2019-01-18

IAEA SAFETY STANDARDS

for protecting people and the environment

STATUS: SPESS STEP 12

Approved by Review Committees

Reviewed in NSOC (Shaw).

For submission to CSS for approval.

Design of Auxiliary Systems and Supporting Systems for Nuclear Power Plants

DS 440

DRAFT SAFETY GUIDE

New Safety Guide

FOREWORD

Later

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide provides recommendations on how to meet the requirements established in IAEA Safety Standards Series No. SSR-2/1 (Rev.1), Safety of Nuclear Power Plants: Design [1], in relation to the design of auxiliary systems and supporting systems for nuclear power plants.

1.2. Auxiliary systems and supporting systems are those systems that provide electricity, service gas, water, compressed air, air conditioning, means of communication, means of lifting and lowering items, and fuel and lubricants, all of which are important for the operation and safety of nuclear power plants. The reliability of these systems should be commensurate with their importance for safety.

OBJECTIVE

1.3. The objective of this Safety Guide is to provide recommendations for designers, operating organizations, regulatory bodies and technical support organizations on the design of auxiliary systems and supporting systems, in order to meet the requirements established in SSR-2/1 (Rev. 1) [1] for these systems.

SCOPE

1.4. This Safety Guide provides design recommendations for the auxiliary systems and supporting systems for nuclear power plants with pressurized water reactors, boiling water reactors or pressurized heavy water reactors.

1.5. The list of auxiliary systems and supporting systems considered in this Safety Guide is set out in paras 2.5 and 2.6. The scope does not extend to the detailed design of specific components of these systems, for example heat exchangers.

1.6. The recommendations provided in this Safety Guide are targeted primarily at new nuclear power plants. For nuclear power plants designed to earlier standards, it is expected that in the safety assessments of such designs a comparison will be made with the current standards (for example as part of the periodic safety reassessment for the plant), to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements: see para. 1.3 of SSR-2/1 (Rev. 1) [1].

1.7. The terms used in this Safety Guide are to be understood as defined and explained in the IAEA Safety Glossary [2].

STRUCTURE

1.8. Section 2 provides a definition of auxiliary systems and supporting systems and describes their functions and extent. Section 3 describes the general design concepts and design recommendations that are common to the auxiliary systems and supporting systems addressed in the Safety Guide. Section 4 provides recommendations on specific design considerations for a selection of auxiliary systems and supporting systems.

2. GENERAL ASPECTS

DEFINITIONS AND FUNCTIONS OF AUXILIARY SYSTEMS AND SUPPORTING SYSTEMS

2.1. A nuclear power plant has the following main (or primary) systems: the reactor core, the reactor coolant system and the containment structure and containment system and their associated safety systems and safety features (see Requirements 43–58 of SSR-2/1 (Rev.1) [1]). The remaining systems are considered auxiliary systems (see Requirements 59–82 of SSR-2/1 (Rev.1) [1]) to the main systems and their associated features.

2.2. A stepwise approach to defining auxiliary systems is shown in Figure 1. An auxiliary system is a system that, on its own, has no primary function in ensuring the operation of the nuclear power plant, but which has to be available for other systems, including the main systems, to carry out their functions.

2.3. Alternatively, an auxiliary system could be a system that provides services for the operation of the nuclear power plant (e.g. communication systems, compressed air system). Auxiliary systems can provide ‘essential services’, namely the resources necessary to maintain the operability of a safety system. They can also provide supplies to systems important to safety. Such services could include electricity, water, compressed air, fuel and lubricants.

2.4. In this Safety Guide, the term ‘supporting systems’ is used to describe those auxiliary systems that support safety functions.

EXTENT OF THE AUXILIARY SYSTEMS AND SUPPORTING SYSTEMS

2.5. The auxiliary systems and supporting systems addressed in this Safety Guide, as defined in para. 2.2, do not include those systems that are (or are intended to be) addressed in other Safety Guides. For example:

(a) Heat transport systems (Requirement 70 of SSR-2/1 (Rev.1) [1]) removing residual heat are addressed in detail in IAEA Safety Standards Series No. DS481, Design of the Nuclear Coolant System and Associated Systems in Nuclear Power Plants [3];

(b) Fire protection systems (Requirement 74 of SSR-2/1 (Rev.1) [1]) are addressed in IAEA Safety Standards Series No. NS-G-1.7 [4], Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants;

(c) The steam supply system and feedwater system (Requirement 77 of SSR-2/1 (Rev.1) [1]) are addressed in DS481 [3];

(d) Radiation protection systems (Requirement 81 of SSR-2/1 (Rev.1) [1]) are addressed in IAEA Safety Standards Series No. NS-G-1.13 [5], Radiation Protection Aspects of Design for Nuclear Power Plants.

2.6. Based on paras 2.2 and 2.5, and in accordance with the requirements of SSR-2/1 (Rev.1) [1], the auxiliary systems and supporting systems that are considered in this Safety Guide are as follows:

(a) Communication systems (Requirement 37 of SSR-2/1 (Rev.1) [1]).
(b) Heat transport systems (Requirement 70 of SSR-2/1 (Rev.1) [1]) that are not considered in DS481.
(c) The process and post-accident sampling system (Requirement 71 of SSR-2/1 (Rev.1) [1]).
(d) The process radiation monitoring system (Requirement 82 of SSR-2/1 (Rev.1) [1]);
(e) The compressed air system (Requirement 72 of SSR-2/1 (Rev.1) [1]).
(f) Air conditioning systems and ventilation systems (Requirement 73 of SSR-2/1 (Rev.1) [1]).
(g) Lighting and emergency lighting systems (Requirement 75 of SSR-2/1 (Rev.1) [1]).
(h) Overhead lifting equipment (Requirement 76 of SSR-2/1 (Rev.1) [1]).
(i) Systems for treatment of radioactive effluents and radioactive waste (Requirements 78 and 79 of SSR-2/1 (Rev.1) [1]).
(j) Supporting systems for the emergency power supply and the alternate power source (Requirement 68 of SSR-2/1 (Rev.1) [1]).
(k) Other systems not explicitly indicated in SSR-2/1 (Rev.1) [1] but which (depending on the design of the nuclear power plant) are usually considered auxiliary systems or supporting systems. These are:
    - The equipment and floor drainage system;
    - The de-mineralized water system.

SAFETY FUNCTIONS

2.7. Auxiliary systems and supporting systems can directly or indirectly contribute to the fulfilment of safety functions, for example to ensure essential services (such as electrical, pneumatic, hydraulic power supplies, lubrication), or can provide a supporting function for a safety system or a safety feature for design extension conditions. The safety functions associated with specific auxiliary systems and supporting systems are described in Section 4.

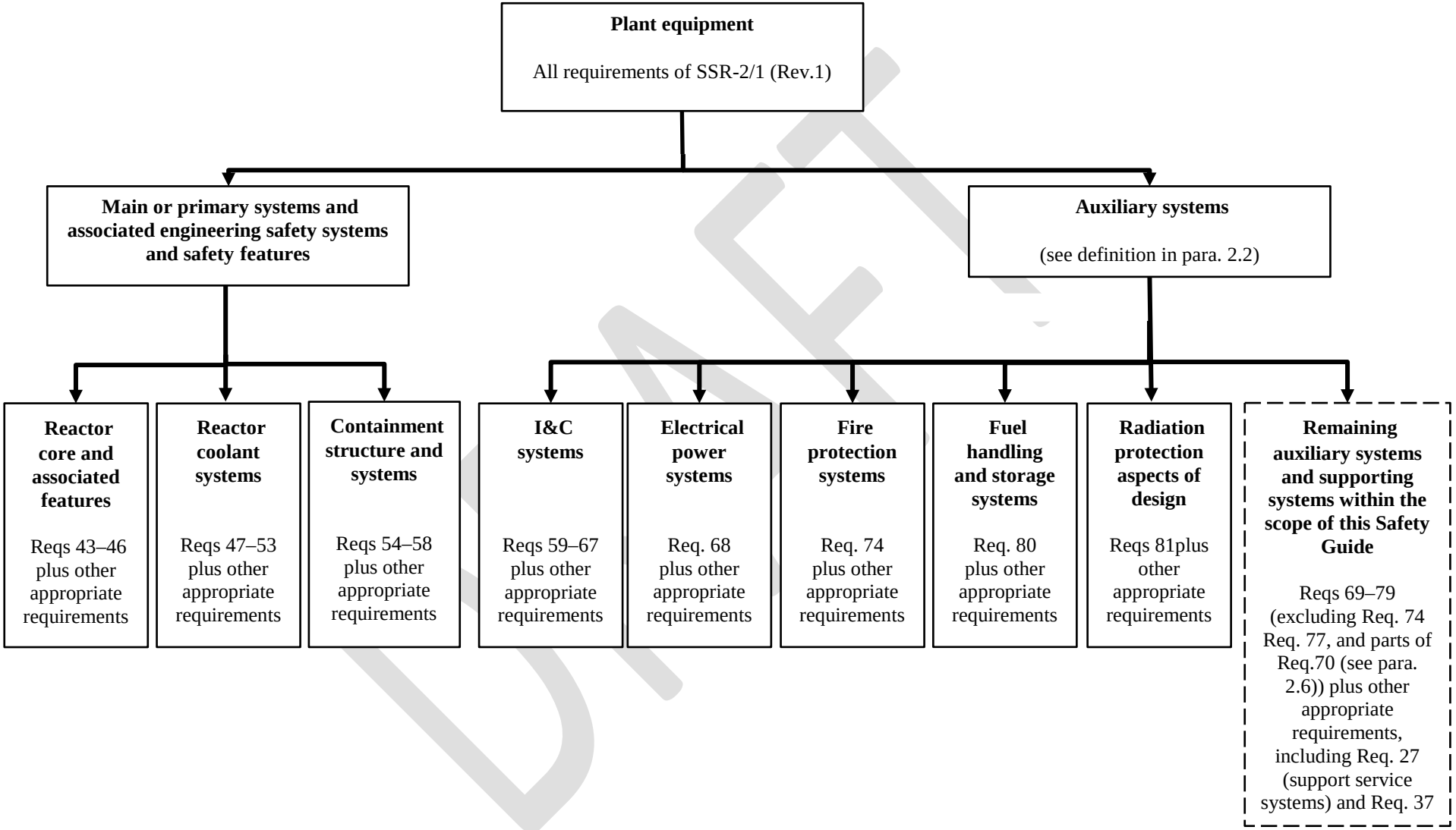

FIG.1. The auxiliary systems and supporting systems within the scope of this Safety Guide

3. GENERAL CONSIDERATIONS IN DESIGN

3.1. This section provides recommendations for design that are common to the auxiliary systems and supporting systems considered in this Safety Guide and that are applicable, as appropriate, to all water cooled reactors. The recommendations in this section are aimed at meeting the requirements established in SSR-2/1 (Rev.1) [1] for auxiliary systems and supporting systems, in particular Requirement 69 on the performance of auxiliary systems and supporting systems, which states that:

> "The design of supporting systems and auxiliary systems shall be such as to ensure that the performance of these systems is consistent with the safety significance of the system or component that they serve at the nuclear power plant.".

OBJECTIVES OF THE DESIGN

3.2. The design of auxiliary systems and supporting systems should assist in the fulfilment of the fundamental safety functions described in Requirement 4 of SSR-2/1 (Rev.1) [1]. The specific measures necessary to ensure this will differ depending on the system, the reactor type, the operating conditions and the plant site conditions.

3.3. The design of the auxiliary systems and supporting systems should be such that safety and security are addressed in an integrated manner and that safety measures do not compromise nuclear security and nuclear security measures do not compromise safety. Nuclear security measures should be consistent with the objective and essential elements established in IAEA Nuclear Security Series No. 20 [6] and the recommendations provided in IAEA Nuclear Security Series No. 13 [7].

3.4. The safety class of auxiliary systems and supporting systems or components of such systems should be assigned with due consideration of the following:

(a) The safety class of the systems or components that they support;
(b) The safety function fulfilled by the systems or components that they support, and for which the operation of the auxiliary systems and supporting systems or components is necessary;
(c) The consequences of failure of the auxiliary systems and supporting systems.

3.5. Each system providing an essential service should have the capacity, autonomy time[1], availability, robustness and reliability that is commensurate with the associated safety function(s) and with the maximum necessary demands of the systems that it supports, with appropriate margins.

[1] 'Autonomy time' refers to the period of time that a system can continue to operate autonomously, e.g. while other systems are unavailable.

3.6. For nuclear power plants that rely on the forces of buoyancy or gravity or on stored energy sources to perform a safety function and that contain fewer active components there might be much less need for safety classified auxiliary systems and supporting systems to support the safety functions.

3.7. The performance of a safety function depends not only on the reliability of the main systems that ensure its fulfilment but also on the reliability of the auxiliary systems and supporting systems that are necessary to support the main systems in performing this function. Therefore, the reliability and design requirements of auxiliary systems and supporting systems should be commensurate with the reliability of the systems they support. Hence, the design of auxiliary systems and supporting systems should be assessed at the same level of detail as for the main systems they support. In addition, the requirements of SSR-2/1 (Rev.1) [1] relating to the design basis for structures, systems and components apply, as appropriate, to the design of the structures, systems and components of auxiliary systems and supporting systems.

DESIGN BASIS

General

3.8. The design basis for the safety classified structures, systems and components of auxiliary systems and supporting systems should include any conditions associated with normal operation, anticipated operational occurrences and accident conditions (design basis accidents and design extension conditions) for which the operation of the auxiliary systems and supporting systems is necessary.

3.9. Design conditions and design loads should be calculated, as appropriate, with account taken of bounding cases determined for each of the relevant plant states or hazards.

3.10. The expected performance of the structures, systems and components of auxiliary systems and supporting systems should be derived from the demands induced by the safety functions that the supported systems have to ensure.

3.11. A design basis should be defined for every structure, system and component and should take into account the following (see paragraphs 3.12 to 3.79):

- The safety function(s) to be performed by the structure, system or component;
- The postulated initiating events that the structure, system or component has to withstand;
- The loads and load combinations that the structure or component has to withstand;
- The protection against the effects of internal hazards;
- The protection against the effects of external hazards;
- Design limits and acceptance criteria (applicable to the design of structure, system and component);
- Reliability;

- Provision against common cause failures within a system and between systems belonging to different levels of defence in depth;
- The safety classification;
- The environmental conditions considered in the qualification programme;
- Design codes and standards;
- Layout considerations;
- Interface considerations;
- Considerations for a multiple unit nuclear power plant, if appropriate;
- Use of probabilistic safety assessment in the design.

