1], paras 6.88, 6.89). The EPSs should be designed to Class 1E requirements³ and in the following circumstances should be seismically qualified to ensure:

¹ A station blackout is the complete loss of AC power supplies from off-site, the plant power generator and the EPSs. It does not include the failure of uninterruptible AC power supplies or the failure of alternative AC power sources.

² The terms ‘electrical grid’ and ‘grid’ are used for that part of the electrical power system providing off-site power to the nuclear power plant. The transmission line is the power line connecting the plant concerned to the grid.

³ Class 1E requirements: the safety classification for the electrical equipment and systems that are essential for emergency shutdown of the reactor, containment isolation, reactor core cooling and the removal of containment heat and reactor heat, or that are otherwise essential to preventing a significant release of radioactive material to the environment.

- (a) *For anticipated operational occurrences*: Provision of power to those systems whose functioning is necessary to keep radioactive releases within authorized limits. Anticipated operational occurrences include those occurrences that primarily and directly affect the plant's electrical power systems, such as the loss of off-site power or the loss of power generation at the plant.
- (b) *For design basis accidents and certain severe accidents*: Provision of power to those systems necessary to keep radioactive releases within authorized limits over the total accident recovery period, with account taken of the consequential effects of the loss of power generation at the plant and/or the loss of off-site power over this period.

2.2. To fulfil these functions the EPSs should supply power to all safety systems and to other designated plant items important to safety as indicated in Ref. [2].

2.3. In addition, items not important to safety (production loads) may derive their power from the EPSs, provided that the reliability of the EPSs is not adversely affected and the quality of the power supply is not degraded.

2.4. A set of design bases should be specified and used to design the EPSs. They should specify the required functional tasks, the necessary characteristics, the performance objectives, the operating and environmental conditions, and the necessary reliability. Reference should be made to the following paragraphs of Ref. [1]: paras 5.4–5.8 on the general design basis; paras 5.18 and 5.19 on site related characteristics; and paras 5.21–5.23 on design rules and design limits. Since the EPSs are safety system support features, the recommendations of the section on design bases in Ref. [2] will generally apply.

2.5. The design basis is required to specify the necessary capabilities of the plant to cope with a specified range of operational states and design basis accidents within the defined radiological protection requirements (Ref. [1], para. 5.4). The general design basis for EPSs should cover:

- (a) Capacity requirements for EPSs and their capability to perform their safety functions over the required time period;
- (b) Variables that should be monitored for initiating required actions by the EPSs;
- (c) Environmental conditions to which the EPSs will be subjected;
- (d) Necessary protection against conditions that could cause degradation of the EPSs;

- (e) Variables that should be monitored to verify the stability of the EPSs;
- (f) Identification of all loads powered by the EPSs, with distinctions made between those important to safety and those not important to safety, and with identification of their non-electrical and electrical characteristics and requirements;
- (g) Specified time period over which the EPSs are required to supply power to the loads so that they can meet their functional requirements;
- (h) Required performance characteristics of all components of EPSs;
- (i) Operating conditions for the power supplies of the EPSs, including the conditions under which it is permissible to connect, disconnect and shut down the power supplies;
- (j) Requirements for maintaining and testing the various components of the EPSs to ensure compliance with the operational limits and conditions;
- (k) Consideration of human factors;
- (l) Availability goals;
- (m) Reliability goals.

RELIABILITY, FORM AND ARRANGEMENT

2.6. The design management of a nuclear power plant is required to ensure that the structures, systems and components important to safety have the appropriate characteristics, specifications and material composition to enable the safety functions to be performed and the plant to operate safely and with the necessary reliability for the full duration of its design life (Ref. [1], para. 3.2). The EPSs should be designed for high functional reliability and testability and to have the capability to carry out their safety functions. Their design requirements, form and layout should be consistent with all the requirements for the safety systems to be supplied with power.

2.7. Paragraphs 5.48–5.56 of Ref. [1], which deal with design for optimized operator performance, apply. Further recommendations and guidance are provided in Ref. [2]. In order to implement advanced human factor concepts in the design of EPSs, international standards (such as this Safety Guide) and national standards should be followed (Ref. [1], paras 3.6, 5.21).

2.8. In determining the necessary redundancy to be incorporated into the EPSs, account should be taken of the design considerations set out in the Appendix and the frequency of the postulated initiating events for which the EPSs have to perform their function. In some States, this necessary redundancy is determined by means of a probabilistic approach. As a minimum, the EPSs

are required to be designed to satisfy the single failure criterion (see paras 2.9–2.10).

SINGLE FAILURE CRITERION AND EQUIPMENT OUTAGES

2.9. Paragraphs 5.34–5.39 and 6.88–6.89 of Ref. [1] establish the requirements for applying the single failure criterion to EPSs. Paragraph 5.42 of Ref. [1] establishes the relationship between design and operation in the event of equipment outages such as those due to testing, repair and maintenance.⁴

2.10. In the application of the single failure criterion to EPSs, only one failure is assumed to occur at any one time. This means, for example, that when one part of the EPSs is electrical and another is steam driven, only one failure and its consequential failures need be assumed to occur within the entire (electrical and steam) EPSs at any one time.⁵

COMMON CAUSE FAILURES

2.11. The possibility of common cause failures, which could render the EPSs unavailable to perform their safety functions when called upon, should be considered in the design, maintenance, testing and operation of the EPSs. 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 or from human involvement (e.g. in operations and maintenance). 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 may affect the principles of diversity and independence should also be considered (e.g. poor fuel oil quality (see para. 4.92)). Paragraphs II.8–II.10 of Ref. [1] explain the use of diversity in this context.

⁴ In this application of the single failure criterion for the EPSs, the coincidence of maintenance work on a division of the EPS equipment and the occurrence of a single failure when a PIE calls for operation of the EPS is assumed in some States.

⁵ Further recommendations and guidance on the application of the single failure criterion and the treatment of common cause failures are provided in Ref. [3].

COMBINATIONS OF EVENTS

2.12. Paragraphs 5.20, 5.31 and I.14–I.18 of Ref. [1] establish the basis and the requirements for considering severe accidents and combinations of events in the design of nuclear power plants.

2.13. If the likelihood of occurrence of combined events or multiple failures is required to be considered in the general design basis, proper protection against these should be provided. In the case of EPSs, the likelihood of common cause failures following the loss of off-site power should be considered. Conservative deterministic assumptions or probabilistic safety assessment could indicate the need to include an independent power source (an alternate AC source) within the EPSs to cope with this possible event. The possibility of core degradation which could result for some plant designs from the total loss of AC power (station blackout) is one example for which such a likelihood should be considered. Such an independent power source could be dedicated to the critical safety function alone.

STATION BLACKOUT

2.14. With regard to the considerations applicable to severe accidents, as discussed in para. 5.31 of Ref. [1], analysis may reveal that a station blackout could lead to severe core damage, depending on the design of the plant and the time period considered. Even allowing for high levels of reliability in off-site power and in the designs of EPSs, the possibility of a station blackout should be taken into account as a conservative design assumption.

2.15. The behaviour of the plant under this assumption should be analysed to determine the expected length of time after the station blackout until critical cooling conditions of the core would be reached.

2.16. Several design measures are possible as a means of increasing the capability of the EPSs to cope with a station blackout, if measures are warranted by its likelihood. These measures include, for example, increasing the capacity of batteries to supply power to safety instrumentation and control equipment, and to other vital equipment, or installing an alternative AC source. For multiunit plants, this alternative AC source may be shared (see para. 3.15 on the sharing of components in multiunit plants).

2.17. Procedures to cope with a station blackout and to restore normal conditions should be developed.

3. GENERAL RECOMMENDATIONS ON DESIGN

REDUNDANCY

3.1. The EPSs should be divided into independent redundant divisions (see Ref. [1], Appendix II). The redundancy should be consistent with that of the safety systems served. Each division should have the reliability necessary to permit the systems it serves to fulfil their safety functions. In setting the level of redundancy, account should also be taken of any increase in the unavailability of the EPSs resulting from equipment being taken out of service for the purposes of maintenance and testing.

INDEPENDENCE

3.2. Following the principle of independence, the divisions of EPSs should be protected by physical separation and should be functionally isolated (electrically or otherwise) from one another (see Ref. [1], Appendix II). The physical separation of circuits and equipment should be achieved by the use of structures, spacing and barriers or combinations thereof, depending on the need to protect against all the postulated initiating events considered in the design basis (e.g. fires, chemical explosions, aircraft crashes or missile impacts). The functional isolation of divisions should be achieved by preventing a failure in one of the divisions from leading to the unavailability of, or generating faults in, another division. Additional recommendations and guidance on this subject are given in Ref. [3].

3.3. Equipment and circuits that are required to be independent should be determined and delineated in the early phase of the plant design and should be marked distinctly in documents and drawings to aid their identification (see Ref. [1], Appendix II).

3.4. The functional failure of the support features of safety systems should not compromise the independence of the circuits or the equipment of the safety

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

3.5. Systems other than safety systems that are supplied from the EPSs should either be automatically disconnected on an accident signal or be connected to the EPSs with safety grade equipment, and should not be able to reduce the functional independence or reliability of the EPSs below the level required for the EPSs to perform their safety functions.

3.6. One way of realizing independence is to use dedicated power supplies for the individual components of safety systems if they are also designed with regard to proper physical separation or protection.

DIVERSITY

3.7. Paragraphs II.8–II.10 of Ref. [1] explain the use of diversity. If a diverse non-electrical system is used as a diverse approach to supply emergency power it will to some extent also require an electrical power supply. This can either be achieved by the use of dedicated power sources or be supplied by means of non-interruptible power sources.

CONTROLS AND MONITORING

3.8. Sufficient instrumentation and control equipment is required to be provided to monitor and control the EPSs from the control room (Ref. [1], paras 6.68–6.75). This equipment should be determined on the basis of its capacity to function under operational states, design basis accident conditions and certain severe accidents. Systematic consideration of human factors and the human–machine interface is required to be included in the design process to ensure an appropriate and clear distinction of functions between operating personnel and the automatic systems provided (Ref. [1], para. 5.50). The instrumentation and control equipment should incorporate advanced features to take account of human factors in the design in order to reduce the likelihood of operator errors.

3.9. The instrumentation and control equipment required to enable the EPSs to perform their safety functions is considered part of the EPSs and is classified

as safety equipment. Recommendations and guidance on this equipment are provided in Ref. [2].

3.10. Paragraph 6.75 of Ref. [1] requires that “Sufficient instrumentation and control equipment shall be available, preferably at a single location (supplementary control room) that is physically and electrically separate from the control room, so that the reactor can be placed and maintained in a shut down state, residual heat can be removed, and the essential plant variables can be monitored should there be a loss of ability to perform these essential safety functions in the control room.” For this purpose, an analysis should be made to determine which functions of the EPSs should be monitored and actuated from the supplementary control room to ensure that the necessary safety functions that have been specified can continue to be performed. The applicable recommendations of Ref. [2] should be met.

3.11. Information on the operational status of the EPSs and on their controls that is sufficient for monitoring the status of the EPSs should be provided in the plant control room and the supplementary control room. The alarm and annunciator systems relating to the EPSs should be designed for efficient and error free detection, diagnosis and action by operators.

3.12. The components and variables to be monitored and the methods and equipment selected for obtaining and providing the information on the operational status of the EPSs will depend on the plant concerned and on the design of its EPSs and should be specified accordingly.

IDENTIFICATION

3.13. The safety systems’ equipment and its interconnections should be suitably identified (e.g. by tagging or colour coding) to differentiate these safety systems from other plant systems. In addition, within a safety system, redundant divisions should be suitably identified to reduce the likelihood of inadvertent maintenance, testing, repair or calibration being performed on an incorrect division. Such identification should not require reference to drawings, manuals or other reference material. Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant part of the safety system do not themselves require identification.

