

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

AVA Documents
Document Sharing Hub

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	TAJIKISTAN
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].