Safety functions

3.12. The safety function(s) to be fulfilled by an auxiliary system or supporting system and the contribution of each component important to safety should be described at a level of detail sufficient for a correct safety classification.

Postulated initiating events

3.13. The design of the plant should be such that a failure of the auxiliary systems and supporting systems would not lead to a postulated initiating event. If such an event is foreseeable, the design should include appropriate measures for the mitigation of the event, with account taken of the effects of the failure of the auxiliary system or supporting system on other plant systems.

Internal hazards

3.14. Paragraphs 3.15–3.17 provide recommendations on meeting Requirement 17 of SSR-2/1 (Rev.1) [1], in particular para. 5.16 on internal hazards.

3.15. Internal hazards that should be considered are those of internal origin that could jeopardize the performance of a structure, system or component of an auxiliary system or supporting system. A list of typical internal hazards usually considered is provided below for guidance; however, this list should be supplemented, as necessary, to include design specific hazards relevant for the structures, systems and components of the auxiliary system or supporting system:

- Breaks in high energy systems;
- Heavy load drop;
- Internal missiles;
- Fire and explosions;
- Flooding;
- Electromagnetic interference.

3.16. Layout and design provisions should be provided to protect the structures, systems and components of auxiliary systems and supporting systems against the effects of the internal hazards to be considered in accordance withpara. 3.7. For example, where relevant:

(a) The structures, systems and components of auxiliary systems and supporting systems should be protected against impacts of high energy hazards (internal explosions, internal missiles, pipe whipping, jet impingement, heavy load drops), or else they should be designed to withstand the loads generated by such hazards;
(b) Redundant systems should be segregated to the extent possible, or else they should be adequately separated and protected, as necessary, to prevent the loss of the safety function performed by the systems;
(c) The segregation, separation and protection measures implemented should also be adequate to ensure that the system response as modelled in the analysis of postulated initiating events is not compromised by the effects of the hazard;
(d) A single hazard should not have the potential for a common cause failure between auxiliary systems and supporting systems that support safety systems designed to control design basis accidents, and the safety features required in the event of design extension conditions, especially accidents with core melting.

3.17. More detailed recommendations are provided in NS-G-1.7 [4] and NS-G-1.11 [8].

External hazards

3.18. Paragraphs 3.19–3.28 provide recommendations on meeting Requirement 17 of SSR-2/1 (Rev.1) [1] in relation to external hazards.

3.19. Auxiliary systems and supporting systems needed to ensure the operation of systems necessary to mitigate accident conditions should be designed to withstand or should be protected against the effects of design basis external hazards and against common cause failure mechanisms that could be generated by those hazards. The design of these auxiliary and supporting systems should be consistent with the design of such mitigatory systems and with due consideration of the function of the auxiliary systems and supporting systems.

3.20. Any structure, system or component whose failure could compromise the operation of the auxiliary systems and supporting systems described in para. 3.19 should be designed to withstand the same design basis external hazards or be protected against the effects of these design basis external hazards and against common cause failure mechanisms that could be generated by those hazards.

3.21. Any structure, system or component of an auxiliary system or a supporting system whose failure could initiate accident conditions should be designed to withstand or should be protected against the

effects of design basis external hazards and against common cause failure mechanisms that could be generated by those hazards.

3.22. For each external hazard, components of auxiliary systems and supporting systems whose operability or integrity is necessary during and/or after the hazard should be identified and specified in the design basis of the components.

3.23. The design methods, and the design and construction codes used should provide adequate margins to avoid cliff edge effects in the event of a slight increase in the severity of the external hazards.

3.24. For external hazards, short term actions to be performed by auxiliary systems and supporting systems, and which are necessary to meet the limits and engineering criteria established for the supported system in the event of accident conditions, should be accomplished with on-site systems that are ready to operate in a time commensurate with the short term actions to be taken (see para. 5.17 of SSR-2/1 (Rev.1) [1]).

3.25. The autonomy time of systems supporting safety functions should be longer than the time at which off-site services are credited. The measures taken at the plant and at the site can be credited in determining this time, provided that the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously has been considered (see para. 5.15B of SSR-2/1 (Rev.1) [1]). With regard to external supplies, consideration should be given, as necessary, to the adverse conditions and damage caused by the external hazards.

3.26. Compliance with para. 5.21A of SSR-2/1 (Rev.1) [1], requires that the structures, systems and components ultimately necessary to prevent an early or large radioactive release are still operable in the event of levels of external natural hazards exceeding those considered for design, with account taken of the hazard evaluation for the site. This applies to auxiliary systems and supporting systems whose operability is necessary for this purpose.

3.27. With regard to external flooding, either all the structures hosting the systems described in para. 3.26 should be located at an elevation higher than the elevation of the design basis flood, or else adequate provisions (e.g., water tight doors) need to be provided in the design to protect these systems and ensure that their safety functions can be maintained.

3.28. More detailed recommendations are provided in IAEA Safety Standards Series No. NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants [9] and IAEA Safety Standards Series No. NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants [10].

Accident conditions

3.29. Accident conditions relevant for the design of an auxiliary system or supporting system are those conditions having the potential to jeopardize the safety functions that the auxiliary system or supporting system is contributing to.

3.30. Depending on the design, the failure of certain auxiliary systems and supporting systems has the potential to lead to worse accident conditions, including a severe accident. Therefore, particular attention should be paid to ensure a high reliability of such systems, in particular for accident sequences associated with a loss of off-site power and accident sequences associated with a loss of cooling function or a loss of the ultimate heat sink.

3.31. When considering multiple failures leading to design extension conditions, the failure of auxiliary systems and supporting systems that support safety systems, or that support safety features for design extension conditions without significant fuel degradation, should be taken into account.

3.32. Accident conditions should be used as inputs for determining capabilities, loads and environmental conditions in the design of the parts of the auxiliary systems and supporting systems needed for these accident conditions.

3.33. More detailed recommendations on meeting Requirements 18–20 of SSR-2/1 (Rev.1) [1] are provided in IAEA Safety Standards Series No. SSG-2, Deterministic Safety Analysis for Nuclear Power Plants [11].

Reliability

3.34. Paragraphs 3.35–3.47 provide recommendations on meeting Requirements 17, 21-26, 29-30, and 68 of SSR-2/1 (Rev.1) [1].

3.35. To achieve the necessary reliability of auxiliary systems and supporting systems that support safety functions, the following factors should be considered:

(a) Safety classification and the associated engineering requirements for design and manufacturing;
(b) Design criteria relevant for the systems (e.g. number of redundant trains, seismic qualification, environmental qualification, power supplies);
(c) Prevention of common cause failures by implementation of suitable measures, such as physical separation and functional independence;
(d) Layout provisions to protect the systems against the effects of internal and external hazards;
(e) Periodic testing and inspection;
(f) Maintenance;
(g) Use of equipment designed to be fail-safe.

Systems designed to cope with design basis accidents

3.36. The design should be such that the safety functions of safety category 1 or 2 (as defined in IAEA Safety Standards Series No. SSG-30, Classification of Structures, Systems and Components in Nuclear Power Plants [12]), for which a part of an auxiliary system or supporting system is needed in the event of design basis accidents, can be fulfilled despite the consequential failures caused by the postulated initiating event and any single failure postulated for any safety system or safety group necessary to accomplish the functions. The unavailability of systems owing to maintenance, testing or repair should also be considered.

3.37. The on-site *emergency* power supply should be designed as to have adequate capability to supply power to electrical equipment necessary to fulfil the safety functions in the event of design basis accidents. Auxiliary systems and supporting systems and associated equipment needed in accident conditions should be powered by the emergency power supply or the alternate power source.

3.38. As applicable, vulnerabilities to common cause failures between redundant parts of auxiliary systems and supporting systems that support safety systems should be identified, and design or layout provisions should be implemented to make the redundant parts independent as far as practicable.

3.39. Recommendations relating to the reliability of the systems with regard to the effects of internal hazards, external hazards and environmental conditions are addressed in paras 3.15–3.17, 3.19–3.28 and 3.58–3.65, respectively.

Safety features for design extension conditions without significant fuel degradation

3.40. A reliability analysis of the auxiliary systems and supporting systems that support safety systems designed for given safety functions should be undertaken to identify the need for additional safety features to fulfil these safety functions.

3.41. The more likely combinations of postulated initiating events and common cause failures in redundant safety systems should be analysed. If the consequences exceed the limits for design basis accidents, the vulnerabilities should be removed or additional design features should be implemented to cope with such situations. The additional features for the safety functions that are reactor technology and design dependent should be designed and installed such that they are protected against common cause failures.

3.42. The recommendations in paras 3.36–3.39 should also be applied in respect of design extension conditions without significant fuel degradation, taking into account that meeting single failure criterion is not required and that the relevant additional safety features are expected to be unlikely to fail due to the same common cause failures that lead to the failure of systems designed for design basis accidents.

3.43. Any additional safety features for design extension conditions should be supplied by the alternate power source.

Safety features implemented to mitigate the consequences of design extension conditions with core melting

3.44. The auxiliary systems and supporting systems necessary to mitigate the consequences of an accident with core melting are required to be capable of being supplied by any of the available power sources: see para. 6.44B of SSR-2/1 (Rev.1) [1].

3.45. As far as practicable, independence between safety systems and specific safety features necessary to mitigate the consequences of an accident with core melting should be implemented in the design. In particular, an auxiliary system or a supporting system should not serve both a safety system and a safety feature for a design extension condition with core melting.

3.46. The recommendations in paras 3.36–3.39 should also be applied in respect of design extension conditions with core melting, taking into account that meeting the single failure criterion is not required and that the relevant additional safety features are expected to be unlikely to fail due to the same common cause failures that lead to the failure of systems designed for design basis accidents.

3.47. Recommendations on the reliability of the auxiliary systems and supporting systems with regard to the effects of internal hazards, external hazards and environmental conditions are addressed in paras 3.15–3.17, 3.19–3.28 and 3.58–3.65, respectively.

Defence in depth

3.48. Paragraphs 3.49 and 3.50 provide recommendations on meeting Requirement 7 of SSR-2/1 (Rev.1) [1].

3.49. For a given set of safety functions to be fulfilled, auxiliary systems and supporting systems could participate in the different plant states according to the defence in depth concept.

3.50. The following recommendations contribute to the implementation of independence between levels of defence in depth:

(a) For a given safety function, successive items belonging to different levels of defence, and which are necessary to fulfil that safety function, should be identified.
(b) Vulnerabilities to common cause failures between the items described in (a) should be identified and the consequences assessed. Where the challenge to the safety function leads to unacceptable consequences, the vulnerabilities to common cause failures should be removed to the extent possible. In particular, safety features designed to mitigate the consequences of accidents with core

melting should, as far as practicable, be independent from equipment designed to mitigate the consequences of design basis accidents;

(c) The independence implemented between systems should not be compromised by vulnerabilities to common cause failure in instrumentation and control systems necessary for the actuation or the monitoring of the systems.

Safety classification

3.51. Paragraphs 3.52–3.56 provide recommendations on meeting Requirement 22 of SSR-2/1 (Rev.1) [1]. The recommendations provided in SSG-30 [12] should also be considered.

3.52. The safety class of any part of an auxiliary system or supporting system necessary to support a system designed to fulfil a safety function should be commensurate with the category of the safety function. If part of a supporting system is supporting safety systems or safety features of different safety classes, this part should have a safety class that is commensurate with the system or component having the highest safety class.

3.53. The effect of the failure of a structure, system or component should be considered both in terms of the fulfilment of the safety function, and in terms of the radioactive release. For items for which both of these factors are relevant, the safety class and the associated quality requirements that are necessary to achieve the expected reliability should be defined with due account taken of these two factors. For items that do not contain radioactive material, the safety class and the quality requirements should be directly derived from the consequences assuming the considered safety function is not fulfilled.

3.54. The engineering requirements applicable to a whole system or a set of systems (e.g. requirements relating to independence, or the emergency power supply) that are necessary to perform a safety function should be commensurate with the consequences assuming that the safety function is not fulfilled.

3.55. The safety classification should be established in a consistent manner such that all systems (including the supporting systems) necessary for the fulfilment of one safety function are assigned to the same safety class.

3.56. With regard to implementing the safety classification described in SSG-30 [12]:

(a) Systems necessary to perform or to support a safety function in the event of a design basis accident should be assigned to safety class 1 or safety class 2;

(b) Systems implemented to cope with the loss of safety systems in the event of design extension conditions without significant fuel degradation should be assigned to safety class 2 or safety class 3;

(c) Systems necessary to perform or to support a safety function in the event of design extension conditions with core melting should be assigned to at least safety class 3.

Environmental qualification

3.57. Paragraphs 3.58–3.65 provide recommendations on meeting Requirement 30 of SSR-2/1 (Rev.1) [1]. The recommendations provided in IAEA Safety Standards Series No. SSG-48, Ageing Management and Development of a Programme for Long Term Operation of Nuclear Power Plants [13] should also be considered.

3.58. The structures, systems and components that form part of the auxiliary systems and supporting systems that support a safety function should be qualified to perform their functions in the entire range of environmental conditions that might prevail prior to or during their operation, or should otherwise be adequately protected from those environmental conditions (see Requirement 30 of SSR-2/1 (Rev. 1) [1]).

3.59. The relevant environmental and seismic conditions that could prevail prior to, during and following an accident, and the ageing of structures, systems and components throughout the lifetime of the plant, are all required to be taken into consideration in the environmental qualification: see Requirement 30 of SSR-2/1 (Rev. 1) [1]). Further recommendations are provided in NS-G-1.6 [10] and SSG-48 [13].

3.60. Environmental qualification should be carried out by means of testing, analysis and the use of operating experience or, as necessary, by a combination of these.

3.61. Environmental qualification should include the consideration of such factors as temperature, pressure, humidity and radiation levels, as appropriate, with account taken of local accumulation of radioactive aerosols, vibration, steam impingement, flooding and contact with chemicals. Margins and synergistic effects should also be considered. In cases where synergistic effects are possible, materials should be qualified for the most severe effect, or the most severe combination or sequence of effects.

3.62. Techniques to accelerate the testing for ageing and qualification may be used, provided that there is adequate justification to do this.

3.63. For components subject to the effects of ageing by various mechanisms, the design life and, if necessary, the replacement frequency should be established. In the qualification process of such components, samples should be aged to simulate the end of their design lives before being tested under relevant accident conditions.