CAPACITY AND CAPABILITY

3.14. The EPSs should have sufficient capacity and capability to fulfil their safety functions successfully in the event of a single failure. The capacity and capability should be determined by analysis and verified by tests. The effects of all continuous, random loads (e.g. loads actuated by temperature or pressure), and switched and transient loading demands, including the load sequencing and the period of time for which each load must be supplied, should be taken into consideration in the tests. Loads that are not important to safety and that are not automatically disconnected when the EPSs are required to supply power to cope with postulated initiating events should be assumed to be connected and should be included in the calculation of total loads.

SHARING OF COMPONENTS IN MULTIUNIT PLANTS

3.15. Each unit in a multiunit power plant should have separate and independent EPSs. In exceptional cases, parts of the EPSs may be shared. In these rare cases, it should be demonstrated that the safety requirements of each unit individually, and of all the units collectively, are met. Account should be taken of potential common cause failures and of the possibility that one or more units are shut down while maintenance is performed on the common parts of the EPSs. As a minimum, the combined capability of the shared parts together with those parts dedicated to each of the units should be sufficient to accommodate both the most demanding postulated initiating event that could credibly affect one or more units and the orderly shutdown of, and removal of heat from, the unaffected units.

OPERATING LIMITS

3.16. The parameters of the EPSs, 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. Recommendations and guidance on the operational limits and conditions for nuclear power plants are given in Ref. [4].

CONTROL OF ACCESS TO THE EPSs

3.17. Unauthorized access to, or interference for any reason with, structures, systems and components important to safety is required to be prevented (Ref. [1], para. 5.65). Access to EPS equipment and support systems should be limited, with consideration given to the need to prevent unauthorized access, the possibility of error by authorized personnel and the possible need for immediate access in the event of an emergency. The methods employed should include combinations of physical protection (e.g. locked enclosures, rooms, alarms and telephones) and administrative measures according to the degree of supervision and the remoteness of the equipment.

4. RECOMMENDATIONS ON THE DESIGN OF SYSTEMS AND FEATURES

4.1. This section provides recommendations for the design and the necessary features of the EPSs and develops the recommendations of previous sections. To fulfil the required safety functions, the EPSs may supply power as compressed gas, water, steam or electricity or in other forms, depending on the design of the system to be served.

4.2. In addition to providing recommendations for the design of EPSs, this section also provides guidance on certain other plant components that have an interface with the EPSs. In particular, guidance is given on loads not important to safety and on controls whose failure could affect the proper functioning of the EPSs.

4.3. Included in the electrical parts of the EPSs are the components and systems necessary for generating and converting electrical power and distributing it to those safety systems requiring it. Certain other electrical loads may also be supplied provided that the relevant rules set out in paras 4.44–4.45 are complied with. The following paragraphs deal with recommendations for design of the electrical parts of the EPSs. The non-electrical equipment in the EPSs is dealt with in paras 4.69–4.92.

DESIGN AND FEATURES OF THE ELECTRICAL PARTS OF THE EPSs

4.4. The EPSs can be powered from the normal power supply or (optionally) from the alternative on-site power supplies (see Fig. 1). The boundaries of the EPSs are (a) at the input terminals of the circuit breakers used to connect the EPSs to the normal and the alternative power supplies, (b) at the input terminals for the safety system loads, and (c) at the load side of the isolation devices of those loads other than safety system loads that derive their electrical power from the EPSs. Items other than safety system items (including those important to safety and those not important to safety) may also be included. Guidance on on-site and off-site power supplies is provided in the Appendix.

4.5. The electrical parts of the EPSs are generally divided into three types of electrical system according to the different power requirements of the loads as follows:

- (1) An AC power system the assigned AC loads of which allow a certain interruption of the power supply. Usually the AC power system of the EPSs is fed by a power system for which limited credit is given in the safety analysis. The loss of this power supply triggers the startup of a standby electrical power system which is loaded within a prescribed time sequence.
- (2) A direct current (DC) power system that supplies DC loads without interruption from a battery. This DC system includes a battery charger that is connected to the AC system of the EPSs.
- (3) A non-interruptible⁶ AC power system that is supplied by the DC power system of the EPSs by means of inverters and is also connectable to the AC power system of the EPSs.

4.6. An example of a single division of the EPSs is shown in Fig. 1. Figure 2 shows an example of an arrangement for a power system that connects the normal and the alternative power supplies to the EPSs. Figures 3 and 4 show possible interfaces between the non-electrical and electrical parts of EPSs. Figure 5 shows an example of non-electrical EPSs.

⁶ A non-interruptible power supply may experience a perturbation in its output, such as a dip in voltage 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.

LEGEND OF SYMBOLS FOR THE FIGURES



Generator



Transformer



Isolation device with terminals (breaker)



Removable link



AC-DC transformer



DC-AC transformer



Battery



Safety system load with input terminal



Load other than a safety system load with input terminal



Motor



Pump



Boundary of the EPSs

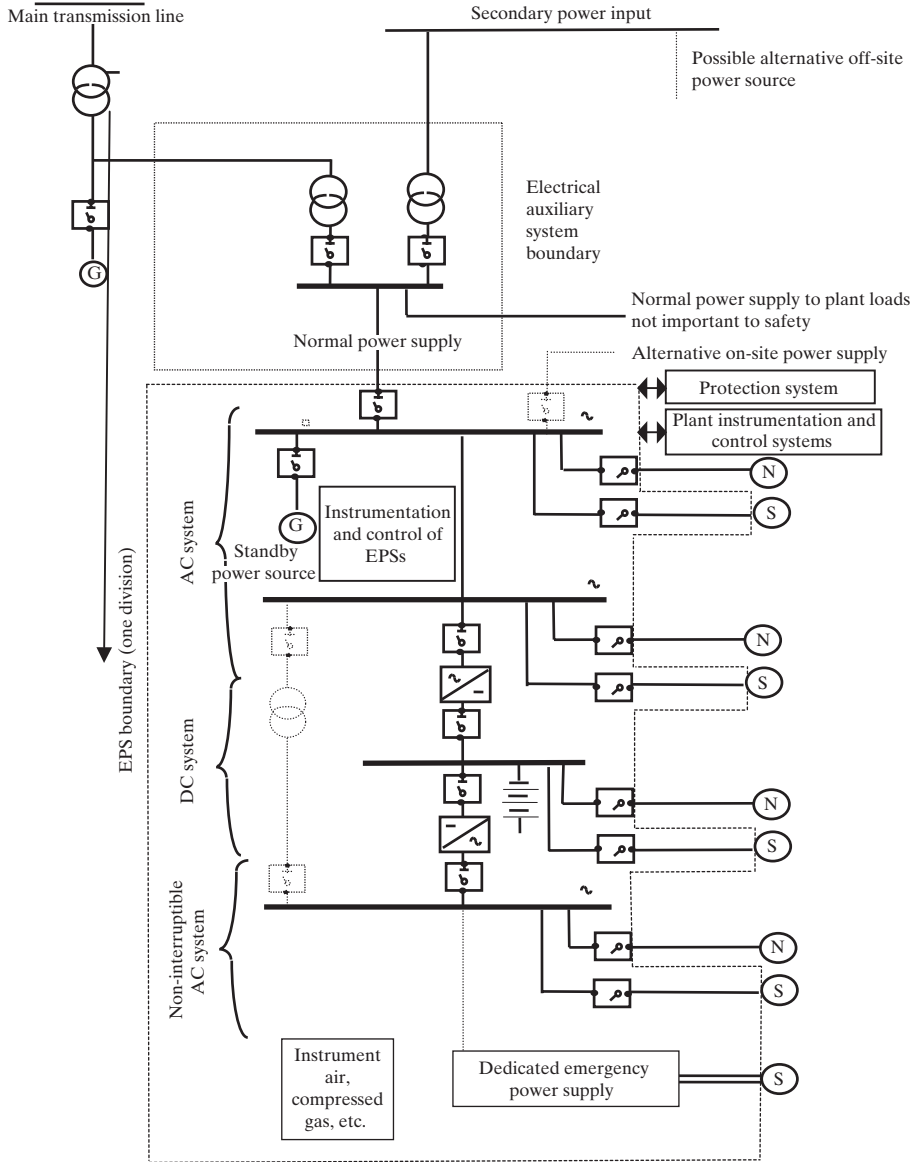


FIG. 1. Schematic representation of the different parts of the plant power supplies as discussed in this Safety Guide, with their boundaries.

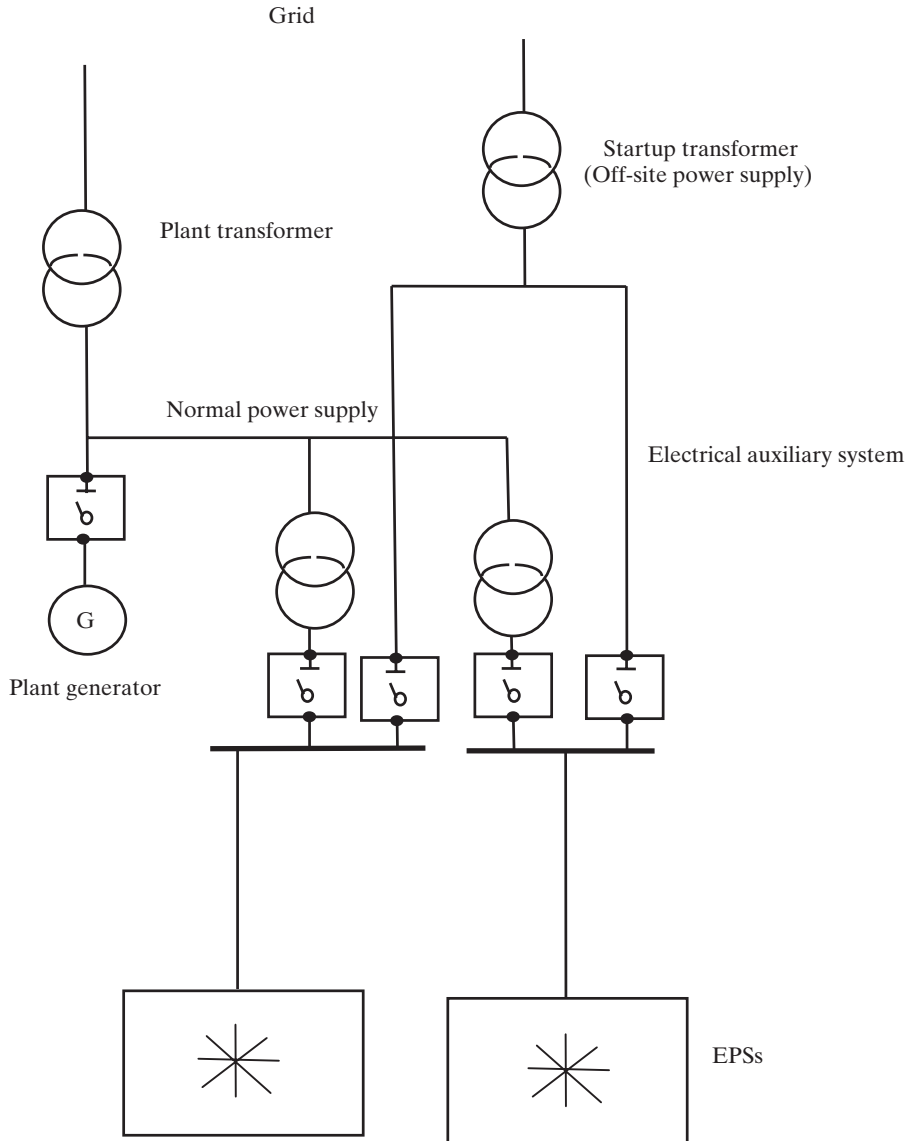


FIG. 2. Example of grid connections and arrangements of the EPSs with two 100% divisions of the EPSs.

