03 October 2019

IAEA SAFETY STANDARDS

for protecting people and the environment

Status: SPESS STEP 12

Approved by the Review Committees.

Reviewed in NSOC (Shaw/Asfaw)

For submission to the CSS for approval

Protection against Internal Hazards in the Design of Nuclear Power Plants

DS 494

DRAFT SAFETY GUIDE

Revision and merge of NS-G-1.7 and NS-G-1.11

FOREWORD

Later

CONTENTS

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 protection against internal hazards in the design of land based stationary water cooled nuclear power plants.

1.2. This Safety Guide is a revision and merger of IAEA Safety Standards Series No. NS-G-1.11, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants[1], and IAEA Safety Standards Series No. NS-G-1.7, Protection against Fires and Explosions in the Design of Nuclear Power Plants[2], both of which are superseded by this Safety Guide. This revision principally consists of updating the technical content to make it consistent with the requirements established in SSR-2/1 (Rev. 1) [1]. In addition, internal hazards due to electromagnetic fields or electromagnetic interference, and those due to the release of hazardous substances originating from within the site boundary are included in the scope of this Safety Guide.

OBJECTIVE

1.3. The objective of this Safety Guide is to provide recommendations to regulatory bodies, nuclear power plant designers and licensees on hazard assessment (including for combinations of hazards) and design concepts for protection against internal hazards in nuclear power plants, in order to meet the requirements established in SSR-2/1 (Rev. 1) [1].

SCOPE

1.4. This Safety Guide applies primarily to nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district

[1] 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)

[2] 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)

heating or desalination). For innovative developments in future systems, for plant modifications or for other reactor types, some parts of this Safety Guide might not be fully applicable or might need some judgement in their interpretation.

1.5. This Safety Guide covers the design features necessary to protect items (i.e. structures, systems and components (SSCs)) important to safety in nuclear power plants against the effects of internal hazards during all modes of operation. The following internal hazards are reviewed in this Safety Guide: fires; explosions; missiles; pipe breaks; flooding; collapse of structures and falling objects with a focus on heavy load drop; electromagnetic interference; and release of hazardous substances originating from within the site boundary.

1.6. This Safety Guide does not cover conventional industrial safety, except where this could affect the safety of the nuclear power plant.

1.7. The recommendations provided in this Safety Guide are targeted primarily at new nuclear power plants. For plants designed with 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].

STRUCTURE

1.8. Section 2 outlines general considerations for protection against internal hazards in nuclear power plants. Section 3 provides general design recommendations for protection against internal hazards in nuclear power plants. Section 4 provides specific recommendations for protection against fires, explosions, missiles, pipe breaks, flooding, collapses of structures and falling objects with a focus on heavy load drop, electromagnetic interference, and release of hazardous substances originating within the site boundary. Appendix I provides guidance on dealing with hazard combinations. Appendix II provide detailed guidance on protection against internal fires.

GENERAL CONSIDERATIONS

2.1. Requirement 17 of SSR-2/1 (Rev. 1) [1] states:

> **"All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determining the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant."**

2.2. Paragraph 5.16 of SSR-2/1 (Rev. 1) [1] states:

> "The design shall take due account of internal hazards such as fire, explosions, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact and release of fluid from failed systems or from other installations on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised."

2.3. Section 3 and Section 4 of this Safety Guide provide general design recommendations and specific design recommendations, respectively, to meet Requirement 17 and para. 5.16 of SSR-2/1 (Rev. 1) [1] regarding internal hazards.

2.4. An item important to safety is an item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public [2]. In accordance with this definition, and the definition of design extension conditions in SSR-2/1 (Rev. 1) [1], safety features for design extension conditions are items important to safety. Therefore, safety features for design extension conditions need to be designed or protected against applicable internal hazards. In addition, safety features for design extension conditions could be sources of internal hazards that need to be considered.

2.5. Internal hazards are those hazards to the safety of the nuclear power plant that originate from within the site boundary, and are associated with failures of facilities and activities that are under the control of the operating organization. The internal hazards covered in this Safety Guide are listed in para. 1.5.

2.6. The hazards caused by (or occurring at) different facilities on the same site are also considered to be internal hazards.

2.7. Internal hazards can also be generated by external hazards (e.g. an earthquake followed by an internal flood, an earthquake causing a fire).

2.8. Effects induced by internal hazards can also result in cascading effects, and induce other internal hazards (e.g. a missile can cause a pipe break and then internal flooding).

2.9. All credible combinations of hazards (see Appendix I) are also considered within the scope of this Safety Guide.

2.10. Internal hazards have the potential to induce initiating events, to cause failures of equipment that is necessary to mitigate the consequences of such events, and to adversely affect (directly or indirectly) the barriers for the prevention of the release of radioactive materials. Internal hazards could, because of their nature, simultaneously challenge more than one level of defence in depth, and increase, for example, the degree of dependency between the originator of initiating events and the failure of mitigation equipment.