3.64. Components that have been used for qualification testing (actual testing on the supplied equipment) should generally not be used subsequently in the construction of the nuclear power plant, unless it can be shown that the conditions and methods of testing do not themselves produce any unacceptable degradation of safety performance.

3.65. Qualification data and results should be documented as part of the design documentation.

Codes and standards

3.66. Paragraphs 3.67–3.69 provide recommendations on meeting Requirement 9 of SSR-2/1 (Rev.1) [1].

3.67. For the design of safety classified structures, systems and components of auxiliary systems and supporting systems, widely accepted or well proven codes and standards should be used. The selected codes and standards should be applicable to the particular design and should form an integrated, comprehensive and consistent set of standards and criteria. If different codes and standards are used for different aspects of the same structure, system or component, the consistency of such codes and standards should be clearly demonstrated.

3.68. For design and construction, the latest editions of codes and standards should preferably be considered. However, another edition might be used with appropriate justification.

3.69. Codes and standards have been developed by various national and international organizations, covering such areas as:

- Mechanical design;
- Structural design;
- Selection of materials;
- Fabrication of equipment and components;
- Inspection of fabricated and erected structures, systems and components;
- Electrical design;
- Design of instrumentation and control systems;
- Environmental and seismic qualification;
- Fire protection;
- Shielding and radiation protection;
- Quality assurance.

Layout considerations

3.70. The layout of auxiliary systems and supporting systems should be such that:

(a) Provision is made for construction, assembly, installation, erection, commissioning, operation, maintenance, decommissioning, and demolition;
(b) Appropriate conditions (e.g. easy access and adequate lighting) for carrying out necessary activities (e.g. inspection and maintenance) are ensured;

(c) The radiation exposure of workers performing tasks on auxiliary systems and supporting systems is kept as low as reasonably achievable;
(d) Adverse interactions with other structures, systems and components in all plant conditions are minimized;
(e) Alternative means to access auxiliary systems and supporting systems that could require local manual operations are provided;
(f) A safe means of escape and of access for rescue workers, including normal and emergency lighting, is ensured.

3.71. Measures to prevent unauthorized access to or interference with auxiliary systems and supporting systems (including unauthorized remote access to computer systems) should be included in the design.

3.72. As a general rule, all auxiliary systems and supporting systems should be designed and located so that, in the event of a fault or accident, sufficient capability to perform the supported safety functions will remain.

Interconnection considerations

3.73. The interconnection of auxiliary systems and supporting systems that provide essential services to each other — or the connection of systems with systems of a lower safety class that could compromise the functionality of the systems of a higher safety class — should be avoided unless it can be proven that the interconnection is beneficial in terms of safety. Where such interconnections are established, provision should be made to enable the isolation of essential services from other services if necessary.

Considerations for a multiple unit nuclear power plant

3.74. The design is required to be such that auxiliary systems and supporting systems that support safety systems or that support safety features for design extension condition are not shared between units of a multiple unit nuclear power plant: see Requirement 33 of SSR-2/1 (Rev. 1) [1].

3.75. As stated in para. 5.63 of SSR-2/1 (Rev. 1) [1]: “To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design.”

Use of probabilistic safety assessment in the design

3.76. Paragraphs 3.77–3.79 provide recommendations on meeting Requirement 10 of SSR-2/1 (Rev.1) [1], in relation to the use of probabilistic safety assessment.

3.77. The use of probabilistic safety assessment should not be considered a substitute to a design approach that is based on deterministic safety assessment, but rather a part of the process to identify safety enhancements and to judge their effectiveness.

3.78. Probabilistic safety assessment should complement deterministic safety assessment, in particular in checking and in adjusting the list of multiple failure conditions involving auxiliary systems and supporting systems, and in identifying additional safety features to achieve a balanced design. In this respect, probabilistic safety assessment should be considered a good tool for assessing the likelihood of the loss of auxiliary systems and supporting systems and assessing the consequences of this loss for the supported system or function. However, the limitations of probabilistic safety assessment should be taken into account.

3.79. As a complement to investigations relating to fabrication, testing and inspection, and to the evaluation of the operating experience, probabilistic safety assessment should be used together with deterministic safety assessment in demonstrating a very low probability of an early radioactive release or a large radioactive release for design extension conditions with core melting. This should include consideration of the reliability of relevant parts of the auxiliary systems and supporting systems that support a safety function (e.g. heating, ventilation and air conditioning systems) and other aspects usually considered in Level 2 probabilistic safety assessment.

4. SPECIFIC CONSIDERATIONS IN DESIGN

4.1. This section provides recommendations for selected examples of auxiliary systems and supporting systems of a common design. It is recognized that for other designs, including for nuclear power plants relying on passive safety features, the configurations of the systems could be different; hence, some of the recommendations might not be appropriate or might need some judgement in their interpretation and adaptation to those systems.

4.2. The selected examples include all those auxiliary systems and supporting systems explicitly identified as such in SSR-2/1 (Rev.1) [1], as well as other auxiliary systems and supporting systems that have been selected owing to their importance for safety. For auxiliary systems and supporting systems not included in this section, the general design considerations described in Section 3 apply.

4.3. For the selected examples, the recommendations are provided in accordance with the following headings:

(a) System and/or equipment functions;
(b) Specific design basis.

4.4. The recommendations provided in this section are aimed at ensuring a high reliability of those auxiliary systems and supporting systems that support safety systems or that support safety features for design extension conditions.

COMMUNICATION SYSTEMS

4.5. Paragraphs 4.6–4.24 provide recommendations on meeting Requirement 37 of SSR-2/1 (Rev.1) [1], which states that:

> "Effective means of communication shall be provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and to be available for use following all postulated initiating events and in accident conditions."

4.6. The means of communication usually include:

(a) An alarm system designed as an acoustic loudspeaker system that can provide site alarms or unit alarms from the main control room or supplementary control room. Different kinds of alarm can be provided: for example, fire alarms, first aid alarms, evacuation alarms and general alarms.
(b) A verbal communication system that facilitates the communication with personnel within the plant. This system typically includes:
    - A wired communication system for direct voice communication between the main control room (or the supplementary control room when the control room is unavailable) and local control stations;
    - A paging system to enable plant-wide paging of personnel;
    - Specific means for alerting personnel in noisy areas (a loudspeaker system).

(c) Telephone communication systems. These systems include:

- The main telephone system used for general communications. The capacity of this system is consistent with the normal operational needs of the plant;
- A secondary telephone system that constitutes a backup telephone system to be used in the event that the main telephone system is not available;
- A wireless system that can be used in normal and emergency conditions.

(d) An off-site communication system that provides communication links with external organizations and facilities, including authorities for emergency preparedness and response.

(e) Video surveillance systems to monitor major components (e.g. reactor coolant pumps, strategic places in the containment) or maintenance activities outside of the main control room.

System and/or equipment function

4.7. An appropriate communication system should be provided for information flow and transfer of instructions between different locations so that persons present at the nuclear power plant and on the site can be given warnings and instructions in normal operation, anticipated operational occurrences and accident conditions. The communication system should also provide appropriate means necessary for the performance of mobile activities.

4.8. Communication facilities should be provided in the main control room to facilitate safe and efficient plant operation. To contact the staff responsible for managing and supervising plant operations within the nuclear power plant or in the immediate vicinity, two independent systems should be provided, as follows:

- A loudspeaker system;
- A dedicated paging system to allow plant-wide paging of personnel.

4.9. The facilities for emergency preparedness and response are required to include diverse communication systems: see para. 5.67 of SSR-2/1 (Rev. 1) [1] and para. 5.43 of IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [14]. These systems should provide for communication between the main control room, the supplementary control room and other emergency response facilities (see para. 6.25 of GSR Part 7 [14]), as well as the off-site response organizations.

Specific design basis

4.10. Communication systems that are essential to the safe operation of the nuclear power plant should be designed and located in order to have the capacity to provide effective communication within the plant (the internal communication system) and effective communication between the plant and off-site organizations (the external communication system) during normal operation, anticipated operational occurrences and accident conditions, and during conditions arising from relevant internal or external hazards.

4.11. The internal communication system and the external communication system should have a backup power source.

4.12. Communication systems that are essential to the safe operation of the plant should have an appropriate safety classification.

4.13. Effective communication should not be impeded by interference from other electronic or electrical equipment. Equally, wireless communication equipment should not produce interference that affects item important to safety (see also para. 4.20).

4.14. The main control room should be designed as the communication centre of the plant for normal operation and during the early stage of an accident.

4.15. The alarm system should be designed to provide:

(a) Site alarms for accident conditions that affect the whole site. These alarms are broadcast to all locations on the site.
(b) Local alarms for accident conditions whose impact is limited to one part of the plant.

4.16. The sound level of the audible alarm system (e.g. sirens) should be higher than the station background noise and should be compatible with the use of personal protective equipment. An illuminated alarm signal should be used in noisy areas, in addition to the audible alarm system.

4.17. The paging system should reach all areas of the plant and should be audible over the whole site, both inside and outside buildings. The design should be such that it is possible to use this system from the main control room and the supplementary control room, with the main control room having a priority over other available control points.

4.18. The main telephone system should have the necessary number of access locations to meet operational requirements. Its capacity should be sufficient to cover the needs of all individuals working at the plant.

4.19. In the event that the main telephone system is not available, a backup telephone system should provide telephone links between all relevant parts of the plant. This secondary telephone system should be independent of the main telephone system.

4.20. A wireless system with the capability to ensure normal and emergency communications with on-site personnel and off-site personnel should be provided. The wireless system should be independent of the main telephone system and the secondary telephone system, and should be tested to determine whether there are locations on the site where a signal cannot be received (‘dead zones’). Areas of the plant in which wireless radio transmission could cause serious electromagnetic interference and have consequences for the plant, for example plant trips, should be clearly marked in the plant as radio exclusion areas.

4.21. An external communication system is required for emergency preparedness and response needs: see para. 4.9. Secure, reliable, permanent, acoustic and two-way voice links should be provided with

off-site authorities: If practicable, these links could be direct 'station to station' telephone links for which no dialling is necessary. This communication system is required to remain operable even during large-scale disruptions, for example of the electricity supply or of the Internet (see para. 5.69 of GSR Part 7 [14]). The number of telephones or other communication devices in each location should be commensurate with the expected demand on the system.

4.22. The internal communication system and the external communication system should be adequate for the coordination of emergency preparedness and response activities, including emergency drills.

4.23. Other communication facilities should be provided, including a video surveillance system to enable monitoring of specific areas that are difficult to access, such as the areas containing the reactor coolant pumps or strategic locations inside the containment.

4.24. Detailed recommendations relevant to the diversity of communication systems are provided in paras 8.39–8.46 of IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [15].

HEAT TRANSPORT SYSTEMS

4.25. Paragraphs 4.26–4.44 provide recommendations on meeting Requirement 70 of SSR-2/1 (Rev.1) [1], in relation to the removal of heat from systems and components that are necessary in operational states and in accident conditions. In particular, paras 4.26–4.44 consider the heat transport systems other than those that are addressed in DS481 [3] and in IAEA Safety Standards Series No. DS487, Design of Fuel Handling and Storage Systems for Nuclear Power Plants [16].

4.26. The following systems are part of heat transport systems considered in this Safety Guide:

(a) Water cooled components such as those cooled by the component cooling water system (e.g. the thermal barrier of the reactor coolant pump, the non-regenerative heat exchanger of the chemical and volume control system, pump motors and bearings). The component cooling water system can be either a recirculating cooling water system or an open loop water system, depending on the design.
(b) The chilled water system used to cool some heating, ventilation and air conditioning systems.
(c) The ventilation systems performing cooling by air renewal or by cooling coils.

The component cooling water system and the chilled water system are considered in paras 4.27–4.44: heating, ventilation and air conditioning systems are considered in paras 4.108–4.170.

General considerations for heat transport systems

System and/or equipment function

4.27. Heat transport systems are required to ensure that systems and components are sufficiently cooled so that they continue to perform their design function(s), and that the systems that they serve are

capable of performing their safety function under all operational states and accident conditions: see Requirement 70 of SSR-2/1 (Rev. 1) [1].

Specific design basis

4.28. The design of a heat transport system should take into account all forms of heat load likely to affect a particular process. Adequate cooling of structures, systems and components by heat transport equipment such as heat exchangers and coolers (e.g. bearings, oil coolers, electrical equipment) should be provided so that their design temperature limit is not exceeded.

4.29. In addition to the heat loads to be considered, the design of the heat transport system should take into account the design temperature limit of the heat sink, based on suitably conservative calculations performed with appropriate allowances for uncertainties.

4.30. When a heat transport system ensures the cooling of equipment necessary for the fulfilment of a safety function:

(a) The heat transport system should have a safety classification commensurate with the safety function and should meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance). In particular, for heat transport pipes located outside buildings, the need to provide trace heating to protect them against extremely cold weather or the provision of other measures to protect against other relevant external hazards should be considered.
(b) The reliability of the cooling chain should be assessed with account taken of common mode failures; if necessary diverse means of heat transport should be implemented in relevant parts of the cooling systems.

4.31. The risk of a leak of the reactor coolant or the cooling medium through the boundary should be considered and the consequences of this leak should be assessed with regard to a possible loss of cooling function, the potential radiological impact and the effects of dilution caused by the mixing of borated water with clear water.

4.32. A heat transport system that supports a safety function should include a means of monitoring coolant levels and/or direct leak detection to facilitate the early detection of loss of coolant. On detection of a loss of coolant, reserve supplies of coolant should be available to provide make-up. Sufficient water volume should be provided to ensure adequate cooling for all situations considered in accident conditions, and adequate provision should be made to replenish the water volume and to ensure long term heat removal. Alternatively, the installation of completely separate safety trains, including a make-up system for each train, is another means of providing appropriate cooling in the short term and in the longer term.

Chilled water system

4.33. Usually, the chilled water system provides chilled water for cooling the heating, ventilation and air conditioning system loads (e.g. cooling of the main control room ventilation, of the electrical building ventilation or of the containment ventilation during power operation) and other process loads. The chillers of the chilled water system are cooled by the component cooling water system or by air.

System and/or equipment function

4.34. The design of the plant should include a chilled water system supplying a sufficient quantity of chilled water in specific areas for ensuring cooling of heating, ventilation and air conditioning systems (e.g. electrical building ventilation and main control room ventilation) and process loads in all plant states.

Specific design basis

4.35. The parts of the chilled water system that supports a system that fulfils a safety function (safety category 1 or 2) in the event of a design basis accident should have an appropriate safety classification and should meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance) and should be designed and fabricated in accordance with acceptable design codes.