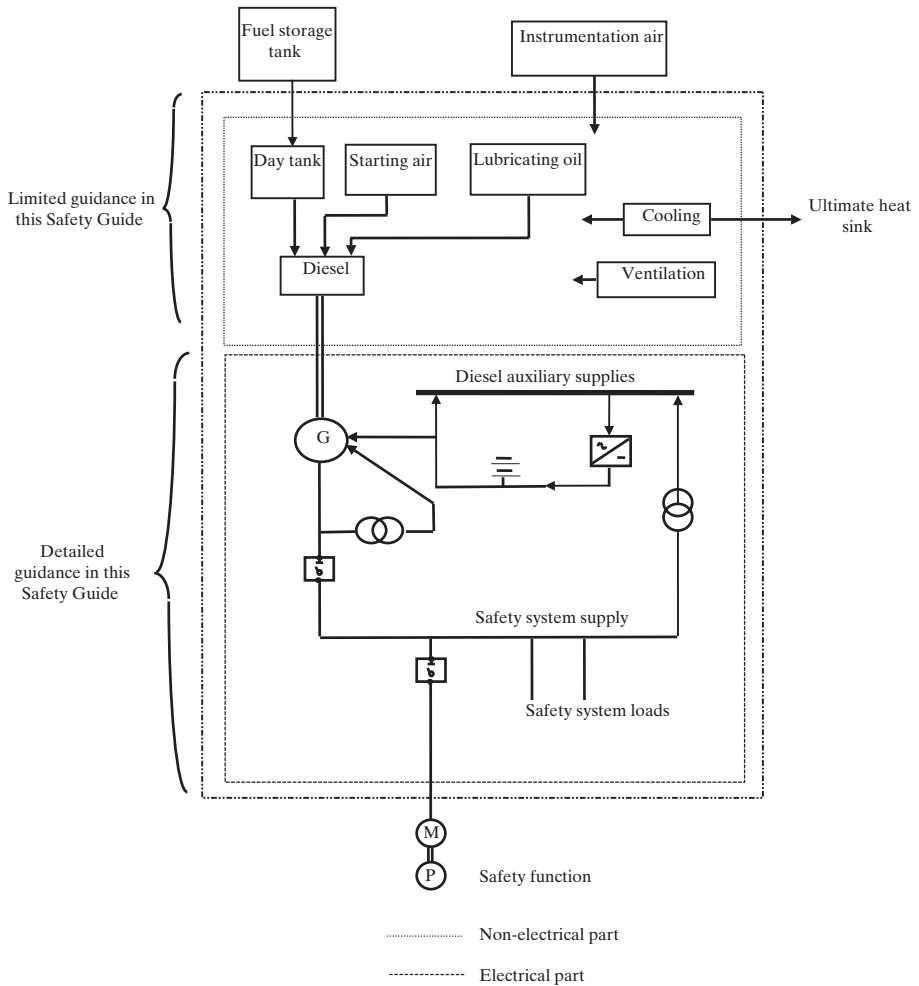


FIG. 3. Example of the boundaries of the EPSS for combined non-electrical and electrical equipment (functional schematic of the supply unit for the standby diesel generator).

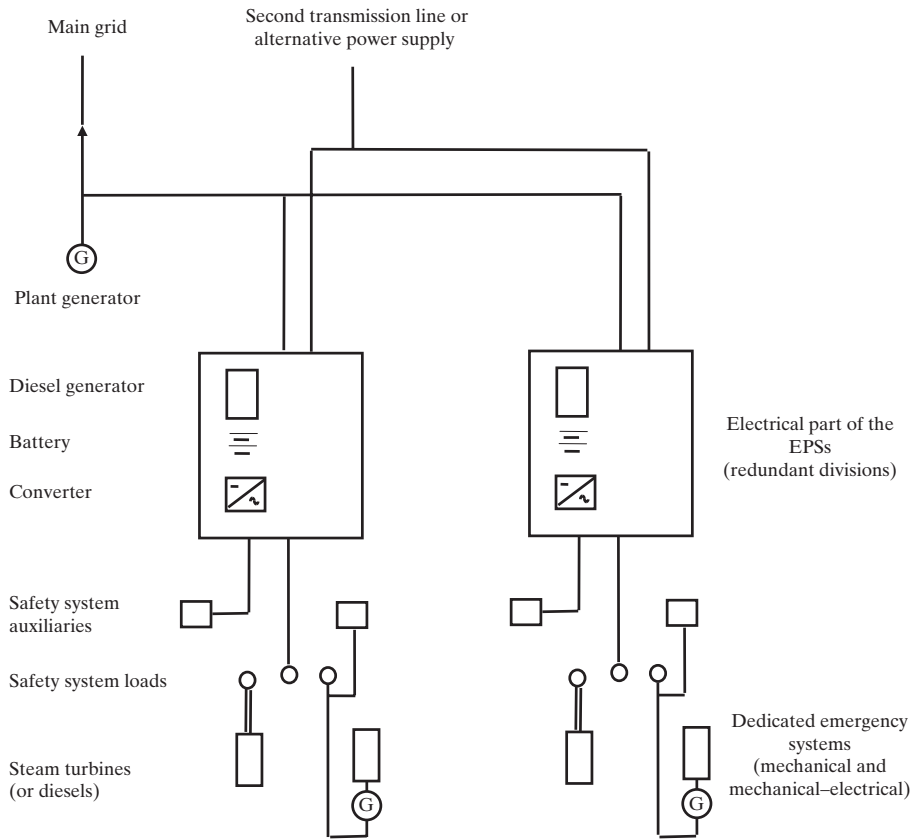


FIG. 4. Schematic example of the configuration of the EPSs (limited to two divisions; transformers, breakers, etc., are not shown).

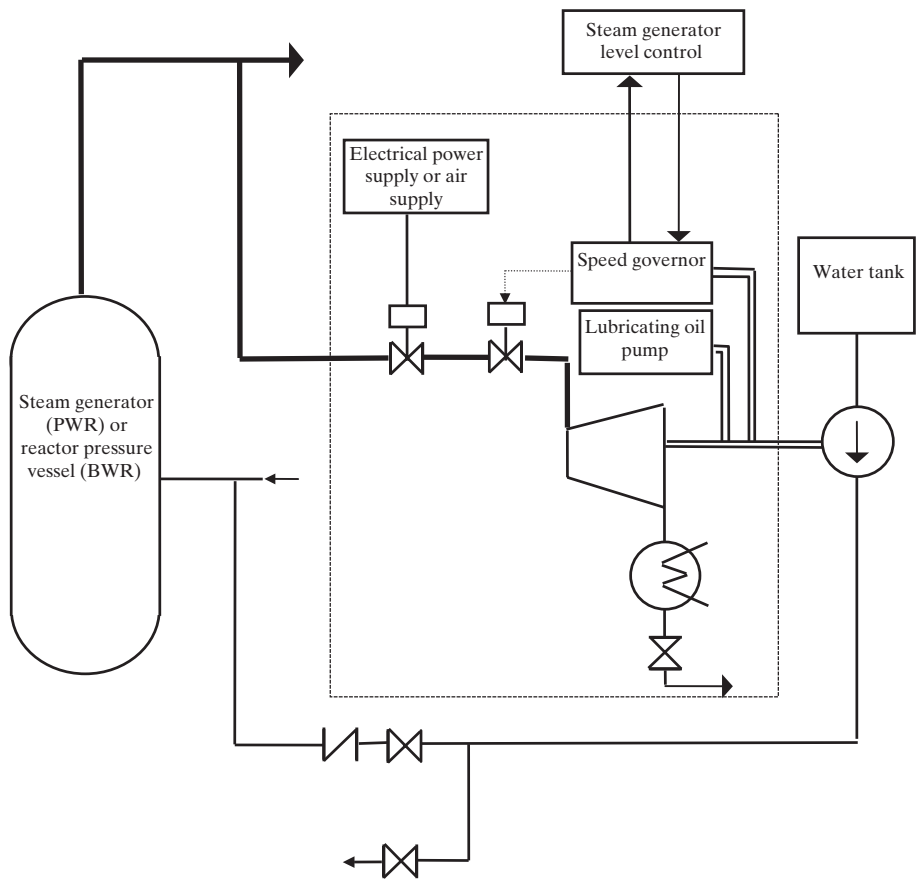


FIG. 5. Example of the boundary of the non-electrical EPSs (functional schematic of the steam driven pump for the emergency feedwater supply). (BWR: boiling water reactor; PWR: pressurized water reactor.)

AC power system of the EPSs

4.7. The AC power system should provide AC power for the connected loads in operational states, under design basis accident conditions and in the event of certain severe accidents. The AC power system should be divided into redundant divisions in accordance with paras 3.1 and 4.37. Each division should consist of a connection to a normal power supply, a connection to an alternative on-site power supply (if provided), a standby electrical power source and a distribution system and its branch circuits down to the terminals for (but not including) safety system loads.

4.8. The normal power supply should be the preferred method of providing AC power to the EPSs. Alternative power supplies may be used. The design basis of the EPSs should reflect the capability, capacity, reliability, availability and electrical characteristics of these power supplies.

4.9. The standby power sources should not be used to supply power to the EPSs on a continuous basis since long term utilization can reduce their reliability and increase the frequency of their maintenance and outage times in a manner that may not be compatible with their operability requirements.

4.10. Degradation of the normal power supply of each EPS bus (i.e. overvoltage, undervoltage, overfrequency or underfrequency) should be detected on the buses of the AC power system of the EPSs. The affected bus should be automatically disconnected from its power source if the degradation exceeds the levels specified in the design requirements. Subsequent to disconnection, this bus should be automatically connected directly to (a) the alternative power source, or (b) the standby power source for that division of the EPSs, and in that order of precedence.

4.11. When the standby power source is called on to supply power to an EPS bus, that bus should be automatically disconnected from the plant's electrical auxiliary system⁷. This is necessary to prevent power being supplied from the standby power source of the EPSs to the large number of other, large loads connected to the normal power distribution system. The use of the standby power source should be limited to the period of time necessary to recover the

⁷ An electrical auxiliary system is a system for distributing and connecting power from the plant generator, the transmission lines or other off-site power sources to electrical loads (those important to safety and those not important to safety).

normal or alternative power supplies and up to the time when the transfer can be achieved reliably.

4.12. When the alternative on-site power is called on to supply power to the bus of the EPSs, that bus should be manually or automatically disconnected from the electrical auxiliary system of the plant.

4.13. When the function of supplying power is transferred from standby power sources to either the normal or the alternative power supplies or from the alternative to the normal power supply, the transfer should be sequenced so that it involves only one division of the EPSs at a time. Transfer actions for the reinstatement of power from the normal power supply should be accomplished manually.

4.14. The protection system is required, unless its adequate reliability is ensured by some other means, to be designed to permit periodic testing of its functioning when the reactor is in operation, including the possibility of testing channels independently to determine failures and losses of redundancy that may have occurred (see Ref. [1], paras 6.81–6.83). The preferred approach to design specifies only one standby power source per division, thereby avoiding the necessity of using in parallel and synchronizing standby generators. Means should be provided for the periodic testing of standby power sources during plant operation. When testing a standby power source during plant operation, means should be provided to synchronize the standby generator to the normal power supply. The standby generator should be connected to the normal power supply for testing purposes only.

DC power system of the EPSs

4.15. The DC power system supplies power to instrumentation, control, monitoring, protection, switching and auxiliary power systems, in operational states, under design basis accident conditions and in certain severe accidents. The DC power system should be divided into redundant divisions in accordance with paras 3.1 and 4.37. Each division should consist of at least a battery, a battery charger and a distribution system.