2.11. While it might not be practical or possible to prevent an internal hazard from triggering an anticipated operational occurrence, one of the objectives of layout and design of the nuclear power plant is to ensure, to the extent practicable, that internal hazards do not trigger an accident.

2.12. The aim of considering internal hazards in the design of nuclear power plants is to ensure that the fundamental safety functions (see Requirement 4 of SSR-2/1 (Rev. 1) [1]) are fulfilled in any plant state, and that the plant can be brought to and maintained in a safe state after the occurrence of any credible internal hazard. This implies the following:

(a) Redundant systems are segregated to the extent possible or adequately separated, and protected as necessary, to prevent the loss of the safety function performed by the systems;
(b) The design of individual SSCs is such that design basis accidents, or design extension conditions potentially induced by internal hazards, are avoided to the extent practicable;

(c) The segregation, separation and protection measures implemented are adequate to ensure that the system response described in the analysis of postulated initiating events is not compromised by the effects of the internal hazard;

(d) The design is such that an internal hazard does not lead to a common cause failure between redundant safety systems designed to control design basis accidents, and between these systems and the safety features necessary in the event of design extension conditions with core melting;

(e) An internal hazard occurring elsewhere in the plant does not affect the habitability of the main control room. If the main control room is not habitable, access to, and habitability of the supplementary control room are ensured. In addition, and when necessary, access by plant personnel to equipment in order to perform local actions is possible.

2.13. In accordance with the concept of defence in depth (the first level of defence in depth), protection against internal hazards is provided in general by ensuring the high quality and reliability of SSCs, by environmental qualification of these SSCs, by application of the principles of redundancy, diversity, and by physical separation, segregation, and design of appropriate barriers and other protective means. Therefore, the design against the effects of internal hazard is an iterative process, integrating the needs of protection against several internal hazards. Proper surveillance and in-service inspections of SSCs need to be implemented for early detection of the occurrence of an internal hazard (or of signs that can lead to the occurrence of an internal hazard) and implementation of necessary corrective actions to ensure protection against the hazard. Identification of hazards at an early stage in the design is often used as a practical method to identify and eliminate hazards.

GENERAL DESIGN RECOMMENDATIONS FOR PROTECTION AGAINST INTERNAL HAZARDS

3.1. Notwithstanding the measures taken to minimize the likelihood of an internal hazard, such hazards are possible. The capability of the nuclear power plant to withstand internal hazards and to mitigate the effects of postulated initiating events caused by them is required to be an integral part of the design of the plant: see para. 5.16 of SSR-2/1 (Rev. 1) [1].

3.2. The design approach proposed in this Safety Guide for the protection of items important to safety and, as applicable, of plant personnel performing actions to protect against internal hazards, is based on the following major steps:

(a) Identification of internal hazards and credible combinations of hazards, and characterization of the effects of the hazard(s);
(b) Design for preventing internal hazards or for preventing the adverse effects of internal hazards;
(c) Design of means for mitigating the adverse effects of internal hazards on items important to safety.

The design approach also includes the assessment of the protection against internal hazards, consistent with the design objectives in para. 2.12, and the verification that these objectives are met for all credible hazards at the plant.

3.3. The design for the protection against internal hazards should take into account design recommendations for safety and design recommendations for security in an integrated manner, such that safety measures and security measures do not compromise each other. Recommendations on nuclear security are provided in Ref. [3].

3.4. Certain postulated hazards might be of such magnitude that providing design features to mitigate the effects of these hazards is not practicable (e.g. an uncontrolled drop of the reactor vessel head). In such cases, the focus is on prevention, and an evaluation should be performed to ensure, with a high level of confidence, that such events are extremely unlikely. Even if such events cannot be completely prevented, design measures are still required to be implemented to mitigate the consequences of such events to the extent practicable: see para. 2.8 of SSR-2/1 (Rev. 1) [1].

3.5. In order to protect items important to safety, a nuclear power plant should have a sustained capability for the early detection and effective control of internal hazards.

IDENTIFICATION AND CHARACTERIZATION OF HAZARDS AND HAZARD COMBINATIONS

3.6. In plant design, internal hazards should be identified using a combination of engineering judgement, operating experience and lessons from similar plant designs, and the results of deterministic safety assessment and probabilistic safety assessments. The identification and the characterization of internal hazards should include a consideration of the initial conditions (e.g. plant shutdown modes), the magnitude and the likelihood of the hazards, the locations of the sources of the hazards, the resulting environmental conditions and the possible impacts on SSCs important to safety, or on other SSCs for which failure could lead to a postulated initiating event. The hazard identification and characterization process should be rigorous, supported by plant walk-downs for verification purposes, and should be well documented.