4.36. Chilled water system lines that penetrate the containment are required to be provided with appropriate automatic or passive containment isolation features: see Requirement 56 of SSR-2/1 (Rev. 1) [1]. Further recommendations are provided in IAEA Safety Standards Series No. DS482, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants [17]. These parts of the system should be safety classified (based on their safety function of safety category 1) and should meet the corresponding design requirements.

4.37. The performance of the chillers of chilled water system should be based on:

(a) The extreme design temperature of either the water of the component cooling water system or the extreme design site conditions (in the case of air cooling), as appropriate;
(b) The maximum heat loads.

4.38. Some plant designs have heat transport systems for items important to safety that are separate from the heat transport systems for items not important to safety. If separate heat transport systems are not used, the part of the system serving items that are not important for safety should be capable of being isolated by adequately classified means: see para. 6.46 of SSR-2/1 (Rev.1) [1].

4.39. The reliability of heat transport to the ultimate heat sink should be assessed. If this reliability is insufficient, appropriate diversity should be implemented (e.g. cooling of some chillers by air if this cooling is initially performed by the component cooling water system, and vice versa).

4.40. Owing to condensation concerns, all the cold parts of the chilled water system should be insulated after painting except those parts that need to be accessible for maintenance purposes.

4.41. Equipment in contact with outside air should be protected against corrosion (especially in the case of plants located near the sea) and should be protected against freezing.

Component cooling water system (other than for residual heat removal)

System and/or equipment function

4.42. The component cooling water system should perform the following functions:

(a) To remove heat from equipment and transfer it to the ultimate heat sink in operational states and accident conditions;
(b) To protect against a release of radioactive substances into the ultimate heat sink.

Specific design basis

4.43. The heat transfer capacity of the component cooling water system in an accident is addressed in DS481 [3].

4.44. When the component cooling water system cools components containing reactor coolant (e.g. the thermal barrier of reactor coolant pumps):

(a) The component cooling water system should be a closed loop to prevent a leak of primary coolant into the ultimate heat sink;
(b) The chemistry of the component cooling water system should be controlled to prevent corrosion;
(c) A monitoring system should be implemented to detect radioactivity in the component cooling water system;
(d) The component cooling water system should be protected against overpressure caused by leaks occurring in heat exchangers with interfaces with coolant systems operated at higher pressure. In such cases, the component cooling water system should be designed to prevent primary coolant leaks outside the containment by means of isolation of the pressurized portion of the component cooling water system.

PROCESS AND POST-ACCIDENT SAMPLING SYSTEM

4.45. Paragraphs 4.46–4.72 provide recommendations on meeting Requirement 71 of SSR-2/1 (Rev.1) [1].

4.46. The process and post-accident sampling system are required to provide all the samples to be analysed during normal operation or following an accident. Depending on the analysis to be performed, these samples can be distributed to different facilities, including the radiation monitoring process system.

System and/or equipment function

4.47. The process and post-accident sampling system should be capable of providing the liquid and gaseous samples necessary in normal operation for analysing the chemical and radiochemical characteristics of the reactor coolant and associated auxiliary systems and supporting systems (e.g. emergency core cooling system, residual heat removal system, chemical and volume control system, and (for boiling water reactors) the reactor water clean-up system), as well as the containment atmosphere and the secondary system.

4.48. The process and post-accident sampling system should sample all normal process systems and principal components including auxiliary systems and supporting systems necessary for monitoring sample compliance with operational limits and conditions (e.g. sampling of the boron concentration in the accumulators in pressurized water reactors).

4.49. The process and post-accident sampling system should have the capability to provide samples during normal operation that provide information to enable the identification of conditions that could jeopardize the integrity of the reactor coolant pressure boundary.

4.50. The process and post-accident sampling system should ensure that radioactive substances are confined when a sample line is connected to a system containing radioactive fluid. The system should collect, condition and deliver representative samples of fluids (liquids and gases) to one or more sampling stations.

4.51. For the spent fuel pool, the process and post-accident sampling system should have the capability to detect conditions that could result in excessive radiation levels, and should provide information for the control of water chemistry necessary for the integrity of the fuel assembly cladding, the internal structures of the spent fuel pool and the cooling systems of the spent fuel pool.

4.52. The process and post-accident sampling system should be capable of monitoring the concentration of soluble neutron absorbers in operational states and in accident conditions.

Specific design basis

4.53. The process and post-accident sampling system should be designed to provide the samples necessary in normal operation to ensure the fulfilment of design requirements and operational needs. The design should provide monitoring to demonstrate that the correct water and gas characteristics in the reactor coolant and associated auxiliary systems and supporting systems (e.g. the moderator and its auxiliaries for pressurized heavy water reactors), and in the containment atmosphere and secondary system, are being maintained.

4.54. The process and post-accident sampling system should be designed to function in design basis accidents and in design extension conditions for which related sampling or monitoring are necessary (e.g. sampling of gas and water within the reactor containment during severe accidents).

4.55. The selection of sampling points is design dependent. For each type of sample, in accordance with its significance, it should be decided whether continuous analysis using on-line monitors installed on a sampling line is necessary, or whether manually taking intermittent samples for analysis is sufficient.

4.56. Generally, analysis of samples should be performed by a laboratory located within the plant. However, for specific infrequent analyses the use of a laboratory located outside the plant or outside the site could be acceptable. As far as practicable, the design and arrangement of the process and post-accident sampling system should be such that the time span between the sampling and the analysis is minimized; this could be achieved by reducing distances or by arranging for rapid delivery of the samples.

4.57. Provision should be made to ensure that samples from liquid and gaseous process streams and tanks are representative. For example, a sample from within a tank should be taken from the recirculation loop in order to avoid sampling from low points or potential sediment traps. For a process stream sample, sample points should be located in turbulent flow zones. Where necessary, fluid samples should be cooled and reduced in pressure before analysis.

4.58. In normal operation, the process and post-accident sampling system should monitor variables and systems that ensure safety, including variables and systems that can affect the fission process and the integrity of the reactor core and of the reactor coolant pressure boundary. The sampling system should provide information for evaluating whether safety systems and other systems important to safety are protected against abnormal failure and whether conditions are consistent with ensuring these systems perform their intended safety functions.

4.59. The process and post-accident sampling system should, as applicable:

(a) Provide verification that the primary and secondary water chemistry (including key parameters, such as chloride, hydrogen and oxygen concentrations) are within prescribed limits, and provide assurance that corrosion mechanisms will be inhibited and will not adversely affect the reactor coolant pressure boundary;
(b) For pressurized water reactors, allow verification in normal operation that the boron concentration (e.g. in the refuelling water storage tank water and in the accumulator water) is adequate to guarantee core subcriticality in the event of relevant accident conditions;
(c) Provide samples to check that the chemical concentration in the spray chemical additive tank is within limits, so as to ensure, in the containment and in accident conditions, adequate iodine removal as well as material compatibility.

4.60. Discharge samples, purge samples and drain samples should be returned, whenever possible, to the system being sampled or to an appropriate waste treatment system. In the case of sample recycling in the reactor coolant system for pressurized water reactors (or in the moderator for pressurized heavy

water reactors), the material of sampling component should meet the recommendations of DS481 [3] on the materials of reactor coolant system.

4.61. If the sampling lines are equipped with power operated valves, these valves should have a closed fail safe position in order to prevent radioactive releases.

4.62. Provision should be made for limiting radioactive releases in the event of a rupture of the reactor coolant sample line (e.g. passive flow restriction or redundant isolation valves that are qualified and close automatically).

4.63. The safety classification and the seismic resistance of a sampling line up to the second isolation valve should be consistent with the safety classification and seismic resistance of the system that is sampled.

4.64. Parts of the process and post-accident sampling system that are downstream of the isolation valves of the reactor coolant system pressure boundary should be regarded as performing a safety function and should have an appropriate safety classification.

4.65. Sampling lines connected to systems located inside the containment are required to be provided with appropriate features for automatic isolation of the containment: see Requirement 56 of SSR-2/1 (Rev. 1) [1]. Sampling lines from the reactor coolant system are required to have at least two isolation valves: see para. 6.22 of SSR-2/1 (Rev. 1) [1]. These containment isolation features should be safety classified (based on their safety function of safety category 1) and should meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance) and should be designed and fabricated in accordance with acceptable design codes. After an accident, it could be necessary, as applicable, to sample the primary coolant to check the boron concentration, to measure the radioactivity and to determine the composition of fission products. To do this, it should be possible to reopen the primary coolant sampling lines after a certain time when the radiological conditions at the sampling locations allow this (if necessary, subject to the implementation of specific precautions).

4.66. The system should be designed and constructed so that the radiation exposure of plant workers is as low as reasonably achievable.

4.67. Appropriate station layout and design features (e.g. shielding, radiation and radioactivity alarms, ventilation) should be provided to reduce the exposure of personnel who use or work near to the process and post-accident sampling system. In particular, to ensure the protection of operating personnel, pipework carrying highly radioactive fluid should be placed behind radiation shielding. Frequently needed information should be displayed and actuators should be operable outside of the radiation shielding.

4.68. To reduce radiation exposures, the following measures should be adopted in the system design:

- Work areas around process and post-accident sampling system components that require regular maintenance should be shielded from high radiation levels from other systems;
- Sufficient work space should be provided for carrying out maintenance on process and post-accident sampling system components;
- Measures to avoid the sedimentation of radioactive sludge in sampling lines should be implemented (e.g. flushing, limiting the number of low points).

4.69. The design of the process and post-accident sampling system should allow the collection and analysis of highly radioactive samples after an accident. This includes samples from the reactor coolant, the containment sump and the containment atmosphere, for example to provide information on the pH of recirculating water, and the concentration of hydrogen and fission products within the containment atmosphere.

4.70. Samples that are radioactive or potentially radioactive should be segregated from non-radioactive samples. The degree of segregation should take into account the needs of the equipment and floor drainage system, and the arrangements for the treatment of effluents.

4.71. When an analysis is performed outside the containment, highly radioactive samples should be re-injected into the containment if there is a risk of exceeding the capability of the plant to manage the samples as radioactive waste.

4.72. Radioactive liquid samples should be processed in glove boxes made from a material, such as stainless steel, that has a surface that can be easily decontaminated. The glove boxes, which should be specially reinforced, should be kept at negative pressure and connected to permanent iodine traps via the ventilation system, to ensure the protection of the personnel processing the samples. In addition, a means for degassing samples should be provided, if necessary, in order to reduce the level of radioactivity in liquid samples.

PROCESS RADIATION MONITORING SYSTEM

4.73. Paragraphs 4.74–4.93 provide recommendations on meeting Requirement 82 of SSR-2/1 (Rev.1) [1].

System and/or equipment function

4.74. In normal operation, anticipated operational occurrences, design basis accidents and, as far as possible, design extension conditions, the process radiation monitoring system should:

(a) Ensure the radiation monitoring of confinement barriers;
(b) Ensure the monitoring of radioactive releases and provide the information needed for performing a diagnosis of the plant radioactivity;
(c) Where necessary, provide warning of a risk of radiation exposure;

(d) Provide the information needed to implement automatic or manual actions for confinement of radioactive material to limit radiological consequences.

4.75. The process radiation monitoring system should, as applicable:

- Monitor the activity of the steam generator in order to detect an unacceptable steam generator tube leak and to determine the necessity to initiate isolation actions on the affected steam generator, as applicable;
- During the cold shutdown, monitor the activity inside the containment, the fuel building and any building where a fuel handling accident could occur, in order to detect an accident that would necessitate an evacuation alarm and actions for confinement of radioactive material;
- Monitor the activity of gaseous effluents in order to verify compliance with the regulatory limits for radioactive discharges;
- Provide the information needed to ensure the confinement of radioactive material located in controlled areas outside of the containment;

4.76. Sampling points for intermittent monitoring by laboratory analyses should be installed, especially for systems that do not operate in normal operation.

Specific design basis

4.77. The integrity of the primary and secondary confinement barriers should be monitored continuously by measurement of the radioactivity of fluids (e.g. the reactor coolant and containment atmosphere) that are in contact with the barriers in all plant states. For the secondary barrier, monitoring of radioactivity in the atmosphere located near the reactor coolant pipes should be performed continuously.

4.78. The radioactivity of fluids (liquids or gases) that are not normally radioactive, but which could be contaminated by leakages from systems that contain radioactive material (e.g. the thermal barrier of the reactor coolant pump or the heat exchanger of the spray containment system) in the event of a loss of integrity of the confinement barrier, should be monitored.

4.79. The levels of radioactivity in the atmosphere of buildings such as the reactor building, fuel building, nuclear auxiliary building, safety system auxiliary building and the waste treatment building should be monitored continuously.

4.80. To detect a leak from the confinement barrier, liquid from the component cooling system (and, for pressurized water reactors and pressurized heavy water reactors, liquid from the secondary side of the steam generators) should be monitored for radioactivity.

4.81. For some post-accident conditions, such as after a loss of coolant accident or a severe accident, the radiation monitoring system should provide monitoring to enable the assessment of the radiological release into the containment atmosphere. For boiling water reactors this monitoring and assessment should be extended to other areas containing reactor coolant system lines.

4.82. For the protection of operating personnel, continuous monitoring of the atmosphere of the containment and other buildings where radioactive releases could occur should be provided to allow actions to be taken and to trigger an alarm for the evacuation of personnel, in particular, in the event of a fuel handling accident. In addition, surface contamination should be monitored in all areas containing large amount of radioactive liquids and solid radioactive waste.

4.83. The process radiation monitoring system should provide information on any radioactive release that might necessitate actions for the protection of operating personnel and the public.

4.84. As applicable, measurement of radioactivity in the main steam pipes, in the blow-downs of the steam generators and in the condenser should be provided to continuously monitor radioactivity in the secondary side, to provide an alarm for operating personnel and to automatically actuate safety systems, as necessary.

4.85. The process radiation monitoring system should have the capability to monitor radioactivity in gaseous radioactive waste storage tanks in order to detect abnormal levels of radioactivity in the radioactive waste processing facilities.

4.86. To ensure the habitability of the main control room in the event of radioactive contamination of the site, process radiation monitoring system should monitor the main control room air inlet and actuate the iodine and particulate filters of the main control room ventilation (see paras 4.169–4.175).

4.87. Monitoring of radioactivity in air should be provided on the main ventilation ducts from rooms in which contamination might occur, e.g. rooms in the fuel building and in the nuclear auxiliary buildings. In the event of air contamination being detected, the relevant parts of the normal ventilation system should be isolated and high-efficiency particulate air (HEPA) filters and iodine filters should be activated (see paras 4.109–4.170).