Battery

4.16. The battery supplies DC power to the distribution system without interruption in the event of a loss of AC power to the battery charger. It consists of storage cells, interconnections and their connections to the distribution system.

4.17. The batteries should be maintained in a fully charged condition by the battery charger during normal operation.

Battery charger

4.18. For each division of the DC power system, the battery charger supplies the steady state DC power and maintains the battery in a fully charged condition. The battery charger itself is supplied from the AC power system of the EPSs as described in para. 4.7.

4.19. The battery chargers should have sufficient capacity to restore the battery from a discharged condition to a minimum charged state within an acceptable period of time while at the same time satisfying the highest combined demands of the various steady state loads following an initiating loss of normal power. If the battery charger is permitted to supply the system with the battery disconnected, the charger should have the capability to satisfy the highest combined demands, including transients. Each battery charger should have disconnecting devices in the AC and DC circuits to enable the charger to be isolated.

4.20. Ventilation should be provided in battery rooms to maintain the concentrations of combustible gases below prescribed levels. This ventilation system should be powered by the EPSs.

Battery capability

4.21. Each redundant battery set should be capable of meeting all required load demands and conditions (including duty cycles and electrical transients occurring in operational states and under design basis accident conditions) for a specified period of time (typically two to four hours), with account taken of such factors as design margins, temperature effects, any recent discharge and deterioration with age. In the event of a station blackout (see paras 2.14–2.17), this battery capability is highly important.

Non-interruptible AC power system of the EPSs

4.22. A non-interruptible AC power system should be provided to supply loads for equipment important to safety and requiring continuous AC power. The electrical characteristics and the continuity of the electrical power should meet the requirements of the loads to be served by the system. The non-interruptible AC system should be divided into redundant divisions. As a minimum, each division should consist of a supply from a DC power system, a DC–AC

converter and a distribution system. A power supply from the AC bus of the same division of the EPSs and having an automatic switchover device should also be provided. Either the DC–AC converter or the other AC power supply, depending on the availability and reliability of these supplies, may be selected to supply power.

4.23. Special consideration should be given to the characteristics and requirements of the loads and the interactions between loads connected to the non-interruptible AC system. For example, if a static inverter is used, the design should ensure that the voltage harmonics produced by the inverter itself, as well as by any non-sinusoidal loads, do not degrade the functions of the systems being supplied.

Standby electrical power source

4.24. The standby power source should consist of an electrical generating unit complete with all auxiliaries and its dedicated separate and independent stored energy supply (e.g. compressed air, stored fuel, oil or water).

4.25. The standby power source should have sufficient capacity and capability to start and supply all loads as specified in the design basis. These loads may include loads for safety systems and loads other than those for safety systems. Paragraphs 4.44–4.45 provide the rules for permitting loads other than safety system loads to be supplied from the EPSs and for including them when determining the capacity of the standby power source.

4.26. The design basis requirements of the standby power source should include:

- (a) The time to start and accept loading in a specified load sequence;
- (b) The performance characteristics, including the capability for no load, light load, rated load, starting load and overload operation for the required time periods;
- (c) The capability for step load operation over the entire load range;
- (d) Reliability.

4.27. The step load capability requires that the standby unit of the electrical power system should maintain the voltage and the frequency within limits for time and level that will not degrade the performance of any load below its minimum requirements, even during transients caused by the addition or removal of the largest load.

Individual power supplies

4.28. Certain equipment (e.g. remote radiation monitors, meteorological equipment and parts of communication systems) may be designed with its own individual power sources and may not, therefore, be connected to the EPSs.

4.29. Such power sources should be designed with a capability and reliability commensurate with the safety functions of the equipment they serve.

4.30. For applications in which the equipment does not operate continuously, the design should include a means of testing the availability of the power source.

Distribution systems

4.31. The recommendations in paras 4.32–4.37 apply to the distribution systems of the AC and DC power systems and that of the non-interruptible power system of the EPSs.

Capability

4.32. Each distribution system should have sufficient capacity and capability to supply the required loads under all required operating conditions of the EPSs and to withstand the maximum credible overcurrent under electrical fault conditions and transient conditions without damage to, or adverse effects on, any of its components. Each distribution system should be capable of switching the power supplies and loads as demanded by the control.

Support system equipment

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

Protective devices of the main and branch circuits

4.34. All main and branch circuits of the EPSs should be protected against overloads, ground faults and short circuits by the use of protective devices, which should be located in enclosures and structures designed to protect the EPSs from the effects of postulated initiating events. The protective devices

should be part of the safety system and should be qualified for service for protection against overloads and short circuits.

4.35. The protective devices against overloads and short circuits should be properly sized, calibrated and co-ordinated so that the EPSs perform as designed and protect the equipment, buses and cables of the main and branch circuits from damage in overload and fault conditions. The co-ordination of the protective devices should be such that only the faulty part of the EPSs is isolated and the remaining intact circuit is unaffected.

4.36. It may be necessary in some situations to operate the equipment of safety systems in overloaded conditions to ensure the fulfilment of certain safety actions. This need should be taken into account at the design stage. For example, the set points of circuit protective devices may be set higher than the levels necessary to protect the equipment from damage due to overloads. Where this is the case, the overloaded equipment should not be able to affect adversely either the other circuits or the associated equipment to such an extent that their functioning is impaired. The continued operation of safety system equipment under overloaded conditions with the consequent risk of its damage or destruction need not form part of the safety justification for design basis accidents, although it should be recognized that unforeseen circumstances may arise. 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. Verification action should be taken to prevent any overload conditions from remaining undetected.

Connection between redundant divisions

4.37. Automatic connection between redundant divisions of the EPSs should be prohibited. If provision is made for connections between redundant divisions, it should be shown that the requirements of the connected safety system loads are met with account taken of the potential for the propagation of failures from one division to another and the potential for overloading the power sources. The fact that such connections reduce the independence of the divisions and their connected safety system loads should also be taken into account.

Controls for the EPSs

4.38. Controls should be automatic. Manual control should only be accepted if it can be demonstrated that its performance is sufficiently reliable, with account taken of human factors. Recommendations regarding dependence on manual operator action are given in Ref. [2]. Requirements on design for optimal operator performance are established in paras 5.48–5.56 of Ref. [1]. Recommendations on the performance and reliability of these automatic controls are made in Ref. [2].

4.39. The functions of the controls should include the following:

- (a) Automatic disconnection of loads (as specified in the design basis) and all other power supplies from the bus of the EPSs when the standby power source or an alternative on-site power source is supplying power. Automatic selection between the alternative on-site power source and the standby power source according to the criteria of paras 4.7–4.14 should be included as part of the design for EPSs. Equipment for selecting alternative off-site power supplies providing power to EPSs via the normal power supply is not part of the EPSs.
- (b) Automatic start and connection of the standby power source and the loads to the EPSs' bus in the specified sequence. This should conform to the startup time requirements imposed on safety equipment to match the assumptions made in the safety analysis. The load sequencing programme should work correctly irrespective of the actual sequence of demand.
- (c) Synchronization of the EPSs back to the normal power supply when the latter is being reinstated.

4.40. Manual control should be provided to (a) permit switching the various available power supplies and loads onto the bus of the EPSs as required, and (b) facilitate testing, maintenance and repair.

4.41. Sufficient equipment for the complete control of each division of the EPSs should be provided, consistent with the role of the EPSs. This equipment should be physically separated from that used for controlling other divisions and should be contained within the appropriate structural enclosures of its division. In areas of convergence, such as the control room, adequate physical separation and electrical isolation devices should be provided between the instrumentation and control circuits of each division of the EPSs, to the extent that no postulated initiating event affecting the required instrumentation and control equipment could prevent the EPSs from performing their functions.

Isolation of instrumentation and control systems

4.42. Electrical isolation methods should be used as required in instrumentation and control circuits to maintain the independence of redundant circuits and equipment so that safety functions required during and following any postulated initiating event can be performed. These isolation devices should be part of the EPSs. Recommendations and guidance are provided in Ref. [2] for instrumentation and control circuits that are important to safety.

Monitoring

4.43. Adequate methods of monitoring and monitoring displays should be used (see Table 1).

TABLE 1. EXAMPLES OF MONITORING DISPLAYS

| Equipment | Parameter |
|----------------------------------|--|
| General | Voltage Frequency Current Power |
| Diesel generator | Winding temperature Lubricating oil pressure Water temperature Starting air pressure Fuel oil level Control voltage Breaker position |
| Diesel generator bus, switchgear | Voltage Current Frequency Breaker position Control voltage |
| Battery | Voltage Current Breaker position |
| Battery charger | Voltage Current Breaker position |

TABLE 1. EXAMPLES OF MONITORING DISPLAYS (cont.)

| Equipment | Parameter |
|--|---|
| Supply to typical large pump motor (over 200 kW) | Voltage Current Breaker position |
| Supply to typical medium size motor or to motor operated valve | Voltage Current Breaker position |
| Steam turbine driven pump | Speed Pressure Stop valve position |
| Turbogenerator for seal injector pump | Frequency Voltage Stop valve position Breaker position |
| Instrument air system | Pressure |

Note: The typical parameters listed are for illustrative purposes only; they are not necessarily provided in every instance, nor do they represent a minimum requirement.

Loads other than safety system loads

4.44. Loads other than safety system loads, including loads important to safety and loads not important to safety, may derive their electrical power from the EPSs. Systems not important to safety either should be automatically disconnected on an accident signal or should be connected to the EPSs by means of isolation devices. The isolation devices should meet the requirements for the safety system equipment.

4.45. The use of the EPSs for purposes not important to safety and the inclusion of the extra equipment necessary for such purposes should not reduce the functional independence or the system reliability of the EPSs or their capability to perform their safety functions, and it should not interfere with the ability to test the EPSs. As indicated in para. 3.14, all loads that are not automatically disconnected when the EPSs are required to supply power to cope with postulated initiating events should be assumed to be connected and should be included in the total load calculations.

Grounding

4.46. Grounding of the EPSs is important to safety because it is related, either directly or indirectly, to the reliability of the system. All plant grounding systems and provisions should be considered and analysed collectively since they may interact with one another. Detailed information is available in several national or international standards [5–14].

4.47. Grounding grids and ground connections on a site should be connected together electrically to keep the voltage differences between the elements of the EPSs below the required values.

4.48. 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 the EPSs or the lightning protection grounding. The plant grounding may be supplemented by specific ground connections.

4.49. Where non-grounded circuits are used in the EPSs, they should be provided with equipment for the detection of ground faults so that grounding faults may be detected and isolated.

4.50. Equipment grounding should be provided by connecting the metallic frames of all electrical equipment and apparatus to ground.

Buses and cables

Insulation

4.51. The buses and cables of the EPSs should be selected, rated and qualified for their service and for environmental conditions with account taken of the cumulative radiation effects and thermal ageing expected over their service life. The buses and cables should also be sufficiently fire retardant to prevent the propagation of fires. Special attention should be given to the qualification of cables that have to withstand conditions inside the containment during and after a loss of coolant accident, a main steam line break or other adverse environmental conditions.

Rating and sizing

4.52. The buses and cables should have a voltage rating equal to or greater than the voltage of the system of which they are a part and an impulse rating greater

than any credible transient voltage to which they may be subjected. The buses and cables should be sized to carry safely the currents of the main circuits and branch circuits required under voltage variations and to meet the demands of the loads without exceeding the allowable conductor temperatures over their service life. The main circuits and branch circuits should be sized on the basis of conditions of the full load current and short circuits (e.g. fault current and breaker interruption time) and should withstand temperatures for cable short circuits. In the calculation of conductor temperatures, the maximum environmental temperatures, the normal or fault currents, the load factors and the arrangements of other cables in the same or nearby raceways should be taken into account. In addition, consideration should be given to the influence of cable supports, wall penetrations, floor penetrations, fire stops and fire retardant coatings on the heating of cables and the resultant temperatures. Aspects of fire protection are considered in Ref. [15].