3.7. Possible combinations of internal–internal and internal–external hazards and any consequential effects (e.g. high energy pipe break, , pipe whip, jet effect, flooding) are required to be considered in the design of the plant: see para. 5.32 of SSR-2/1 (Rev. 1) [1]. The combinations to be considered will depend on the site characteristics and the general plant design.[3]

3.8. All credible combination of hazards should be considered in the design. The screening out of any combinations should be justified (see Appendix I).

3.9. The identification of hazards includes assumptions about their characteristics. Bounding or conservative assumptions could be made about these characteristics in order to address uncertainties, provided these assumptions are justified.

3.10. Paragraph 5.15A of SSR-2/1 (Rev. 1) [1] states:

[3] For example, some combinations of hazards might involve external events that are not plausible in certain locations (e.g. sandstorms, blizzards). Therefore, it is not necessary or even feasible to prescribe a set of combined hazards that would be applicable to all sites.

> "Items important to safety shall be designed and located, with due consideration of other implications for safety, to withstand the effects of hazards or to be protected, in accordance with their importance to safety, against hazards and against common cause failure mechanisms generated by hazards."

The relevant internal hazards should be identified, and the effects and environmental conditions created by these hazards are required to be evaluated and taken into account in the design and layout of the plant: see Requirement 17 of SSR-2/1 (Rev. 1) [1]. This is considered in paras 3.11–3.34, which also apply, as appropriate, to internal hazards resulting from combinations of hazards.

PREVENTION OF INTERNAL HAZARDS AND OF THE EFFECTS OF THE HAZARDS

3.11. Some hazards may be screened out either because they are physically impossible (e.g. heavy load drop if there is no lifting equipment) or by a stringent justification, including, at a minimum, very high quality design, manufacturing, construction, in-service inspection and due consideration of feedback from operating experience.

3.12. When hazards cannot be screened out, measures, including administrative ones, should be implemented to reduce the frequency and potential magnitude of the hazards and their effects on SSCs important to safety. This should be mainly achieved by reducing, as far as practicable, the potential sources of hazards (e.g. limiting the use of combustible materials and the presence of ignition sources), supported by surveillance and in-service inspections. It can also be achieved by location and layout (e.g. ensuring the best orientation of fast rotating machines).

MITIGATION OF THE EFFECTS OF INTERNAL HAZARDS

3.13. For each internal hazard that is considered in the design, measures should be implemented to control and to limit the consequences. These measures will depend on the type of hazard and on the specific technical solutions included in the design. In general, specific measures for the detection of the occurrence of the respective hazard should also be included.

3.14. The design features for protection from the effects of internal hazards are required to be safety classified: see Requirement 22 of SSR-2/1 (Rev. 1) [1]. This safety classification should be conducted in accordance with the recommendations provided in IAEA Safety Standards

Series No. SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants [4]. Protective design features are required to be classified on the basis of their function and their safety significance: see para. 5.34 of SSR-2/1 (Rev. 1) [1].

3.15. Measures to mitigate the consequences of events can be passive, active or procedural. Passive design solutions – without moving parts or an external energy supply – are generally considered preferable to the implementation of active measures or of procedures.

3.16. For active protective features, where applicable, the worst single failure should be assumed.

3.17. The consideration of failure of a passive protective feature is not necessary, provided that it is demonstrated that its failure is very unlikely and that its function would remain unaffected by the postulated hazard (see para. 5.40 of SSR-2/1 (Rev. 1) [1]).

3.18. If it is feasible, the early detection of the occurrence of internal hazards, supported by appropriate actions in response to the detection of the hazard, contributes to the mitigation of the possible consequences.

3.19. Measures for mitigation of the effects of internal hazards should include, as appropriate, redundancy, diversity and physical separation, including segregation of redundant trains. The concept of segregation is applicable at the level of:

(a) Plant layout: for example, separating the emergency diesel generators from one another.
(b) Building layout: for example, mitigating the effects of missile hazards by proper orientation of equipment.
(c) Rooms and compartments: for example, dividing them into fire compartments or cells.
(d) SSCs: for example, separating cables of different safety trains from one another.

3.20. The layout and design provisions that protect SSCs important to safety from the effects of internal hazards should be such that the design objectives in para. 2.12 are met.

3.21. The reliability of the means of detecting internal hazards and mitigating their consequences should be consistent with their role in providing defence in depth.

ASSESSMENT, VERIFICATION AND SUCCESS CRITERIA

3.22. To evaluate the adequacy of the design, qualitative and/or quantitative success criteria should be defined, consistent with the design objectives in para. 2.12.