4.88. Any tank that might contain radioactive fluid as a result of leaks from the reactor coolant system in accident conditions should be monitored to stop the possibility of discharge to the liquid waste processing system and to assist the plant personnel in deciding on effluent reinjection into the containment.

4.89. A continuous measurement of the activity concentration of radionuclides in liquid releases should be provided on the liquid radioactive waste discharge system when discharges are taking place. If the measurements indicate that authorized discharge limits could be exceeded, automatic isolation of the discharge line should occur and should be accompanied by an alarm.

4.90. All gaseous releases should be discharged through a single ventilation stack. The radioactivity of noble gases within the stack should be monitored over a wide range of activity concentrations and the monitoring system should trigger an alarm if authorized discharge limits could be exceeded. In addition, the levels of radioiodine, tritium and ^{14}C in the releases through the stack should be monitored.

4.91. Continuous measurements of dose rate should be provided for each sump that could collect highly contaminated water. In addition, automatic isolation of the discharge of sumps to the radioactive waste processing system should occur if the dose rate exceeds a pre-set threshold.

4.92. The process radiation monitoring system should be able to provide all the information on the radiological conditions within the plant needed to implement the emergency plan.

4.93. More detailed recommendations on radiation protection aspects in the design of nuclear power plants are provided in NS-G-1.13 [5].

COMPRESSED AIR SYSTEM

4.94. Paragraphs 4.95–4.107 provide recommendations on meeting Requirement 72 of SSR-2/1 (Rev.1) [1]. Usually, the compressed air system provides compressed air to the air service system and to pneumatic instruments and actuators. In paragraphs 4.95-4.107, the emphasis is on a compressed air system that provides compressed air to pneumatic instruments and actuators.

System and/or equipment function

4.95. A compressed air system should provide a continuous supply of compressed air to pneumatic instruments and actuators that support components that perform a safety function in every plant state. The compressed air supplied by this system should be of sufficient quality, cleanness, volume flow and pressure.

Specific design basis

4.96. The part of the compressed air system providing compressed air to actuate or control equipment that performs a safety function during normal operation, anticipated operational occurrences, design basis accidents or design extension conditions or accidents should have a safety classification consistent with this safety function and should meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance).

4.97. If the compressed air system provides air for items important to safety and items not important to safety, the part of the system supplying air to items important to safety should be able to be isolated from the part supplying air to items not important to safety.

4.98. The part of the compressed air system that supplies air to items important to safety should be designed to ensure that it functions during adverse environmental phenomena, in anticipated operational occurrences, including loss of off-site power, and in accident conditions, in particular a loss of coolant accidents or a main steam line break. Where reserve air supply tanks are installed inside the containment, any increased internal pressures caused by high temperatures inside the containment during design basis accidents should be taken into account in the design of these tanks.

4.99. If the operation of a pneumatic actuator is necessary in accident conditions, the autonomy time of the compressed air system (such as by means of having reserve air tanks) should be consistent with the length of time that the safety function needs to be ensured: otherwise, the installation of a backup compressed air system should be considered.

4.100. If the compressed air system's capability for acting autonomously is ensured by means of a compressed air storage tank, the upstream filling pipelines should be equipped with check valves to prevent depressurization through upstream pipelines that are not safety classified and therefore to maintain the air supply to items important to safety. Periodic testing of the leak tightness of these check valves should be performed.

4.101. Where needed to support safety systems or safety features for design extension conditions, the capacity of the compressed air reserves should be sufficient to be consistent with the timescale for the availability of mobile equipment to refill the compressed air tanks.

4.102. The compressed air system should be designed in such a way as to avoid a containment bypass or pressurization of the containment. Systems located inside the containment that are needed in the long term after an accident should not depend on compressed air systems for fulfilling their safety functions. To avoid gradual pressurization of the containment due to the leakage of compressed air systems, consideration should be given to the installation of a dedicated post-accident compressed air system to supply instruments inside the containment with air exhausted from the containment.

4.103. Compressed air lines that penetrate the containment are required to be provided with automatic isolation features: see Requirement 56 of SSR-2/1 (Rev. 1) [1]. These containment isolation features should be safety classified (based on their safety function of safety category 1) and should meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance) and should be designed and fabricated in accordance with acceptable codes.

4.104. The quality of the compressed air is influenced by the quality of the intake air: consequently, suitable air intake positions (e.g. a dust-free environment, away from harmful or hazardous gases) should be selected.

4.105. Adequate compressed air quality (in terms of dew point, solid particle content and size distribution, maximum total oil or hydrocarbon content, humidity and chemical contamination) should be ensured at the supply points in all plant states. Therefore, periodic sampling and analysis of the compressed air should be performed.

4.106. The routing of the pipework of the compressed air system should provide for the draining of condensable gases and vapours. The possibility of liquid plugs should be avoided by utilizing an adequate slope in the routing of the pipework.

4.107. To increase the reliability of the supply of compressed air to instruments, ring topology and air distributors (air headers) should be implemented. If air headers are used, redundant valves should be supplied by different air distribution headers.

HEATING, VENTILATION AND AIR CONDITIONING SYSTEMS

4.108. Paragraphs 4.109–4.170 provide recommendations on meeting Requirement 73 of SSR-2/1 (Rev.1) [1].

General considerations for heating, ventilation and air conditioning systems

4.109. The design requirements for the heating, ventilation and air conditioning system depend on its safety functions. Heating, ventilation and air conditioning systems have two main functions: controlling radioactive releases, and maintaining the ambient conditions (e.g. temperature, humidity and levels of airborne radioactive substances) necessary for items important to safety and for the accessibility and habitability of rooms. Therefore, it is usual to distinguish the following two groups of heating, ventilation and air conditioning system:

(a) The heating, ventilation and air conditioning systems (or parts of these systems) participating in the control of radioactive releases, in particular by filtering the air in specific areas. This group includes the engineered safety feature ventilation system of the controlled area, the fuel building ventilation system, the ventilation system for the radioactive waste effluent treatment building, the containment sweeping ventilation system and, if applicable, the annulus ventilation system.

(b) The heating, ventilation and air conditioning systems maintaining the ambient conditions required for systems and components important to safety and for the habitability of control rooms and on-site emergency response facilities. This group includes the ventilation systems for the electrical building, the diesel generator building, the pumping station and the control room area.

System and/or equipment function

4.110. The design of a nuclear power plant should include heating, ventilation and air conditioning systems that contribute to fulfilling the fundamental safety function of confinement of radioactive material and limitation of accidental radioactive releases.

4.111. The heating, ventilation and air conditioning systems should perform one or more of the following functions, as appropriate:

(a) Maintaining the ambient conditions of rooms in terms of temperature, humidity and airborne radioactive substances;

(b) Monitoring and limiting gaseous radioactive releases during normal operation, anticipated operational occurrences and accident conditions;

(c) Protecting operating personnel and/or equipment from risks coming from inside or outside the buildings (e.g. releases of hazardous substances, extreme weather conditions).

4.112. The ambient conditions of rooms (e.g. in terms of temperature, humidity and airborne radioactive substances) are required to be maintained within acceptable limits for items important to safety: see Requirement 73 of SSR-2/1 (Rev. 1) [1]. In addition, the ambient conditions are required to be compatible with the need for access by personnel: see para. 6.48 of SSR-2/1 (Rev. 1) [1]. To maintain these conditions, the heating, ventilation and air conditioning systems should provide a sufficient minimum rate of air renewal.

4.113. Gaseous radioactive releases during normal operation, anticipated operational occurrences and accident conditions should be monitored and limited, with the following taken into account:

(a) The pressure of rooms located in controlled areas should be maintained below atmospheric pressure in order to prevent the dispersion of radioactive substances into the atmosphere in normal operating conditions (see para. 6.49 of SSR-2/1 (Rev. 1) [1]). This could be achieved by ensuring that the flowrate of intake air is less than flowrate of exhaust air.

(b) An air flow from rooms with a lower contamination risk towards rooms with higher contamination risk should be maintained, as far as practicable, in accident conditions.

(c) The air in contaminated areas (or potentially contaminated areas) should be filtered before it is discharged to the environment in order to ensure that discharges are as low as reasonably achievable, and are kept below authorized limits in normal operating conditions and anticipated operational occurrences and below acceptable limits in accident conditions.

(d) The radioactivity of the exhaust air from the controlled area should be monitored. This air should be discharged to the vent stack.

4.114. The heating, ventilation and air conditioning systems should contribute to protection of personnel and/or equipment against relevant risks arising from postulated internal events (e.g. internal fires and explosions) and from postulated external events (e.g. extreme weather conditions, asphyxiant or toxic gases).

Specific design basis

4.115. Areas in which there is a risk of exposure to radioiodine, in particular in rooms where systems containing radioactive liquid are likely to release significant amounts of radioiodine in accident conditions, should be considered in the design, including the establishment of adequate criteria for the confinement function of these rooms in various accident conditions.

4.116. The ventilation of areas in which there is a risk of exposure to radioiodine should be designed to contribute to the limitation of radioactive releases.

4.117. The design of the heating, ventilation and air conditioning systems that contribute to the limitation of radioactive releases should ensure that these systems control and limit the discharge of radioactive substances in normal operation, anticipated operational occurrences and accident conditions.

4.118. The design of the heating, ventilation and air conditioning systems that contribute to the limitation of radioactive releases should filter the exhausted air using pre-filters, HEPA filters and, if necessary, using iodine filters, before the air is discharged through the stack. The efficiency of the HEPA and iodine filters should be commensurate with the authorized limits on discharges in normal operation and anticipated operational occurrences and with the acceptable limits established for accident conditions.

4.119. For determining the rate of air renewal, the following conditions should be considered:

- Areas where the risk of internal exposure is significant;
- Areas where the risk of internal exposure is negligible;
- Areas where the risk of internal exposure is not negligible but where the risk of radioiodine releases is negligible.

4.120. The design of the heating, ventilation and air conditioning systems that contribute to the limitation of radioactive releases, in particular the release of radioiodine, should ensure that an adequate level of protection is provided and should take into account wind effects.

4.121. The design of the heating, ventilation and air conditioning systems maintaining the ambient conditions (temperature, humidity, acceptable levels of airborne radioactivity level and fresh air) necessary for the operation of items important to safety, and for accessibility and habitability reasons should take into account the basic atmospheric conditions and the extreme atmospheric conditions (e.g. in terms of temperature and humidity, and the duration of these conditions) defined for the design of the nuclear power plant.

4.122. When part of a heating, ventilation and air conditioning system supports a safety system in performing its safety function (safety category 1 or 2) in the event of a design basis accident, it should have an appropriate safety classification and meet the corresponding design requirements, such as the following:

(a) The concept of redundancy should be applied in the design to satisfy the single failure criterion.
(b) The system should be powered by the on-site emergency power supply.
(c) The system should be protected against internal and external hazards. In particular, the redundant trains should be physically separated and the components should be resistant to seismic loads. More particularly, and unless duly justified, ventilation system should be designed to prevent explosive gases, toxic gases and heat from external sources from

entering buildings containing items important to safety, and intake and exhaust ventilation ducts should be protected against external explosion.

(d) The system should be subject to periodic inspection and testing. Detailed recommendations are provided in IAEA Safety Standards Series No. NS-G-2.6, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants [18].

(e) Components should be designed, manufactured, commissioned and tested in accordance with acceptable quality standards.

(f) Components should be designed and manufactured in accordance with acceptable design codes.

4.123. For the interaction of the heating, ventilation system and air conditioning systems with fire protection systems, the recommendations provided in paras 2.19, 4.14, 5.10, 5.13, 5.48, 6.8 and 6.9 of NS-G-1.7 [4] should be considered.

Engineered safety feature ventilation system of the controlled area

System and/or equipment function

4.124. The engineered safety feature ventilation system of the controlled area includes (but is not limited to) the following:

- Emergency core cooling system rooms located outside the containment;
- Residual heat removal system rooms if the system is installed outside the containment;
- Containment spray system rooms located outside the containment.

4.125. The functions of the engineered safety feature ventilation system of the controlled area should be to maintain the necessary ambient conditions for personnel access and for the operation of items important to safety, in normal operation, anticipated operational occurrences and accident conditions.

4.126. The engineered safety feature ventilation system of the controlled area should directly contribute to the confinement of radioactive material to help ensure that the acceptable radiation protection limits for the plant are not exceeded.

Specific design basis

4.127. The engineered safety feature ventilation system of the controlled area both supports a safety function (safety category 2) and directly performs a safety function (safety category 1 or 2); as such, it should have an appropriate safety classification and should meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance) and should be designed and fabricated in accordance with acceptable design codes.

4.128. The engineered safety feature ventilation system should be designed such that the air flow is from areas that are not designated as controlled towards the controlled area.

4.129. The emergency core cooling rooms, the residual heat removal rooms and the containment spray system rooms should be considered areas where the risk of internal exposure from radioiodine is significant during accident conditions.

4.130. If the residual heat removal system is installed outside the containment:

(a) The engineered safety feature ventilation system of the controlled area should be designed taking into account a possible break of a residual heat removal system line outside the containment;

(b) During shutdown states, the residual heat removal system rooms should be maintained at lower pressure than the engineered safety feature rooms of areas that are not designated as controlled.

4.131. The parts of the engineered safety feature ventilation system that are not important to safety should be capable of being automatically isolated in the event of accident conditions.

Fuel building ventilation system

System and/or equipment function

4.132. The functions of the fuel building ventilation system should be to maintain suitable ambient conditions (e.g. temperature, humidity and levels of airborne radioactive substances) for personnel access, if necessary, and for components important to safety in all plant states.

4.133. The fuel building ventilation system should contribute to the confinement of radioactive material to help ensure that the acceptable radiation protection limits for the plant are not exceeded.

Specific design basis

4.134. The fuel building ventilation system should be designed to control the concentration of airborne radioactive material in the spent fuel pool equipment areas to permit personnel access during normal operation, anticipated operational occurrences and after a design basis accident involving fuel handling.

4.135. The controlled area of the fuel building should be considered an area where the risk of internal exposure from radioiodine is significant, unless an analysis demonstrates that some rooms are not affected by such a risk.

4.136. The parts of the fuel building ventilation system necessary to ensure the confinement of radioactive material (safety category 1 or 2) or the operation of safety components (supporting a function of safety category 2) in the event of a design basis accident involving fuel handling should have an appropriate safety classification and meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance).