Installation

4.53. Buses, cable trays and their supports should be designed to withstand, with an appropriate margin, the mechanical loads, including SL-2 earthquake loads (see Ref. [16], para. 2.3), imposed by the cables and their associated fittings. The design of switchboard compartments and other critical equipment should be vermin proof where relevant. Cable raceways should be permanently identified with their respective divisions of the EPSs and each cable on installation should be given adequate identification to ensure its installation in the proper raceway; as a minimum, cables should be permanently identified at each end after installation.

Connectors, terminations and splices

4.54. Connectors, terminations and splices should be selected and qualified for their applications and for the in-service conditions anticipated over their service life (see paras 6.3–6.9). In general, the use of cable splices should be prohibited in high voltage systems, in raceways and inside the containment.

Separation by classes

4.55. At least three classes of cables should be identified for the purpose of physical separation: (1) control and instrumentation cables, (2) low voltage power cables (e.g. 1000 V or less), and (3) medium voltage power cables (e.g. 20 kV or less). The classes of a common division should be placed in separate raceways. Where, in exceptional cases, two or three classes are in the same

raceway, the cables 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. Cables for higher voltages are not usually used in the EPSs; if they are used, their separation from the other cables should also be considered. Low level analogue, digital and other instrumentation cables should be manufactured with sufficient twisting and shielding so as to minimize interference from electromagnetic and electrostatic noise.

Independence

4.56. The buses and cables of one division of the EPSs should be physically separated and electrically isolated from the buses and cables of other divisions of the EPSs to the extent necessary to ensure that a fault in one division does not propagate to others divisions.

4.57. Events of particular concern are fires, initiated either by external causes or by electrical faults in internal equipment, and electrical overcurrents causing electrical insulation to melt. Such propagation from one division to another can result from the close proximity of redundant divisions. Recommendations and guidance on prevention of the propagation of fires are provided in Ref. [15].

4.58. The requirements for preventing the propagation of the effects of overcurrents and short circuits should be met by the physical separation of cables of different divisions and by the installation of isolation devices on all cables that may potentially link divisions together. The adequacy of the physical separation should be justified by analysis or by testing in which account is taken of the potential hazards in the area.

Physical protection

4.59. To permit the EPSs to meet the single failure criterion, cables connected to them should be adequately protected against the hazards that may result from postulated initiating events. Hazards that could affect the EPSs include the effects of fire and the failure or malfunction of fluid systems and mechanical and structural components. The following should therefore be taken into account in the design of the EPSs:

- (a) *Mechanical systems.* The circuits of the electrical parts of the EPSs should be routed or protected so that failure of the associated mechanical equipment of one division of the EPSs cannot disable circuits or the equipment of another division that is essential to the performance of the

safety function. The possible effects of pipe whip, jet impingement, high levels of radiation, pressurization, elevated temperatures, humidity and the generation of missiles as a result of the failure of rotating equipment or other high energy systems should be considered. Recommendations and guidance on protection against the failure of mechanical equipment are provided in Ref. [17].

- (b) *Failure of structures and equipment.* The independence of redundant divisions of the EPSs should be maintained both during and following the failure of structures and equipment that were not designed to withstand credible postulated initiating events. The effects of the failure of structures and equipment on a single division of the EPSs need not be considered unless the division is required to mitigate the consequences of such a failure.

Electrical penetrations

4.60. All penetrations through the containment are required to meet the same design requirements as the containment structure itself (Ref. [1], para. 6.52). All electrical penetration assemblies in the containment structures and passages that are provided for the conductors should be considered safety system equipment; they should be rated and qualified for the service conditions and environmental conditions, including the cumulative effects of irradiation, that are expected over their service life.

4.61. Adequate consideration is required to be given to the capability of penetrations to remain functional in the event of a severe accident (Ref. [1], para. 6.54). The containment penetrations should have a continuous service voltage rating that is greater than or equal to the voltage of the systems of which the conductors are a part. They should also have an impulse rating that is greater than or equal to the maximum credible transient voltage. The penetration conductors should be of such a size as to be able to carry safely currents for which account is taken of voltage variations and short circuits over the period of time required for the protective device to clear a fault, as well as demands from loads in normal operation, anticipated operational occurrences and design basis accidents. Allowable temperatures of conductors should not be exceeded and pressure boundaries of the assemblies should not be degraded. The penetration conductors should be protected by means of redundant protective devices. The penetration assembly should be designed 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.

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

4.63. The penetrations and associated connectors, terminals, splices, materials and methods should be qualified in accordance with paras 6.3–6.9.

Lightning protection

4.64. Provision should be made so that a lightning strike will not prevent the EPSs from fulfilling their required safety function. The systems for achieving this may rely on external or internal protection.

4.65. The external provisions should take the form of 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. Both should be grounded so as to conduct the lightning current to ground outside the building.

4.66. The internal protection may be in the form of shielding and surge arresters to protect the EPSs against both the high induced 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. The internal protection grounding should be connected to the rest of the lightning grounding in such a way as to prevent high transferred potentials from injuring personnel or damaging equipment.

Surge voltage protection

4.67. Overvoltage surges can be caused by lightning strikes, electrical faults or switching phenomena. Voltage surge suppressors or arresters should be provided to prevent surges from exceeding the allowable voltage limits set for the equipment or its insulation.

Fire protection

4.68. Reference [15] provides recommendations and guidance on fire protection.

DESIGN AND FEATURES OF THE NON-ELECTRICAL EQUIPMENT IN THE EPSs

4.69. The non-electrical equipment in the EPSs includes equipment such as steam turbines, gas turbines, hydroturbines, diesel engines and compressed gas vessels for starting engines. If the equipment is not located on the plant site, it should be ensured that the management of the nuclear plant has full control and command as regards the priority use of the equipment.

4.70. The EPSs provide the motive force to drive pumps, compressors and generators and to operate valves, instruments and controls, depending on the design of the system to be served. Non-electrical equipment is that part of the EPSs that is provided for supplying mechanical power or energy other than electrical energy to standby units and to systems and components important to safety.

4.71. The electrical parts of the EPSs for which paras 4.4–4.68 provide recommendations on design considerations have a direct interface with non-electrical equipment in many instances. Those recommendations should be applied to electrical auxiliaries or to other electrical equipment directly connected to non-electrical equipment in the EPSs. The following paragraphs provide recommendations on design considerations for the non-electrical equipment only.

Boundaries of non-electrical equipment

4.72. The non-electrical equipment includes those components needed to provide the motive force to components that are used to generate electrical power, to pump water, to compress air, to position valves and to operate instruments and controls.

4.73. The boundaries of the non-electrical equipment on the input side include storage reservoirs of sufficient capacity as to be capable of providing the necessary 'fuel' (e.g. pressurized nitrogen or air, fuel oil) to the prime mover for the time period specified in the design requirements for the plant.⁸ On the load side, the boundary terminates at the component being served (see Figs 3 and 5).

⁸ In the case of steam taken from the steam generator at a pressurized water reactor, the boundary of the EPSs ends at the connection of the piping to the process system.

Connection of redundant divisions

4.74. Automatic connection between redundant divisions of the non-electrical equipment should be prohibited. If provisions are made for connections between redundant divisions, it should be shown that the requirements of the connected safety system loads are met with account taken of the potential for the propagation of failures from one division to another and the potential for overloading the power sources. The fact that such connections reduce the independence of the divisions and their connected safety system loads should also be taken into account.

Controls for the non-electrical equipment of the EPSs

4.75. Controls should be automatic. Manual control should be accepted only if it can be demonstrated that its performance is sufficiently reliable with human factors taken into account. The recommendations and considerations for dependence on manual operator action are the same as those for electrical systems set out in para. 4.38. Specifically, the functions of the controls for non-electrical equipment should include the following:

- (a) Automatic switching to a mode totally dedicated to emergency needs alone if non-electrical equipment is being utilized in another mode;
- (b) Automatic start of the standby unit;
- (c) Switching to the emergency mode according to (a) above, bypassing of those protection devices used to protect equipment for normal operational, testing and maintenance modes only.

4.76. Manual control should be provided to facilitate testing, maintenance and repair.

4.77. Sufficient equipment should be provided for the complete control of each division of the EPSs. This should be physically separated from equipment for controlling other divisions and should be contained within the structural enclosures of its division. In areas of convergence, adequate physical separation and isolation devices should be provided between the instrumentation and control equipment of each division of the EPSs to the extent that no postulated initiating event that affects the required instrumentation and control equipment should be able to prevent the EPSs from carrying out their function.

4.78. Recommendations and guidance on the design of instrumentation and control systems are provided in Ref. [2].

Monitoring

4.79. Adequate methods of monitoring should be used (see Table 1).

Loads other than safety system loads

4.80. Equipment of the EPSs should be dedicated to the emergency needs alone. In non-emergency conditions, EPSs may be used to supply normal operational loads and other loads as anticipated in the design basis.

4.81. The recommendations for non-electrical equipment that may also be used for loads other than safety system loads are analogous to those in paras 4.44–4.45.

4.82. All items within the boundaries of the EPSs, including the isolation devices, should meet the requirements for equipment for safety systems.

Fire and physical protection

4.83. Reference should be made to the recommendations made in paras 4.56–4.59 and to Ref. [15].

Instrument air

4.84. The design of the instrument air system should, with account taken of reliability considerations, supply the devices of safety systems by means of headers that are separate from those supplying non-safety-related systems. With such an arrangement, isolation devices should be installed so that in the event of an accident they can be closed to allow instrument air to be reserved for safety system devices only.

4.85. If components important to safety that are connected to the instrument air system are designed to go into a fail-safe position on the loss of air pressure, then maintaining pressure in the instrument air system may be considered a non-safety-related function. If, however, components important to safety require air pressure to go into a safe position, the instrument air system should be designated as a safety system. An instrument air system designated as a safety system should be designed with redundancy, independence and diversity

to ensure the necessary level of reliability. Where a single instrument air system is provided, the necessary reliability can be achieved by providing diverse pressure producing equipment for those components requiring pressure to reach the safe position. Examples of diverse pressure producing devices include compressed air or gas storage reservoirs or an independent compressed gas system that is connected to the component important to safety and separated by an isolation device from the instrument air system. The capability of systems that provide components important to safety with compressed gas should be sufficient to supply EPSs in operational states and under design basis accident conditions.

4.86. The systems supplying compressed air and gas to components important to safety should be free of contaminants such as oil, moisture and particulate matter. The dew point of the air in the system should be sufficiently low as to prevent water from condensing in any part of the system and thus potentially adversely affecting the functioning of the components.

4.87. The instrument air system should not be used to provide air for general plant services other than the instrument and control components for which it is designed. If compressed air is needed for other purposes, a separate and independent compressed air system should be provided as a backup. If an independent compressed air system is used as a backup to the instrument air system, isolation devices should be provided to prevent air from flowing into the backup system. In addition, devices should be provided to prevent contaminants from entering the instrument air system, which should be operated at a higher pressure than the backup system in order to minimize cross flow. Provisions should be made to monitor, inspect, test and maintain the instrument air system.

Standby non-electrical power system

4.88. The standby non-electrical power system should consist of a prime mover complete with all auxiliaries and its dedicated separate and independent stored energy supply (e.g. compressed air, stored fuel, oil and water supplies).

4.89. Diesel units are the most commonly used standby non-electrical power sources. Diesel units and other units such as steam turbines, hydroturbines and gas turbines are subject to the recommendations of this Safety Guide.