4.137. The fuel building ventilation system should be designed such that the air flow is from areas of the fuel building that are not designated as controlled (if any) towards the controlled area.

4.138. The fuel building ventilation system should be designed to:

(a) Detect the need for isolating any part of the system devoted to areas that are not designated as controlled (if any);
(b) Have the capability to isolate the part of the system not important to safety when necessary;
(c) Actuate components not used in normal operation that are necessary during accident conditions.

4.139. The fuel building ventilation system should be designed:

(a) To limit radioactive releases to the environment in the event of a fuel handling accident in order to meet the safety objectives for the plant;
(b) To maintain, in normal operation and anticipated operational occurrences, the level of radioactivity in gaseous releases to the environment below the authorized limits and as low as reasonably achievable.

Effluent treatment building ventilation system

System and/or equipment function

4.140. The functions of the ventilation system for the effluent treatment building should be to maintain suitable ambient conditions for personnel access and for the correct operation of equipment during normal operation.

4.141. The ventilation system for the effluent treatment building should ensure the confinement of radioactive material in the effluent treatment building in accident conditions, including conditions caused by the SL-2 design basis earthquake. Depending on the results of the safety analysis, the confinement of radioactive material could be based on static confinement or dynamic confinement.

Specific design basis

4.142. The ventilation system for the effluent treatment building should be designed to control the concentration of airborne radioactive material in the controlled area of the effluent treatment building to enable access by personnel during normal operation.

4.143. The ventilation system for the effluent treatment building should be designed such that in normal operation the level of radioactivity in gaseous releases to the environment is below the authorized limits and is as low as reasonably achievable. The components of the ventilation system for the effluent treatment building that ensure the control of radioactive releases should have an appropriate safety classification (based on their safety function of at least safety category 3).

4.144. The ventilation system for the effluent treatment building should be designed such that the air flow is from areas of the effluent treatment building that are not designated as controlled areas towards the controlled area.

4.145. Design provisions (e.g. means of isolation, intake and exhaust ducts that are resistant to earthquake) should be made if the confinement of radioactive material within the controlled area of the effluent treatment building in the event of the SL-2 design basis earthquake is ensured by static confinement.

Containment ventilation systems

4.146. The containment is usually divided into two separate areas:

(a) The service area, which personnel can access when the reactor is at power;
(b) The area containing the compartments for the main equipment of the reactor coolant system. This area is not accessible by personnel when the reactor is at power.

4.147. Several systems are used to perform the heating, ventilation and air conditioning of the containment. Depending on the design, these systems consist of:

(a) Systems that provide a closed loop ventilation of the containment to maintain the ambient conditions required for the proper operation of instrumentation and equipment and to reduce radioactive discharges by reducing the concentration of aerosols and radioiodine inside the reactor building. These systems ensure the cooling of the reactor cavity.
(b) The containment sweeping ventilation system, which operates during cold shutdown and maintains acceptable ambient conditions for personnel. This system also limits radioactive releases into the environment in the event of a fuel handling accident in the containment. During normal operation, before the entry of personnel inside the containment, the system reduces the level of radioactive gases in the service area atmosphere.

System and/or equipment function

4.148. The containment sweeping ventilation system should ensure the confinement of radioactive material in the event of a fuel handling accident within the containment.

4.149. The containment sweeping ventilation system should be designed to control the concentration of airborne radioactive material and to contribute to the maintenance of ambient conditions in the containment to enable personnel access during cold shutdown states and after a design basis accident involving fuel handling. In particular, the containment sweeping ventilation system should reduce the airborne radioactivity due to noble gases and tritiated water vapor during shutdown states.

Specific design basis

4.150. The part of the containment sweeping ventilation system that ensures the confinement of radioactive material (safety category 1 or 2) should have an appropriate safety classification and meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality

assurance) and be designed and fabricated according acceptable design codes. In particular, this part of the system should have the capability to ensure it performs its safety function in the event of the SL-2 design basis earthquake.

4.151. The containment sweeping ventilation system should limit radioactive releases to the environment in order to meet the safety objectives in the event of a fuel handling accident within the containment. The scenarios to be considered with respect to the design of this system should include an outage with an open containment.

4.152. The design of the containment sweeping ventilation system should take into account that, during the transfer of spent fuel in the fuel storage pool, damaged fuel cladding could cause releases of radioactive gases and aerosols in some area of the containment. In addition, the containment sweeping ventilation system should be designed:

(a) To ensure that, in normal cold shutdown states, the level of radioactivity in gaseous releases to the environment is below the authorized limits and is as low as reasonably achievable;
(b) To contribute to the isolation of the containment (safety category 1). Isolating devices should have an appropriate safety classification based on a high level of radioactivity within the containment in accident conditions;
(c) To protect the containment against excessive negative pressure;
(d) To improve the efficiency of the hydrogen control system in the containment.

Specific considerations for heating, ventilation and air conditioning systems maintaining ambient conditions

Ventilation systems of areas not designated as controlled areas containing equipment important to safety

4.153. This section concerns ventilations systems whose only function is to maintain the necessary environmental conditions for systems and components that are important to safety, and for personnel access. Depending on the layout, these systems could include the ventilation system for the electrical building, the diesel generator building, the pumping station and the part of the safety auxiliary building usually containing the emergency feed water system and component cooling system.

System and/or equipment function

4.154. The design of the ventilation systems for areas not designated as controlled areas should be such that the ambient conditions of rooms in terms of temperature, humidity and cleanness of the air, are maintained within acceptable limits for components important to safety and for personnel access.

Specific design basis

4.155. Any parts of the ventilation systems for areas not designated as controlled areas that are necessary for a system to fulfil a safety function (safety category 1 or 2) in the event of a design basis

accident should have an appropriate safety classification and meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance) and should be designed and fabricated according acceptable design codes.

4.156. The operation of heating, ventilation and air conditioning systems in essential areas of the electrical building in the event of a station blackout should be ensured.

4.157. The risk of hydrogen explosion should be taken into account in the design of the ventilation systems for electrical rooms containing batteries.

4.158. In electrical rooms, the air introduced by the ventilation should be of sufficient quality to protect against damage to electrical contacts from dust, dirt, sand grit and humidity.

4.159. More detailed recommendations are provided in IAEA Safety Standards Series No. SSG-34, Design of Electrical Power Systems for Nuclear Power Plants [20].

Ventilation systems for the main control room, supplementary control room and on-site emergency response facilities

System and/or equipment function

4.160. The functions of the ventilation system for the main control room are to maintain the operation of safety components and to keep the main control room habitable in all plant states. This includes during the presence of smoke, explosions, toxic gases and/or radioactive contamination in the external environment. These functions are ensured by maintaining ambient conditions (temperature, humidity, clean and fresh air) and concentrations of airborne radioactive substances at levels compatible with the habitability of the main control room and with the operation of the components.

Specific design basis

4.161. The ventilation system for the main control room should be designed to ensure the operation of safety components (safety category 2) and should have an appropriate safety classification and meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance) and should be designed and fabricated according acceptable design codes.

4.162. The ventilation system for the main control room should be designed to automatically maintain the main control room at a pressure higher than the atmospheric pressure during operational states and accident conditions to avoid the ingress of radioactive substances in the event of radioactive contamination of the site.

4.163. The ventilation system for the main control room should be designed to clean the air supplied to the main control room using appropriate iodine filters and particulate filters in the event of radioactive contamination of the site.

4.164. The design of the ventilation system for the main control room should enable the isolation of the main control room in order to avoid the ingress of any substance that could be harmful to personnel or to the operation of equipment.

4.165. The ventilation system for the main control room or an associated system should be capable of removing smoke in the event of fire within the control room.

4.166. The ventilation system for the supplementary control room should not be a common system shared with the main control room. The recommendations provided in paras 4.161–4.165 for the ventilation system for the main control room also apply to the ventilation system for the supplementary control room.

4.167. The ventilation system for on-site emergency response facilities should not be a common system shared with either the main control room or with the supplementary control room. The design of this ventilation system should be such that the habitability of the on-site emergency response facilities is ensured, with a reasonable level of confidence, under a wide range of hazardous conditions, including extreme conditions not considered in the nuclear power plant design.

Heating, ventilation and air conditioning systems for turbine buildings in boiling water reactors

4.168. In a boiling water reactor, the heating, ventilation and air conditioning systems for the turbine building should ensure — during normal operation, anticipated operational occurrences and after a design basis accident — that ambient conditions in terms of temperature, humidity and levels of airborne radioactive substances are within the acceptable limits for structures, systems and components and are compatible with the presence of personnel.

4.169. The exhaust air from the turbine building in a boiling water reactor should be discharged to the plant main stack. The gaseous radioactive releases should be monitored and kept below authorized limits.

4.170. The heating, ventilation and air conditioning systems for the turbine building should be designed such that the air flow is from rooms with lower contamination levels towards rooms with higher contamination levels.

LIGHTING AND EMERGENCY LIGHTING SYSTEMS

4.171. Paragraphs 4.173–4.179 provide recommendations on meeting Requirement 75 of SSR-2/1 (Rev.1) [1].

4.172. Lighting systems are usually composed of:

(a) A normal lighting system that provides the lighting needed to perform tasks during normal operation;
(b) An emergency lighting system that provides lighting during fire, anticipated operational occurrences (including events such as loss of off-site power) and design basis accidents;
(c) A station blackout lighting system that provides lighting in the event of the total loss of the external power supply and the internal power supply;
(d) A lighting system that provides lighting for emergency exits for facilitating personnel evacuation.

System and/or equipment function

4.173. The lighting systems and their power sources should be capable of providing sufficient illumination to enable plant personnel to access areas and to perform all necessary manual operations (e.g. maintenance actions, or actions in emergency operating procedures) in all plant states as well as to exit safely from areas in case of evacuation.

Specific design basis

4.174. The emergency lighting system should be immediately available in the event of failure of the normal lighting system, or in the event of the loss of off-site power until the emergency power supply is available.

4.175. Emergency lighting should be provided in (but not limited to) areas where items important to safety are located, as well as in the access and rescue routes to these areas. In particular, this includes the following areas:

- Main control room;
- Supplementary control room;
- Site emergency response facilities;
- Emergency generator area;
- Area containing emergency switchgear, motor control centers, DC batteries and AC–DC inverters;
- Plant areas in which manual actions identified in emergency operating procedures are necessary.

4.176. Emergency lighting in the main control room should be independent of any other lighting system available in the main control room. The average lighting level in the main control room should be adjusted, taking into account the design of indicators and screens, in order to reduce reflection and dazzle and other effects associated with inadequate lighting. In addition, the main control room should be provided with several lighting areas, which can be manually adjusted to provide illumination suitable for plant personnel to perform their tasks.

4.177. In case of a station blackout, a sufficient level of illumination should be provided, as a minimum in the main control room, the supplementary control room, the emergency response facilities, and in locations where operator actions are necessary.

4.178. The station blackout lighting system should be supplied by DC batteries of sufficient capacity to provide a run time that is consistent with the recovery time of the internal or external power supply.

4.179. The lighting system for the emergency exits should provide a minimum level of lighting necessary to enable staff to safely exit rooms and buildings. This lighting system should be supplied by DC batteries having a sufficient capacity to provide a run time that enables the evacuation of personnel in all conditions including fire.

OVERHEAD LIFTING EQUIPMENT

4.180. Paragraphs 4.182–4.198 provide recommendations on meeting Requirement 76 of SSR-2/1 (Rev.1) [1].

4.181. The overhead lifting equipment consists of all components and equipment for moving all heavy loads (i.e. with a mass greater than that of one fuel assembly and its handling device) in the nuclear power plant. The containment structure crane and the fuel building crane are part of the overhead heavy load handling system. The refuelling machines are not considered in this Safety Guide.

System and/or equipment function

4.182. An overhead lifting equipment should provide a means to move and relocate heavy equipment within the power plant.

4.183. Loads to be handled by overhead lifting equipment include the following:

- The drywell head (boiling water reactors);
- The reactor vessel internals;
- The reactor vessel head;
- The reactor coolant pump motor.

Specific design basis

4.184. The design of an overhead lifting equipment is required to include conservative measures to prevent any unintentional dropping of loads that could affect items important to safety (para. 6.55(b) of SSR-2/1 (Rev.1) [1]). Such measures include restricting the movement of the overhead lifting equipment (by design or by interlocks) to areas away from stored fuel and away from equipment that contributes to the fulfilment of a safety function. Alternatively, a load drop evaluation should confirm the absence of unacceptable consequences.

4.185. Safe load paths should be defined for the movement of heavy loads to minimize the potential for a load drop on irradiated fuel in the reactor vessel or the spent fuel pool or on equipment necessary for achieving or maintaining a safe shutdown of the reactor.

4.186. Structural steelwork and mechanisms and components (e.g. chains, cables, wire ropes, slings) of lifting equipment should be designed with an adequate safety margin in relation to the yield strength under the nominal load.

4.187. Overhead lifting cranes should be designed to continue to hold and retain control of their maximum loads in the event of the SL-2 design basis earthquake.

4.188. The use of overhead lifting equipment should be prevented under conditions that could result in unplanned radioactive releases in the event of an accident (see also para. 6.55 (d) of SSR-2/1 (Rev. 1) [1]). For example, an interlock on the crane of the spent fuel cask transfer can prevent the crane from being used when the fuel building door is open.

4.189. The design of overhead lifting equipment should be such that the load can be lowered by manual operation in the event of loss of power, loss of motive torque or mechanical failure (see also para. 6.55 (d) of SSR-2/1 (Rev. 1) [1]).

4.190. Overhead lifting equipment, including transfer and lifting devices, should be designed to prevent impact damage to fuel or items important to safety in the event of loss of electrical power or the occurrence of the SL-2 design basis earthquake.

4.191. To prevent the lifting of excessive loads, all overhead lifting equipment should be equipped with a load weighing device that has a display that is always visible to the operator of the equipment. This weighing device should include an overload protection system.

4.192. In the event of loss of power, all electromechanical components of the overhead lifting equipment should automatically be placed in a fail-safe position. When the power supply is restored, the equipment should be maintained in a locked position until operator intervention.

4.193. Overhead lifting equipment should be equipped with an emergency stop button (i.e. that stops all motion of the equipment), in addition to a height upper limit switch and the normal means of stopping the movement of the equipment.

4.194. Overhead lifting equipment that could impair an item important to safety should be equipped with a securing mechanism that could be implemented either by a safety brake acting on the drum or by a redundant hoisting mechanism. This securing mechanism should be actuated by a redundant over-speed detection or by a redundant detection of the failed hoisting mechanism. The detection device should be completely independent of operator commands and controls.