4.90. The standby non-electrical power system should have sufficient capability in anticipated operational occurrences and under design basis accident

conditions to start and to supply all loads as specified in the design basis. These loads may include loads in safety systems and loads other than those in safety systems. Paragraphs 4.44–4.45 make recommendations for permitting loads other than safety system loads to be supplied and for considering such other loads in determining the capacity of the standby power system.

4.91. Requirements for the design basis that should be met in establishing the capability of the standby power system include:

- (a) The period of time necessary to start and accept loading;
- (b) The performance characteristics, including the capability for no load, light load, rated load, starting load and overload operation for the required time periods.

The reliability of the standby power source should also be defined.

Storage of fuel and other depletable substances

4.92. Sufficient supplies of fuel and other depletable substances should be stored at the plant site to permit the simultaneous operation of all standby power sources at their required loads following the postulated initiating event that consumes the greatest amount of energy. The capacity for the on-site storage of fuel and other depletable substances should be based on an analysis of the time needed to replenish the amounts in storage from off the site. The minimum amounts kept in on-site storage will differ from one State to another and vary between two and seven days' supply. Some stored fuel will deteriorate with time (sometimes rather quickly). For this reason, a fuel evaluation programme, including monitoring, inspection and testing, should be established for the purpose of replacing the fuel if it is found to be necessary. Precautions should be taken to ensure that fuel storage facilities do not pose a fire hazard to the plant. Recommendations and guidance relating to fire protection are provided in Ref. [15]. Protection against other common cause failures should be given special consideration. In particular, the possibility of common cause failure due to there being a single fuel supplier should be considered.

5. DESIGN PROVISIONS FOR THE INSPECTION, TESTING AND MAINTENANCE OF THE EPSs

5.1. Provisions should be made in the design to include programmes to ensure that:

- (a) Each division of the EPSs performs as intended under the conditions specified in the design basis;
- (b) The equipment and the system conform to the design requirements;
- (c) Divisions of the EPSs are maintained in a state of readiness to respond to the demands on them over the lifetime of the plant;
- (d) Effective maintenance can be performed (preferably during normal operation) to keep unplanned outages to a minimum.

5.2. Provisions should be made in the design to ensure that the following test programmes can be implemented:

- (a) A pre-operational test programme to demonstrate the operational and emergency modes to the extent practicable, to be conducted following the installation of all components. This test programme should prove that the design requirements have been met. The test should also establish that each division is independent of other divisions.
- (b) A periodic test programme to demonstrate the continuing operability of the system and to detect and identify any degradation of the system or components within the system.
- (c) A test programme that provides adequate assurance of the readiness of the system to function upon demand and which identifies components with excessively high frequencies of maintenance.

Examples of periodic tests are given in Table 2.

TABLE 2. EXAMPLES OF PERIODIC TESTING AND MAINTENANCE AND THEIR INTERVALS

| Item of equipment | Test parameter/procedure | Test interval |
|-------------------|------------------------------|---------------|
| Switchgear: | | |
| Medium voltage | Functional test ^a | |
| | Mechanical inspection | 2 years |
| | Insulation test ^b | 1 year |

TABLE 2. EXAMPLES OF PERIODIC TESTING AND MAINTENANCE AND THEIR INTERVALS (cont.)

| Item of equipment | Test parameter/procedure | Test interval |
|---|--|---|
| Low voltage | Overhaul | When required |
| | Test of protective devices | 2 years |
| | Functional test ^a | |
| | Mechanical inspection | 2 years |
| Breakers as isolation devices | Overhaul | When required |
| | Test of protective devices | 2 years |
| Power transformers | Isolation function | 1 year |
| | Insulation test | 1–2 years |
| Batteries | Energize (normally de-energized) | 1 year |
| | Liquid level | 1 month |
| | Specific gravity and cell voltage | Pilot cell weekly; all cells monthly |
| Battery charger | Visual inspection | Weekly |
| | Performance discharge test | 5 years ^c |
| | Service test | 1–2 years ^d |
| | Visual inspection | Weekly |
| Standby generator | Calibration | As required |
| | Availability test | 1 month |
| AC/DC and DC/AC converters | Operability test | 1 month |
| Turbine steam driven pump | Availability test | 1 month |
| Turbogenerator for seal water injection | Starting and availability | 1 month |
| | Test on turbogenerator with limited load | 3 months |
| | Performance of the entire test system | 1 year |

^a When operation of the unit permits.

^b Cables and motors may be left connected to switchgear during the switchgear test.

^c The load should equal the manufacturer's rating for the battery for a selected test period, which should preferably be the same period of time as the period of use for which the battery is designed.

^d The discharge rate should correspond as closely as practicable to the load to which the battery will be subjected during the design basis accident for the specified time period (two to four hours).

5.3. In order to ensure the high availability of the EPSs in performing their safety functions, the following measures should be considered:

- (a) Minimizing the time for which equipment is removed from service for the purpose of testing;
- (b) Overriding the test mode on the demand of a safety related action so that the equipment can fulfil its safety function;
- (c) Increasing the redundancy of equipment;
- (d) Using a combination of the above three methods (see Ref. [3]).

5.4. Test methods should be carefully checked for possible negative effects of the test procedures themselves on the EPSs or their availability (e.g. the formation of soot in diesels being tested under no-load conditions or inadequate provisions for restoring normal standby conditions after completion of the test). Slow start test methods should be used to minimize the wear on equipment caused by fast starting of the EPSs.

5.5. Load sequencing and load tests using the actual loads should be performed when the plant is shut down. Only one standby power system should be tested at a time so as to prevent the simultaneous loss of two or more generators. Where the standby power system for a redundant and independent division consists of more than a single electrical generator, its periodic test should demonstrate and verify the entire division's functional performance under conditions as close to the design basis conditions as practicable.

5.6. Provisions should be made in the design to ensure that the following inspections and maintenance programmes are implemented:

- (a) An inspection programme to identify any trend towards degradation (ageing) that could result in the loss of operability of equipment.⁹
- (b) A preventive maintenance programme that periodically inspects components of the EPSs for evidence of deterioration that may not immediately affect performance but which could result in unanticipated failure. The programme should include the replacement of parts that are known to have a limited service life remaining.

5.7. Suitable provision is required to be made in the design and layout of the structures, systems and components of the plant to ensure that radiation doses

⁹ In some States this is referred to as a 'predictive maintenance' programme.

received by the public and by site personnel in all operational states, including maintenance and inspection and decommissioning, do not exceed authorized limits and are as low as reasonably achievable [1, 18–20].

5.8. Provision should be made in the design to ensure that the safety functions can be performed with the required reliability while equipment of the EPSs is being maintained during operation (see paras 2.9–2.10). Provision for an independent temporary power supply should be considered if the maintenance work is extended for a long period of time.

6. CONFIRMATION OF THE DESIGN

QUALITY ASSURANCE

6.1. All activities from the start to the completion of the design and the construction of the EPSs, as well as their operation and maintenance, are required to be planned and conducted under quality assurance programmes (Ref. [1], para. 3.14). Recommendations and guidance are provided in Ref. [21].

6.2. The levels of quality assurance selected for the design of the various parts of the EPSs should be commensurate with their importance to safety.

QUALIFICATION

6.3. A qualification procedure is required to be adopted to confirm that the items important to safety are capable of meeting, throughout their design lives, the demands for performing their functions while being subject to the environmental conditions prevailing at the time of need (Ref. [1], para. 5.45). Equipment used in the EPSs should be capable of fulfilling its performance requirements under the conditions defined by anticipated operational occurrences, design basis accidents and certain severe accidents for the design life of the plant.

6.4. The equipment should be qualified for the operating conditions resulting from anticipated operational occurrences, design basis accidents and certain

severe accidents. The qualification programme should include acceptance criteria for its performance to demonstrate by testing, analysis or a combination of both that the equipment is capable of withstanding the effects of the operating conditions that may occur during its qualified life.

*Qualification methods*¹⁰

6.5. Qualification may be carried out in several ways, either individually or, where necessary, in combination.

Qualification by type testing

6.6. Type testing of the actual performance of equipment by the manufacturer in accordance with recognized standards and conducted under simulated service conditions is a method of qualifying equipment. This method should be used for qualifying the greater part of the equipment in the EPSs. Where the manufacturers' type tests are insufficient for applications in nuclear power plants, additional tests should be performed to demonstrate that the equipment would perform as required in the specified environment.

Qualification by operating experience

6.7. Operating experience can provide information on limits of extrapolation, failure modes and failure rates. Equipment that has operated successfully under comparable service conditions can be considered qualified for equivalent or less severe service.

Qualification by analysis

6.8. Qualification by analysis should include the justification of the methods, theories and assumptions used.

6.9. If the method of qualification by analysis is used, the validity of the mathematical models should be justified on the basis of experimental data or operating experience.

¹⁰ Further guidance is available in several national and international standards (see for instance Refs [22, 23]).

VERIFICATION OF DESIGN

6.10. Recommendations on measures for verifying the adequacy of the design of the EPSs and the general provisions and methods for this verification are provided in Ref. [24].

6.11. As part of the verification, the following should be performed and documented in a form suitable for auditing:

- (a) A performance analysis to demonstrate that the EPSs are capable of fulfilling their safety functions as set out in their design bases;
- (b) Safety assessments at certain stages in the design of the EPSs to demonstrate that the design requirements are met, including compliance with the single failure criterion (see Ref. [24]);
- (c) A reliability analysis (see Ref. [2]), including consideration of common cause failures.

DOCUMENTATION

6.12. Documentation on EPSs should include:

- (a) Information on the design basis, as described in Section 2, including a statement of the assumed off-site electrical grid capabilities.
- (b) Documents and specifications significant for the design, installation, operation, monitoring and testing of the system. These include:
 - (i) A description of the overall power supply system including:
 - Details of how the nuclear power plant is connected to the grid;
 - An explanation of the degree of redundancy of the EPSs;
 - Identification of interfaces with the auxiliary systems to the EPSs (e.g. cooling, ventilation, fuel supply).
 - (ii) A description of the separation criteria for installing equipment, cables and raceways, including wiring and components inside panels.
 - (iii) One-line diagrams, functional control diagrams, schematic diagrams and descriptions of systems.
 - (iv) Layout plans of the buildings of the EPSs together with the arrangements of equipment and associated support systems.
 - (v) Layout plans of cable routes, including trays, ducts and conduits, throughout the plant and identification of redundant divisions and cables and their routing.

- (vi) Co-ordination analysis of electrical protection devices.
- (vii) An electrical load analysis, including both an inventory of electrical loads and a time dependent load analysis from which the capabilities of the necessary components of the EPSs are calculated.
- (viii) Maintenance manuals and documentation for the intended operation of the EPSs, including a periodic test programme.
- (ix) Any special operating and maintenance requirements, e.g. a fuel evaluation programme.
- (x) Documentation of the test programmes and test reports from acceptance tests and operational tests.
- (xi) Quality assurance records.
- (xii) Analyses of voltage and frequency transients, short circuit calculations and voltage drop calculations.
- (xiii) An analysis of the fuel storage capacities for the standby power supply of the EPSs.
- (xiv) An analysis of the consequences of the partial or total loss of power supplies (e.g. off-site and on-site power and power supplies for instrumentation and control).
- (xv) Reports of the equipment qualification programme and test reports.
- (xvi) Specifications of the components of the EPSs.

Appendix

GUIDANCE ON ON-SITE AND OFF-SITE POWER

NORMAL POWER SUPPLIES

A.1. The requirements for EPSs include high reliability, sufficient capacity to supply the necessary power and the possibility of testing their functional capability. The level of reliability of the EPSs in a particular plant depends on the specific situation at the plant site (i.e. the susceptibility to natural and human induced postulated initiating events), the plant configuration (a single reactor or a multiunit plant) and the design of the plant (whether there is an inherent capability for heat removal or a plant generator¹¹ at the plant). Another important parameter that should be considered is the nature of the electrical power supplies (small or large, stable or potentially unstable), since a large part of the EPSs are in general electrically based.