4.195. Overhead lifting equipment inside the containment (especially the girder and crane track) should be designed taking into account the complementary loads resulting from the ambient conditions that could be created within the containment by a loss of coolant accident.

4.196. Prior to commissioning, handling equipment should be tested to at least its maximum expected load. Periodic inspections and tests during normal operation should be carried out to ensure and verify the operation of safety devices, including the upper limit switch, over-speed interlock, overload interlock and restricted areas interlock.

4.197. Design provisions should be implemented in such a way that cranes that might become contaminated have strippable or smooth surface paint or coatings that facilitate the decontamination of potentially contaminated surfaces.

4.198. The overhead heavy load handling systems that are credited in the preliminary decommissioning plan should have a design life and specific design provisions that are commensurate with the expected decommissioning activities.

SYSTEMS FOR TREATMENT AND CONTROL OF RADIOACTIVE WASTE AND RADIOACTIVE EFFLUENTS

4.199. Paragraphs 4.200–4.232 provide recommendations on meeting Requirements 78 and 79 of SSR-2/1 (Rev.1) [1].

General considerations

4.200. The design of the nuclear power plant is required to incorporate features that facilitate the safe handling, storage, treatment, movement and transport of radioactive waste, and the control of effluent discharges: see Requirements 78 of SSR-2/1 (Rev.1) [1]. Provision for the storage of waste in transit and for the removal of waste should also be considered in the design.

4.201. The design is required to include provision for the safe treatment and control of liquid and gaseous radioactive effluents that are discharged from the facility: see Requirements 79 of SSR-2/1 (Rev.1) [1].

4.202. The design should be such as to minimize the generation of radioactive waste in all operational stages in the lifetime of the nuclear power plant, including decommissioning (see also Requirement 12 of SSR-2/1 (Rev. 1) [1].

4.203. The treatment and control of radioactive waste and radioactive effluents includes the collection, processing, and disposal or discharge of radioactive waste produced by let-down, drainage, purge, venting, or leakage in the systems during normal operation as well as other radioactive waste from operation.

4.204. Design measures to facilitate radioactive waste management (see Requirement 12 of SSR-2/1 (Rev. 1) [1]) include the following:

(a) The materials for components in contact with radioactive substances, in particular those in contact with the reactor coolant, are required to be chosen so that amount of radioactive waste will be minimized to the extent practicable and decontamination will be facilitated: see para. 4.20 (a) of SSR-2/1 (Rev. 1) [1].

(b) The chemistry of the reactor coolant and other systems should be designed to minimize the production of corrosion products (e.g. through control of the hydrogen concentration, the possibility of zinc injection and by pH control).

(c) Provision should be made to minimize the deposition of corrosion products that are, or that can be, activated when passing through the reactor core. In particular, the deposition of such corrosion products on the fuel assemblies and on the structures around the reactor core should be minimized;

(d) A clear distinction should be made between conventional waste areas (i.e. in which the waste is not contaminated) and nuclear waste areas (i.e. in which the waste is likely to be contaminated). Provision should be made to minimize the nuclear waste areas.

(e) Adequate provision should be made at the design stage to facilitate future dismantling operations. This should include the installation of large components in such a way that they can be removed and transported for subsequent management, the provision of handling devices for dismantling operations, radiation shielding to facilitate safe dismantling, as well as provision for in situ decontamination.

4.205. The following measures for restricting radiation exposures (see Requirements 5 and 18 of SSR-2/1 (Rev. 1) [1]) from the radioactive waste generated during nuclear power plant operation should be included in the design:

(a) Measures to reduce the quantity and concentration of the radioactive waste generated and transported within the nuclear power plant or released to the environment;

(b) Measures for the isolation of radioactive waste from workers and from the public. Provision is also required to be made for zoning the nuclear power plant based on the potential for radioactive contamination and radiation exposure: see para. 6.73 of SSR-2/1 (Rev. 1) [1].

(c) Provisions for the detection, collection and treatment of liquid spills before they are discharged as effluents.

(d) Facilities for the decontamination of personnel and equipment are required to be provided: see para. 6.76 of SSR-2/1 (Rev. 1) [1]. Provision should also be made for handling the radioactive waste arising from decontamination activities.

4.206. The systems for the treatment and control of radioactive waste and radioactive effluents should be such that these systems are protected, commensurate with the nature and extent of the risk, against internal and external hazards, in particular extreme weather conditions and flooding. For example, in a pressurized water reactor, the circuits carrying concentrated boron acid should be located in heated rooms or should be provided with trace heating in order to prevent boron crystallization.

4.207. The design of the systems for the treatment and control of radioactive waste and radioactive effluents should include measures that allow appropriate periodic inspection and testing of components important to safety, with suitable shielding for radiation protection purposes, and with appropriate containment and filtering systems.

4.208. Structures, systems and components that ensure the confinement of radioactive waste and radioactive effluents should be designed to withstand the SL-2 design basis earthquake.

System for treatment of gaseous effluents

System and/or equipment function

4.209. The design of the system for the treatment of gaseous radioactive effluents should address the following:

- Treatment and monitoring of gaseous effluents such that a minimum retention time is achieved to allow radioactive decay before routing to a common release point;
- Measurement of the volume and radioactivity of effluents to be released;
- Means for isolation of the discharge route if the release limits are likely to be exceeded.

4.210. The provisions in para. 4.209 could be achieved by collecting the gaseous effluents in a buffer tank and then routing them under pressure to decay devices, or by online release via a delay line (e.g. charcoal delay beds) and then via the ventilation system of the auxiliary building before release to the discharge point (e.g. stack).

4.211. Provision for measures such as stacks for the discharge of gaseous low level radioactive waste, and means for sampling and monitoring of these discharges should be made at the design stage.

Specific design basis

4.212. The design of the system for the storage of gaseous effluent should be such that the number and the capacity of the storage tanks for gaseous effluents is sufficient to allow the decay of short lived gases to levels that are below the authorized limits for discharges before release to the environment.

4.213. The design of the system for the storage of gaseous effluent should be such that the rupture of any of the gaseous effluent tanks has no (or only minor) radiological consequences, either on the site or off the site, and does not necessitate any off-site protective actions.

4.214. The design should include the following:

(a) Prevention of an explosion risk, for example in rooms for storage tanks containing hydrogenated gaseous effluent. For example, hydrogen ignition in the purge gas return system could be prevented by maintaining a continuous flow of nitrogen purge through connected components and by recombination.

(b) Protection of the system for the treatment of gaseous effluent against pipe rupture. This could be achieved by following relevant recommendations provided in NS-G-1.11[8].

4.215. The design of the system for the treatment of gaseous effluent should incorporate measures to limit the release of radioactive gases. This should be achieved with equipment and structures of high reliability as well as by detection of radioactivity and by confinement.

4.216. As stated in para. 6.63 of SSR-2/1 (Rev. 1) [1] in relation to the cleanup equipment for gaseous radioactive effluents:

> "Filter systems shall be designed so their efficiency can be tested, their performance and function can be regularly monitored over their service life, and filter cartridges can be replaced while maintaining the throughput of air."

4.217. Gaseous effluent treatment lines that penetrate the containment are required to be provided with automatic isolation features see Requirement 56 of SSR-2/1 (Rev. 1) [1]. These containment isolation features should be safety classified (based on their safety function of safety category 1) and meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance).

System for treatment of liquid effluents

System and/or equipment function

4.218. The system for treatment of liquid effluents includes the reactor coolant treatment system and boron recycling system, the liquid waste processing system and the liquid radioactive waste monitoring and discharge system.

Reactor coolant treatment and boron recycling system

4.219. The design of the systems for reactor coolant treatment and boron recycling should include the following:

(a) Processing of the discharged reactor coolant via systems providing a bleed function (i.e. the chemical and volume control system for pressurized water reactor designs, or the reactor water cleanup system for boiling water reactor designs);

(b) Treatments such as degassing to remove noble gases and hydrogen, purification, and separation of boron and water to allow the recycling of boric acid and water make-up;

(c) Monitoring of the resulting products, and subsequent routing, as appropriate, to the reactor boron and water make-up system for recycling or to the liquid waste treatment systems, the liquid waste discharge systems or the solid waste treatment systems.

System for treatment of liquid radioactive waste

4.220. The system for treatment of liquid radioactive waste can be shared by different units of the power plant. The design of the system should provide storage, adequate treatment and monitoring of the

different kinds of non-reusable spent liquid effluent collected by the equipment and floor drainage system (see paras 4.269–4.285), before transfer to the discharge system.

4.221. The design of the system for treatment of liquid effluent should include the following measures:

(a) Selective front-end storage of all potentially contaminated liquid effluents based on the chemical composition and levels of radioactivity of the various waste streams;
(b) Analysis of the contents of each storage tank and subsequent adequate treatment so that the treated waste is of acceptable quality for re-use within the plant, or meets the conditions for discharge to the environment;
(c) Corresponding transfers to the storage facility of the discharge system for monitoring;
(d) Transfer of any solid waste that is produced (e.g. concentrates, spent ion-exchange resins, spent filters) to the solid waste treatment system.

Systems for monitoring and discharge of liquid radioactive waste

4.222. The system for monitoring and discharge of liquid radioactive waste collects liquid radioactive effluent from each unit and from other site facilities, monitors and records the levels of radioactivity and the chemical and physical composition, and discharges the effluent in a controlled fashion to the environment. The flow rate of the discharge to the environment should be determined by the level of radioactivity of the effluent and the dilution capacity of the environment, so as to meet the authorized limits on discharges.

4.223. The following provisions for the system for monitoring and discharge of liquid radioactive waste should be considered at the design stage:

(a) Measurement of the volumes of liquid effluents to be released;
(b) Determination or adjustment of release rates to ensure compliance with the discharge authorization;
(c) Automatic isolation of the discharge line if authorized limits on discharges are likely to be exceeded.

Specific design basis

4.224. The design of the system for treatment of liquid effluent should be such it has the capacity to monitor, control, collect, process, handle, store and dispose of liquid radioactive waste, and keep liquid releases to the environment as low as reasonable achievable and below the authorized limits on discharges.

4.225. The system for treatment of liquid effluent should not be installed in the same location as systems containing non-radioactive liquids so to avoid any increase in the volume of effluents to be treated due to leaks of non-radioactive liquids. Alternatively, design provisions should be implemented to avoid such leaks or to collect them separately from the radioactive effluents.

4.226. All tanks containing radioactive liquid effluents should have a level control with a high level alarm — reported locally and in the control room — allowing action to be taken to avoid tank overflow.

4.227. To avoid contamination of groundwater, the circuits and equipment containing radioactive liquids should be installed in rooms that have sufficient capacity to hold and retain any liquid leaks or should have other means implemented for the retention of such liquids.

4.228. The design of the system for treatment of liquid effluent should be such that the rupture of any of the liquid effluent tanks has no (or only minor) radiological consequences on the site or off the site, and does not necessitate any off-site protective actions.

System for treatment of solid waste

System and/or equipment function

4.229. The design of the system for treatment of solid waste should address the following:

(a) Collection, storage and processing of solid waste, including sorting, volume reduction (e.g. shredding and use of compactors or incinerators), immobilization of compacted waste or ashes in packages, packaging of low level waste, encapsulation and packaging (e.g. in drums) of solid waste (e.g. spent resins and filters);
(b) Temporary or long-term storage of packaged solid waste on site before shipment to authorized radioactive waste disposal facilities; the minimum on-site storage capacity should be specified.;
(c) Monitoring and removal of surface contamination from the external surfaces of waste packages;
(d) Measurements to determine the inventory of waste packages (e.g. in terms of radioactivity and mass);
(e) Package marking;
(f) Data recording.

Specific design basis

4.230. The design of the system for treatment of solid waste should include means to handle solid wastes produced during normal operation, and to control the release of radioactive liquid effluents arising from the treatment of solid waste.

4.231. The system for treatment of solid waste should be designed to detect conditions that might lead to excessive radiation levels and to provide adequate protection and safety under anticipated operational occurrences and accident conditions.

4.232. Further recommendations are provided in NS-G-1.13 [5]; in addition, the recommendations in NS-G-4.6 [19] for research reactors can also be adapted.

SUPPORTING SYSTEMS FOR THE EMERGENCY POWER SUPPLY AND THE ALTERNATE POWER SOURCE

4.233. Paragraphs 4.234–4.267 provide recommendations on meeting Requirement 68 (in particular, para. 6.45) of SSR-2/1 (Rev.1) [1].

Supporting systems for the emergency power supply

4.234. Requirement 68 of SSR-2/1 (Rev.1) [1] states that:

> "The design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power supply in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power."

4.235. Paragraph 6.45 of SSR-2/1 (Rev.1) [1] states that:

> "The design basis for any diesel engine or other prime mover that provides an emergency power supply to items important to safety shall include:
>
> (a) The capability of the associated fuel oil storage and supply systems to satisfy the demand within the specified time period;
> (b) The capability of the prime mover to start and to function successfully under all specified conditions and at the required time;
> (c) Auxiliary systems of the prime mover, such as coolant systems."

General considerations for supporting systems for the emergency power supply

4.236. Each emergency power source should be provided with its own completely independent supporting systems. These systems include the following:

- Systems for oil storage and oil transfer;
- Lubricating oil system;
- Cooling water system, which is normally integrated into the emergency power source, or can be external to the power source;
- Air starting system or DC motor starting;
- Systems for combustion air intake and exhaust.

System and/or equipment function

4.237. Each emergency power source should be provided with dedicated systems needed for its operation. These systems include those for the fuel oil storage and oil transfer, lubricating oil, cooling water, combustion air intake and engine exhaust air starting, as well as electrical systems. In addition, the emergency power supply should be protected against fire.

Specific design basis

4.238. The essential auxiliary systems and supporting systems necessary for the operation of the emergency power supply should be considered as supporting a system that fulfils a safety function of safety category 1. These auxiliary systems and supporting systems should have the same safety classification as the emergency power supply and should meet the corresponding design requirements, as follows:

(a) The concept of redundancy should be applied in the design to satisfy the single failure criterion applied to the system.
(b) The systems should be powered by the emergency power supply.
(c) The systems should be protected against internal and external hazards. In particular, the redundant trains should be adequately separated and the essential auxiliary systems and supporting systems should remain functional after the SL-2 design basis earthquake and be protected against storms and flooding.
(d) The systems should be subject to periodic inspection and testing;
(e) Components should be designed and fabricated, erected and tested in accordance with acceptable quality standards.
(f) Components should be designed and fabricated in accordance with acceptable design codes.