A.2. A number of measures can be taken on and off the site to achieve the required reliability of the electrical part of the EPSs. These measures are discussed in the following paragraphs. Such measures may involve increasing the reliability of the plant's normal power supply¹², from which the EPSs normally draw power, or providing other sources of power to EPSs when the normal power supply may not be available. Where the reliability of the off-site sources is relatively low, the reliability of the on-site capability should be increased so that all the various safety systems have the necessary power available to perform their safety functions when called upon to do so. This may include the use of dedicated power supplies¹³ to safety systems of special importance¹⁴. In the selection of the combination of measures to be taken, the interdependence of the alternative measures and the overall reliability that the combination provides should be carefully assessed. The application of

¹¹ The term 'plant generator' is used for the turbogenerator that produces the electrical output of the nuclear power plant.

¹² See Fig. 1 for the use of some of the terms.

¹³ The term 'dedicated power supply' means equipment that provides, for example, pneumatic or electrical power exclusively for a particular application; for example, a separate, independent electrical turbogenerator directly driven by a steam turbine to drive pumps and valves.

¹⁴ See Fig. 4 for a schematic overview.

probabilistic safety analysis to determine the adequacy of the solution selected should be considered.

GRID STABILITY

A.3. An electrical 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. In the initial site selection for a nuclear power plant, the stability of the electrical grid should be evaluated. Where there is poor grid stability, measures for improving it should be considered or, if practicable, an alternative site with greater grid stability should be selected. If no alternative site having adequate grid stability is available, the EPSs should be provided with more redundancy and diversity in order to compensate for the higher expected frequency of grid disturbances leading to the loss of off-site power. In addition, in designing the plant, consideration should be given to the capability to withstand load rejection with runback without undergoing a reactor trip or a turbogenerator trip, so as to continue to power house loads¹⁵ (see para. A.13).

A.4. The stability of the electrical grid is a function of many parameters. These include: the system power generation and reserve power generation in peak and off-peak periods; the operating spinning reserve; the number and size of generating units and their characteristics; the number and characteristics of interconnections to adjacent power systems; and the number of transmission lines and their characteristics, including the characteristics of their protective relays and circuit breakers.

A.5. The philosophy followed both in adding new generating capacity and in designing the power system network has a direct influence on the stability of the electrical grid. For example, load flow studies and stability analysis should be used to determine the optimum unit size for a particular system, together with the spinning reserve required to maintain a stable system. The possible effects of other grid disturbances that could lead to severe fluctuations in the system voltage and the frequency, and thereby affect the performance of large electrical machines such as reactor coolant pumps, should also be taken into consideration.

¹⁵ The house load includes all electrical loads in the plant.

A.6. The possibility that the loss of the largest operating unit on the grid may result in instability of the grid, leading to a collapse of the total system and thereby cutting off-site power to the plant, is of particular importance and should be taken into consideration. For some grid systems a practice is employed which consists of load shedding of user loads at the subtransmission and distribution levels in order to maintain the system frequency when there is insufficient generation. As a last resort, the generating units are separated from the grid if the system frequency drops too low. Because of their effect on grid stability, these factors should be carefully considered when selecting a nuclear power unit for a particular power system.

TRANSMISSION LINES

A.7. The number of transmission line connections to the electrical grid will depend on the design capabilities of the entire grid and on the design of the nuclear power plant itself.

A.8. A single connection by transmission line to the grid may be acceptable in situations where the nuclear power plant represents a large proportion of the generation on the electrical grid or where the grid stability is such that the loss of that nuclear power plant would lead directly to the collapse of the grid. In such situations the provision of a second transmission line to the grid would add little by way of enhancing the reliability of the EPSs; other measures should therefore be taken on the site.

A.9. Where the power generation of the nuclear power plant is a small proportion of the total power generation of the grid, and the grid is considered stable in the event of the loss of the plant (or a unit of the plant), the preferred approach is to provide at least two transmission line connections between the plant site and the grid. Each transmission line should have the capability to be available sufficiently quickly to ensure that the fuel design limits and the design conditions of the pressure boundary for the reactor coolant are not exceeded. Where more than one transmission line is used to connect a nuclear power plant to the grid, these should be adequately separated or even connected to different parts of the grid that are relatively independent so as to avoid the common cause failure of two or more lines. The use of three or more connections to the grid may not lead to increased reliability unless the connections can be made at different points in the grid. However, for plants at sites remote from the main grid network, it may not be practicable to run more than a single transmission line. In the case of connection of the plant to the grid

by a single transmission line, it should be ensured that no other transmission lines use the same transmission tower.

A.10. It is possible to lose all the transmission lines to a plant at the same time, regardless of their number. Certain natural phenomena such as tornadoes, earthquakes and hurricanes might cause the loss of all transmission lines to the site. Also, since all the transmission and distribution systems of a grid are interconnected, the collapse of a major part could result in the failure of most, if not all, of the grid.

A.11. Nuclear power plants with a single transmission line may 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, either the nuclear power plant should be designed to withstand the effects of the forced outages or measures should be taken to reduce the number of forced outages, possibly by adding additional transmission lines.

ON-SITE MEASURES

A.12. The normal power supply to the EPSs of a nuclear power plant generally derives its power from the grid via one or more transmission lines or from the plant generator, or from some combination of these. In order to make the least number of transfer demands on the plant's electrical switchgear, the preferred source of supply selected for normal plant operation should be the more reliable of the two alternatives. In cases of loss of power from the preferred source, the most reliable of the remaining sources should be automatically selected.

A.13. 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 just sufficient to meet the electrical power needs of the disconnected plant (the house load) without tripping the steam supply or the turbogenerator. This capability to accept load rejection and to run back to house load is particularly important in designs in which a nuclear plant is supplied by a single transmission line from the transmission grid. Consideration should be given in the design to the benefits of this feature.

A.14. With single or multiple transmission line connections to the grid, electrical power may be supplied to the EPSs under normal operation from the

connection joining the plant generator to the grid, via the plant's electrical auxiliary system (see Fig. 1). The supply of power from the grid when the plant generator is unavailable requires the use of a circuit breaker located on the generator side of this connection. Similarly, ensuring the supply of electrical power from the plant generator when power from the grid is unavailable also requires the use of a circuit breaker located between the generator connection and the transmission line connection(s). The acceptability of this arrangement for supplying electrical power to the EPSs depends on the use of circuit breakers between the plant generator and the transmission line(s). These circuit breakers should be of high quality, fully rated and capable of withstanding the maximum current to which they can be subjected and of interrupting the rated and fault currents for which they are provided. This arrangement provides continuous power, either from the plant's turbogenerator or from the transmission line(s), in all conditions except those where faults occur between the circuit breakers or where there are coincident faults in the plant generator and the transmission line(s). In addition to these provisions, alternative supplies from the external grid that prevent the early startup of standby power sources when the main connection to the grid fails should be considered if necessary.

A.15. An example of arrangements that continue to provide power when there are single faults between the plant generator and the transmission lines is shown in Fig. 2. This illustrates a double connection grid.

ALTERNATIVE POWER SUPPLIES

A.16. In addition to the normal power supply to the EPSs, there may be alternative power sources on or off the site that can be used to increase the reliability of the EPSs but which are not themselves part of these systems; for example, fossil fuel generators normally used for load peaking duties or localized electrical grid networks off the site for special purposes. At a multiunit site, an important feature in this context is the ability to feed power to the EPSs of any one reactor unit from the plant generators of other reactor units independently of the state of the transmission lines to the electrical grid.

A.17. Such alternative power sources should be considered in the design of the EPSs. The reliance placed on alternative power sources, whether they are connected automatically or manually, will depend on a number of factors, including their reliability, their design and, in particular, the degree of administrative control that the plant operators can exercise over their operation.

REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Single Failure Criterion, Safety Series No. 50-P-1, IAEA, Vienna (1990).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000).
- [5] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Terminology and Test Procedures for Neutral Grounding Devices, IEEE Standard 32 – 1972, Piscataway, NJ (1990).
- [6] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Guide for Measuring Earth Resistivity, Ground Impedance and Earth Surface Potentials of a Ground System, IEEE Standard 81 – 1983, Piscataway, NJ (1983).
- [7] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Recommended Practice for Electric Power Distribution for Industrial Plants, IEEE Standard 141 – 1993, Piscataway, NJ (1993).
- [8] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Recommended Practice for Grounding of Industrial and Commercial Power Systems, IEEE Standard 142 – 1991, Piscataway, NJ (1991).
- [9] VERBAND DEUTSCHER ELEKTROTECHNIKER, Bestimmungen für das Errichten von Starkstromanlagen mit Nennspannungen bis 1000 V, DIN VDE Standard 0100, Frankfurt (1973).
- [10] VERBAND DEUTSCHER ELEKTROTECHNIKER, Erdungen für spezielle Starkstromanlagen mit Nennspannungen über 1 kV, DIN VDE Standard 0141, Frankfurt (2000).
- [11] ASSOCIATION FRANÇAISE DE NORMALISATION, Low Voltage Electrical Installations, Certified Standard NF CF15-100, AFNOR, Paris La Défense (2000).
- [12] ASSOCIATION FRANÇAISE DE NORMALISATION, Surge Arresters – Part 1: Non-linear Resistor Type Gapped Surge Arresters for AC Systems, Certified Standard NF EN 6009-1, AFNOR, Paris La Défense (2000).
- [13] ASSOCIATION FRANÇAISE DE NORMALISATION, High Voltage Electrical Installations: Requirements, Certified Standard NF C13-200, AFNOR, Paris La Défense (1989).
- [14] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Electrical Installations of Buildings, IEC Standard No. 60364-4, Geneva (1980).
- [15] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004).

- [16] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003).
- [17] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards Other than Fires and Explosions in the Design of Nuclear Power Plants, Safety Standards Series No. NS-G-1.11, IAEA, Vienna (2004).
- [18] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, Occupational Radiation Protection, Safety Standards Series No. RS-G-1.1, IAEA, Vienna (1999).
- [19] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANISATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).
- [20] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects in the Design of Nuclear Power Plants, Safety Standards Series, IAEA, Vienna (in preparation).
- [21] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations, Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).
- [22] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE Standard A323 — 1983, Piscataway, NJ (1983).
- [23] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Electrical Equipment of the Safety System — Qualification, IEC Standard No. 60780, Geneva (1998).
- [24] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).

GLOSSARY

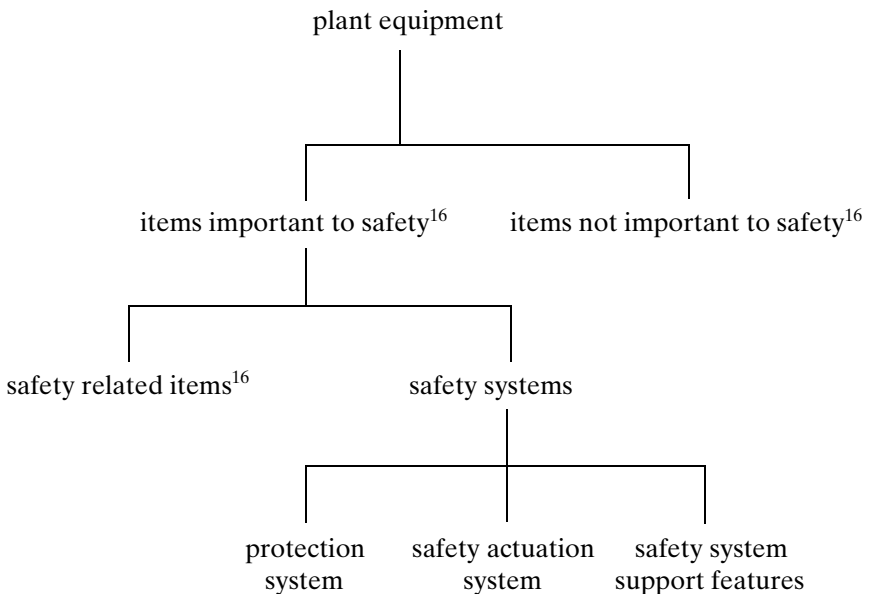
common cause failure. Failure of two or more structures, systems or components due to a single specific event or cause.

design. The process and the result of developing a concept, detailed plans, supporting calculations and specifications for a facility and its parts.

diversity. The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure.

operational limits and conditions. A set of rules setting forth parameter limits, the functional capability and the performance levels of equipment and personnel approved by the regulatory body for safe operation of an authorized facility.

plant equipment:



¹⁶ In this context, an 'item' is a structure, system or component.

item important to safety: An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public. 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 which prevent anticipated operational occurrences from leading to accident conditions; and
- those features which are provided to mitigate the consequences of malfunction or failure of structures, systems or components.

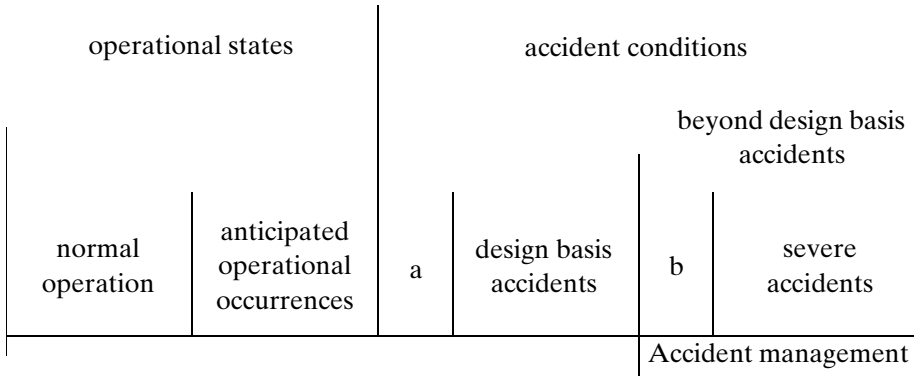
protection system: System which monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition. The ‘system’ in this case encompasses all electrical and mechanical devices and circuitry, from sensors to actuation device input terminals.

safety related item: An item important to safety which is not part of a safety system.

safety system: A system important to safety, 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 and design basis accidents. Safety systems consist of the protection system, the safety actuation systems and the safety system support features. Components of safety systems may be provided solely to perform safety functions or may perform safety functions in some plant operational states and non-safety functions in other operational states.

safety system support features: The collection of equipment that provides services such as cooling, lubrication and energy supply required by the protection system and the safety actuation systems.

plant states:



a = Accident conditions which are not explicitly considered design basis accidents but are encompassed by them.

b = Beyond design basis accidents without significant core degradation.

accident conditions: Deviation from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents.

anticipated operational occurrence: An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

design basis accident: Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

normal operation: Operation within specified operational limits and conditions.

operational states: States defined under normal operation and anticipated operational occurrences.

severe accident: Accident conditions more severe than a design basis accident and involving significant core degradation.

postulated initiating event. An event identified during design as capable of leading to anticipated operational occurrences or accident conditions.

quality assurance. Planned and systematic actions necessary to provide adequate confidence that an item, process or service will satisfy given requirements for quality, for example, those specified in the licence.

redundancy. Provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other.

safety function. A specific purpose that must be accomplished for safety.

single failure. A failure which results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it.

CONTRIBUTORS TO DRAFTING AND REVIEW

| | |
|------------|---|
| Chopra, O. | Nuclear Regulatory Commission, United States of America |
| Duong, M. | International Atomic Energy Agency |
| Faya, A. | Nuclear Safety Commission, Canada |
| Saito, T. | International Atomic Energy Agency |

BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS

An asterisk () denotes a corresponding member. Corresponding members receive drafts for comment and other documentation but they do not generally participate in meetings.*

Commission on Safety Standards

Argentina: Oliveira, A.; Brazil: Caubit da Silva, A.; Canada: Pereira, J.K.; France: Gauvain, J.; Lacoste, A.-C.; Germany: Renneberg, W.; India: Sukhatme, S.P.; Japan: Tobioka, T.; Suda, N.; Korea, Republic of: Eun, S.; Russian Federation: Malyshev, A.B.; Vishnevskiy, Y.G.; Spain: Azuara, J.A.; Santoma, L.; Sweden: Holm, L.-E.; Switzerland: Schmocker, U.; Ukraine: Gryschenko, V.; United Kingdom: Hall, A.; Williams, L.G. (Chairperson); United States of America: Travers, W.D.; IAEA: Karbassioun, A. (Co-ordinator); International Commission on Radiological Protection: Clarke, R.H.; OECD Nuclear Energy Agency: Shimomura, K.

Nuclear Safety Standards Committee

*Argentina: Sajaroff, P.; Australia: MacNab, D.; *Belarus: Sudakou, I.; Belgium: Govaerts, P.; Brazil: Salati de Almeida, I.P.; Bulgaria: Gantchev, T.; Canada: Hawley, P.; China: Wang, J.; Czech Republic: Böhm, K.; *Egypt: Hassib, G.; Finland: Reiman, L. (Chairperson); France: Saint Raymond, P.; Germany: Feige, G.; Hungary: Vöröss, L.; India: Kushwaha, H.S.; Ireland: Hone, C.; Israel: Hirshfeld, H.; Japan: Yamamoto, T.; Korea, Republic of: Lee, J.-I.; Lithuania: Demcenko, M.; *Mexico: Delgado Guardado, J.L.; Netherlands: de Munk, P.; *Pakistan: Hashimi, J.A.; *Peru: Ramírez Quijada, R.; Russian Federation: Baklushin, R.P.; South Africa: Bester, P.J.; Spain: Mellado, I.; Sweden: Jende, E.; Switzerland: Aeberli, W.; *Thailand: Tanipanichskul, P.; Turkey: Alten, S.; United Kingdom: Hall, A.; United States of America: Mayfield, M.E.; European Commission: Schwartz, J.-C.; IAEA: Bevington, L. (Co-ordinator); International Organization for Standardization: Nigon, J.L.; OECD Nuclear Energy Agency: Hrehor, M.*

Radiation Safety Standards Committee

*Argentina: Rojkind, R.H.A.; Australia: Melbourne, A.; *Belarus: Rydleviski, L.; Belgium: Smeesters, P.; Brazil: Amaral, E.; Canada: Bundy, K.; China: Yang, H.; Cuba: Betancourt Hernandez, A.; Czech Republic: Drabova, D.; Denmark: Ulbak, K.; *Egypt: Hanna, M.; Finland: Markkanen, M.; France: Piechowski, J.; Germany: Landfermann, H.; Hungary: Koblinger, L.; India: Sharma, D.N.; Ireland: Colgan, T.; Israel: Laichter, Y.; Italy: Sgrilli, E.; Japan: Yamaguchi, J.; Korea, Republic of: Kim, C.W.; *Madagascar: Andriambololona, R.; *Mexico: Delgado Guardado, J.L.; *Netherlands: Zuur, C.; Norway: Saxebol, G.; *Peru: Medina Gironzini, E.; Poland: Merta, A.; Russian Federation: Kutkov, V.; Slovakia: Jurina, V.; South Africa: Olivier, J.H.I.; Spain: Amor, I.; Sweden: Hofvander, P.; Moberg, L.; Switzerland: Pfeiffer, H.J.; *Thailand: Pongpat, P.; Turkey: Uslu, I.; Ukraine: Likhtarev, I.A.; United Kingdom: Robinson, I. (Chairperson); United States of America: Paperiello, C.; European Commission: Janssens, A.; IAEA: Boal, T. (Co-ordinator); International Commission on Radiological Protection: Valentin, J.; International Labour Office: Niu, S.; International Organization for Standardization: Perrin, M.; International Radiation Protection Association: Webb, G.; OECD Nuclear Energy Agency: Lazo, T.; Pan American Health Organization: Jimenez, P.; United Nations Scientific Committee on the Effects of Atomic Radiation: Gentner, N.; World Health Organization: Carr, Z.*

Transport Safety Standards Committee

*Argentina: López Vietri, J.; Australia: Colgan, P.; *Belarus: Zaitsev, S.; Belgium: Cottens, E.; Brazil: Mezrahi, A.; Bulgaria: Bakalova, A.; Canada: Viglasky, T.; China: Pu, Y.; *Denmark: Hannibal, L.; Egypt: El-Shinawy, R.M.K.; France: Aguilar, J.; Germany: Rein, H.; Hungary: Sáfár, J.; India: Nandakumar, A.N.; Ireland: Duffy, J.; Israel: Koch, J.; Italy: Trivelloni, S.; Japan: Saito, T.; Korea, Republic of: Kwon, S.-G.; Netherlands: Van Halem, H.; Norway: Hornkjøl, S.; *Peru: Regalado Campaña, S.; Romania: Vieru, G.; Russian Federation: Ershov, V.N.; South Africa: Jutle, K.; Spain: Zamora Martin, F.; Sweden: Pettersson, B.G.; Switzerland: Knecht, B.; *Thailand: Jerachanchai, S.; Turkey: Köksal, M.E.; United Kingdom: Young, C.N. (Chairperson); United States of America: Brach, W.E.; McGuire, R.; European Commission: Rossi, L.; International Air Transport Association: Abouchaar, J.; IAEA: Wangler, M.E. (Co-ordinator); International Civil Aviation Organization: Rooney, K.; International Federation of Air Line Pilots' Associations: Tisdall, A.; International Maritime Organization: Rahim, I.; International Organization for*

Standardization: Malesys, P.; United Nations Economic Commission for Europe: Kervella, O.; World Nuclear Transport Institute: Lesage, M.

Waste Safety Standards Committee

*Argentina: Siraky, G.; Australia: Williams, G.; *Belarus: Rozdialovskaya, L.; Belgium: Baekelandt, L. (Chairperson); Brazil: Xavier, A.; *Bulgaria: Simeonov, G.; Canada: Ferch, R.; China: Fan, Z.; Cuba: Benitez, J.; *Denmark: Øhlenschlaeger, M.; *Egypt: Al Adham, K.; Al Sorogi, M.; Finland: Ruokola, E.; France: Averous, J.; Germany: von Dobschütz, P.; Hungary: Czoch, I.; India: Raj, K.; Ireland: Pollard, D.; Israel: Avraham, D.; Italy: Dionisi, M.; Japan: Irie, K.; Korea, Republic of: Song, W.; *Madagascar: Andriambololona, R.; Mexico: Aguirre Gómez, J.; Delgado Guardado, J.; Netherlands: Selling, H.; *Norway: Sorlie, A.; Pakistan: Hussain, M.; *Peru: Gutierrez, M.; Russian Federation: Poluektov, P.P.; Slovakia: Konecny, L.; South Africa: Pather, T.; Spain: López de la Higuera, J.; Ruiz López, C.; Sweden: Wingefors, S.; Switzerland: Zurkinden, A.; *Thailand: Wangcharoenroong, B.; Turkey: Osmanlioglu, A.; United Kingdom: Wilson, C.; United States of America: Greeves, J.; Wallo, A.; European Commission: Taylor, D.; IAEA: Hioki, K. (Co-ordinator); International Commission on Radiological Protection: Valentin, J.; International Organization for Standardization: Hutson, G.; OECD Nuclear Energy Agency: Riotte, H.*