4.239. The auxiliary systems and supporting systems necessary for the operation of the emergency power supply should be housed within buildings in seismic category 1 (see para. 2.14 of NS-G-1.6 [10]).

Fuel oil storage and transfer system

4.240. Usually, each emergency diesel generator is fitted with a short term fuel oil tank (also called a ‘daily tank’) fed from a main fuel oil storage tank. In contrast, each combustion turbine is fed directly from the fuel oil storage system through fuel oil transfer pumps or forwarding pumps. The short term fuel oil tank of each emergency diesel generator should be of sufficient size to enable operation at full load for a length of time compatible with that needed for operator intervention to restore the oil level.

4.241. The main fuel oil storage tank should independently provide fuel oil to operate the emergency power supply at full load for the necessary period of time in design basis accidents. In addition, design should be such that the main storage tank can be refilled for ensuring long term operation.

System and/or equipment function

4.242. Each emergency power source should be fitted with an independent and reliable fuel oil storage and transfer system to ensure the supply of fuel oil needed for its operation in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power.

4.243. Each oil storage tank should have the capability to be refilled during design basis accidents for ensuring the long term operation of the emergency power supply. The availability of adequate and

acceptable off-site sources of fuel oil, as well as the means for transporting and refilling the fuel oil storage tanks, should also be considered.

4.244. The quantity of oil stored within the site should be sufficient to ensure the operation of all emergency power sources at the nuclear power plant in the event of a loss of off-site power due to an earthquake (i.e. as a result of which the off-site power might not be restored for a long time). The quantity of fuel oil stored should be based on the time necessary to restore off-site power or the time necessary to resupply fuel oil.

Specific design basis

4.245. The quality of the fuel oil should be verified periodically in order to ensure that the oil satisfies minimum operating requirements.

4.246. The system for fuel oil storage and transfer should be protected against the relevant hazards for the site such as earthquake and extreme weather conditions.

4.247. Each fuel oil storage tank should be equipped with a fill and vent line located outside. These components should be protected to minimize the possibility of damage from vehicles or external hazards. In addition, the fill and vent point should be located higher than the probable maximum flood level.

4.248. Measures should be taken to minimize fires and explosions caused by the system for fuel oil storage and transfer. In particular, the design should include the following measures:

(a) The capability to detect and control leakage of fuel oil from the system, including the capability to isolate parts of the system in the event of excessive leakage;
(b) Tank dykes to contain the fuel oil in the event of a tank breach;
(c) Locating oil tanks at a sufficient distance away from the main control room to preclude any danger to control room personnel or equipment resulting from an oil tank explosion and/or fire.

4.249. The design of emergency diesel generators should include an overflow line on the short term fuel oil tank to return excess fuel oil delivered by the transfer pump back to the fuel oil storage tank.

4.250. The short term fuel oil tank of an emergency diesel generator should be located at an elevation that provides sufficient positive pressure at the engine-driven fuel oil pump(s). If a booster pump is necessary, it should be powered from a reliable power source, it should start as soon as the engine receives a start signal, and should operate until system fuel oil pressure is established by the engine-driven fuel oil pump.

4.251. If a double-walled storage tank (e.g. an underground tank) is used, the annulus between the two walls should be equipped with a leak detection system.

Cooling water system

4.252. Each emergency power source should be supplied with a cooling system. In general, this cooling is performed by a closed loop mounted integrally with the emergency power source. Included in each cooling system are a jacket water heater and pump to keep the engine warm, a 3-way temperature regulating valve and a lubricating oil cooler.

System and/or equipment function

4.253. Each emergency power source should be equipped with a cooling water system that transfers heat to an ultimate heat sink, in order to maintain the temperature of the emergency power source within the limits specified by the manufacturer.

4.254. The cooling water system should be provided with heaters and circulating pumps, which keep the engine warm under standby conditions, enabling the emergency power source to be started without causing mechanical damage.

Specific design basis

4.255. The design should include measures to inhibit long term corrosion and organic fouling that would degrade the performance of the cooling system. Precautions should be taken to ensure the compatibility of any corrosion inhibitors or antifreeze compounds with component materials.

4.256. When the emergency power source receives a start signal, the cooling water system should automatically provide the required cooling (switching from standby conditions to the required cooling conditions).

Lubrication system

4.257. The lubrication system of an emergency power source consists of an oil sump in its frame, an oil cooler, as well as an oil strainer and a filter.

System and/or equipment function

4.258. Each emergency power source should be equipped with a lubrication system that contains the following:

(a) An oil filtering system to maintain required oil quality during engine operation;
(b) An oil cooling system to maintain the oil temperature within limits specified by the manufacturer;
(c) A system that keeps the lubricating oil passages warmed and filled when the emergency power source is in the standby mode.

Specific design basis

4.259. The lubrication system should be fitted with measures (e.g. relief ports) to prevent explosions and to mitigate the consequences of such events (see NS-G-1.7 [4]).

4.260. The oil capacity of the lubrication system should be sufficient to ensure the operation of the emergency power supply in the event of a loss of off-site power due to an earthquake. In addition, the capacity of lubricating oil storage at the site should be sufficient to ensure long term operation until recovery of the supply of lubricating oil to the site.

Supporting systems for the alternate power source

System and/or equipment function

4.261. Each alternate power source should be provided with dedicated auxiliary systems and supporting systems necessary for the operation of the power source in the event of the loss of off-site power and the emergency power supply. These systems include those for fuel oil storage and oil transfer, lubricating oil, cooling water, combustion air intake and engine exhaust, air starting, as well as electrical systems. In particular, the air starting system should be designed in such a way that several starts are possible without refilling the compressed air tanks.

Specific design basis

4.262. Common cause failures between the auxiliary systems and supporting systems of the emergency power supply and the auxiliary systems and supporting systems of the alternate power source should be minimized.

4.263. The design should be such that essential auxiliary systems of the alternate power source are protected against damage due to the effects of external hazards (including extreme weather) and internal hazards.

4.264. The design of the auxiliary systems and supporting systems of the alternate power source should ensure these systems function for a length of time that is consistent with the time necessary to restore off-site power or, failing that, the emergency power supply. The quantity of fuel oil stored should be based on the time necessary to restore off-site power or the time necessary to resupply fuel oil.

4.265. The essential auxiliary systems and supporting systems of the alternate power source should be resistant to the SL-2 design basis earthquake.

4.266. During the periodic testing of the alternate power source, the operability of the auxiliary systems and supporting systems should be verified as well as the fuel oil quality.

4.267. More detailed recommendations are provided in SSG-34 [20].

OTHER SYSTEMS

4.268. Paragraphs 4.269–4.289 provide recommendations for the design of auxiliary systems and supporting systems that are not explicitly mentioned in SSR-2/1 (Rev.1) [1], but for which design considerations similar to those for the systems addressed in this Safety Guide are normally considered appropriate.

Equipment and floor drainage system

4.269. There are no specific requirements established in SSR-2/1 (Rev.1) [1] for the equipment and floor drainage system; however, Requirement 79 of SSR-2/1 (Rev.1), which requires suitable means to keep liquid radioactive releases to the environment as low as reasonably achievable, is relevant to this system.

System and/or equipment function

4.270. The equipment and floor drainage system should selectively collect the liquid and gaseous effluents produced by the reactor coolant system, the auxiliary systems and supporting systems, the refuelling cavity and the spent fuel pool — as well as potentially contaminated liquids produced in the plant (such as from floor drains, the laundry and decontamination activities) — and route these to storage and waste treatment systems, as appropriate. For pressurized heavy water reactors, any leakage from a system containing heavy water should be collected and pumped back to the system.

4.271. During normal operation, the equipment and floor drainage system should contribute to:

(a) Monitoring the leaktightness of the reactor coolant system and measurement of leaks within the containment;
(b) Limiting radioactive discharges to the environment by the recovery of effluents and by optimizing the balance between effluent treatment and effluent discharge.

4.272. In accident conditions, the equipment and floor drainage system should have the capability to re-inject highly contaminated liquids from the auxiliary buildings or secondary containment into the containment if the level of radioactivity in the effluent is too high to be treated in the short term (i.e. if storage would be needed prior to the treatment) or if the volume of fluids exceeds the waste treatment capacity.

4.273. The equipment and floor drainage system should help to reduce the retention of activity in the nuclear island buildings, and limit discharges to the environment by monitoring levels of radioactivity during normal operation. The equipment and floor drainage system could contribute directly to the safety functions that are fulfilled through providing protection against the effects of internal flooding and explosion (e.g. the prevention of hydrogen explosion from hydrogenated effluents).

Specific design basis

4.274. The equipment and floor drainage system should be designed to:

(a) Collect liquid effluents and transfer them to various systems depending on the ability of the effluents to be recycled or depending on their radiological characteristics, as appropriate;
(b) Collect hydrogenated or aerated liquid effluents from the primary system for recovery and recycling of boron (e.g. in the coolant storage and treatment system);

(c) Collect non-recyclable liquid effluents, transfer them for treatment, if necessary, and then monitor and discharge the effluents to the environment;

(d) Purge the primary system, for example before it is opened for defuelling and venting.

4.275. The equipment and floor drainage system should have sufficient capability to collect, treat and dispose of radioactive and non-radioactive liquid effluents in all plant states. Radioactive and non-radioactive liquids should be collected separately.

4.276. Components of the equipment and floor drainage system should be classified on the basis of their functions and their role as barriers, and should meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic testing maintenance and quality assurance). The following equipment is usually safety classified:

(a) Equipment that monitors leaks in the reactor coolant system, if it is the only means implemented for this purpose;

(b) Monitoring equipment that is credited in the analysis of flooding (see NS-G-1.11 [8]);

(c) Equipment necessary for containment isolation.

4.277. Lines of the equipment and floor drainage system that penetrate the containment are required to be provided with appropriate automatic containment isolation features that meet the single failure criterion: see Requirement 56 of SSR-2/1 (Rev. 1) [1]. This part of the equipment and floor drainage system should be safety classified (based on their safety function of safety category 1) and should meet the corresponding design requirements (e.g. in terms of redundancy, emergency power, protection against internal and external hazards, periodic inspection and testing, maintenance and quality assurance).

4.278. The components of the equipment and floor drainage system that carry radioactive material and whose failure would lead to off-site radiological consequences should be considered items important to safety, and should have a corresponding safety classification. The parts of the system that are considered items important to safety should be capable of being isolated from the parts of the system that are not important to safety.

4.279. The drainage capacity of the equipment and floor drainage system should be sufficient to ensure that safety functions continue to be fulfilled in the event of flooding from pipe breaks, tank leak and other potential sources (e.g. an earthquake causing a leak from tank of non-seismic design).

4.280. Sumps in the equipment and floor drainage system should be covered in order to prevent the transfer of contaminated effluent to the atmosphere and to avoid the contamination of other effluents that are to be recycled. Sump covers should be designed to prevent the retention of contaminated effluent on the floor of the building in normal operation.

4.281. Pumps submerged in the sumps of the equipment and floor drainage system should be designed to be low maintenance. Protection against the drop of various objects that could damage or obstruct the pumps should be provided.

4.282. Pumps submerged in the sumps of the equipment and floor drainage system should be equipped with strainers to protect them against the particles and fragments that the sumps might contain.

4.283. Building sumps in the equipment and floor drainage system should be provided with liquid level instrumentation that triggers an alarm in the event of high levels of liquid to warn the operator of a flooding risk inside the building. Where necessary, each sump and tank in the system should be equipped with a means of level measurement.

4.284. In areas where contamination might arise, the equipment and floor drainage system should be designed to prevent the spread of contamination to other areas.

4.285. To maintain the operability of the equipment and floor drainage system in the event of fire in adjacent fire compartments, the equipment and floor drainage system should, as far as practicable, be independent of similar equipment in other fire compartments (see NS-G-1.7 [4]).

Interfacing water systems

Demineralized water reserve

4.286. The demineralized water reserve is needed, for example, to supply the emergency feedwater system of pressurized water reactors, especially in the event of loss of the ultimate heat sink.

System and/or equipment function

4.287. The demineralized water reserve should supply the emergency feedwater systems in order to provide long term cooling by the steam generators in the event of loss of ultimate heat sink and/or in the event of external hazards.

Specific design basis

4.288. The demineralized water reserve should be designed to supply the emergency feedwater systems in the event of loss of ultimate heat sink and/or in the event of external hazards. As a minimum, the following combinations of external hazards should be considered:

- Storm-induced loss of off-site power and loss of the ultimate heat sink;
- Earthquake-induced loss of off-site power and loss of ultimate heat sink.

4.289. The demineralized water reserve and the associated system should be considered as performing a safety function of safety category 3, and should have an appropriate safety classification. If this safety function is to be performed in the event of an earthquake, the demineralized water reserve and the associated system should be seismic resistant.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev.1), IAEA, Vienna (2016).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (in preparation).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Nuclear Coolant System and Associated Systems in Nuclear Power Plants, IAEA Safety Standards Series No. DS481, IAEA, Vienna (in preparation).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004). (a revision of this publication is in preparation.)

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.13, IAEA, Vienna (2005).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Objectives and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards Other than Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.11, IAEA, Vienna (2004). (a revision of this publication is in preparation.)

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003). (a revision of this publication is in preparation.)

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003). (a revision of this publication is in preparation.)

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2009). (A revision of this publication is in preparation.)

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management and Development of a Programme for Long Term Operation of Nuclear Power Plants, IAEA Safety Standards Series No.SSG-48, IAEA, Vienna (in preparation).

[14] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Fuel Handling and Storage Systems for Nuclear Power Plants, IAEA Safety Standards Series No. DS487, IAEA, Vienna (in preparation).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. DS482, IAEA, Vienna (in preparation).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.6, IAEA, Vienna (2002). (A revision of this publication is in preparation.)

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and Radioactive Waste Management in the Design and Operation of Research Reactors, IAEA Safety Standards Series No. NS-G-4.6, IAEA, Vienna (2008).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-34, IAEA, Vienna (2016).

CONTRIBUTORS TO DRAFTING AND REVIEW

Amri, A.	International Atomic Energy Agency
Bertrand, R.	Consultant, France
Dugay, I.	Electricité de France, France
Krutzler, J.	Hungarian Atomic Energy Authority, Hungary
Ramaswamy, K.	Canadian Nuclear Safety Commission, Canada
Shaw, P.	International Atomic Energy Agency
Villalibre, P.	International Atomic Energy Agency
Wheeler, L.	Nuclear Regulatory Commission, United States of America