3.23. An assessment should be made to demonstrate that the internal hazards relevant to the design of the nuclear power plant have been considered, that provisions for prevention and mitigation have been designed with sufficient safety margins to address the uncertainties in the identification and characterization of internal hazards and their effects, as well as for the avoidance of cliff-edge effects. This assessment should be carried out early in the design phase and should be documented. It should be updated before initial loading of the reactor fuel, and kept up to date during plant operation.

3.24. It should be a goal of the design that a single internal hazard does not trigger an accident, unless the hazard can be considered by itself as a postulated accident (e.g. pipe rupture). In particular, the design should ensure with a high level of confidence that a single internal hazard does not result in design extension conditions with core melting. If this cannot be achieved, the designer should demonstrate that the boundary conditions used in the analysis of the corresponding accident are not affected by the loads resulting from the internal hazard.

3.25. The design features protecting the SSCs that are intended to be used under design extension conditions should be designed or verified for the loads, conditions and durations associated with these scenarios (e.g. effects of hydrogen combustion). These design features should be protected against the consequences of an internal hazard that occurs before design extension conditions have been completely mitigated. Best estimate design loads, conditions and durations can be used for the design or the verification of these protective features.

3.26. Deterministic safety analyses, supplemented if applicable by probabilistic analyses, should be performed to demonstrate the adequacy of the design of the protection against internal hazards. The design should be an iterative process accounting for the results of such safety analyses.

3.27. Internal hazards considered in the deterministic safety analyses for a specified location in the nuclear power plant include the following categories:

(a) Internal hazards that do not trigger, or result from, an anticipated operational occurrence or an accident;
(b) Internal hazards that could trigger, or result from, an anticipated operational occurrence;
(c) Internal hazards that could trigger, or result from, a design basis accident;
(d) Internal hazards that could trigger, or result from, design extension conditions without significant fuel degradation;
(e) Internal hazards that could result from design extension conditions with core melting.

3.28. For internal hazards that do not trigger, or result from, an anticipated operational occurrence or an accident, an assessment should be performed to demonstrate that the plant can be brought to, and maintained in, a safe state even in the event of a single failure, including when equipment is unavailable due to preventive maintenance considered in the design. In practice, a functional analysis is normally performed to demonstrate that an adequate number of functions remain available to reach and maintain a safe state.

3.29. For internal hazards that could trigger, or result from, an anticipated operational occurrence, an assessment should be performed to demonstrate that the plant can be brought to, and maintained in, a safe state, even in the event of a single failure, including when equipment is unavailable due to preventive maintenance considered in the design. A specific analysis of transients is normally not necessary as this is provided by the corresponding analysis of anticipated operational occurrences. In such cases, the analysis of the internal hazards is limited to a functional analysis that should demonstrate that an adequate number of functions to control anticipated operational occurrences and to reach and maintain a safe state are provided by the design.

3.30. For internal hazards resulting from accidents without significant fuel degradation, the objective of the assessment should be to demonstrate that the boundary conditions, in particular for systems credited in the accident analysis, are not affected by the hazard. A specific accident analysis is normally not necessary as this is provided by the corresponding accident analysis in which the rules for design basis accidents or the rules for design extension conditions without significant fuel degradation should be applied, as appropriate (see IAEA Safety Standards Series No. SSG-2 (Rev. 1), Deterministic Safety Analysis for Nuclear Power Plants [5]). As stated in para. 2.11, design basis accidents or design extension conditions induced by internal hazards should be avoided to the extent practicable. If an internal hazard could lead to an

accident without significant fuel degradation, the objective of the assessment should be to demonstrate that the fundamental safety functions are fulfilled and that the plant can be brought to, and maintained in, a safe state.

3.31. For the deterministic assessment of an internal hazard triggered by design extension conditions with core melting, it should be demonstrated by using the corresponding rules [5] that the boundary conditions, in particular for systems credited in the accident analysis, are not affected by the hazard. It should be demonstrated that the SSCs necessary to maintain the integrity of the containment are not affected by the hazard. In particular, the integrity of instrumentations providing necessary measurements should be ensured.

SPECIFIC ASPECTS

3.32. For a site containing multiple units, steps should be taken to ensure that an internal hazard in one unit under construction or in operation or under decommissioning would not have any safety consequences for a neighbouring operating unit or other installations on the site (e.g. spent fuel pool, radioactive waste management facility). Measures for temporary separation should be put in place if necessary to protect the operating units. Consideration should be given to the possibility of internal hazards involving facilities shared between units: see para. 5.63 of SSR-2/1 (Rev. 1) [1].

3.33. The main control room and the supplementary control room should be adequately separated from possible sources of internal hazards as far as applicable. The means by which the control is transferred from the main control room to the supplementary control room should be resilient against internal hazards to prevent malfunction or spurious actuation[4].

3.34. Additional guidance on assessment and verification of specific internal hazards is given in Section 4. Further information on the approach to hazard combinations is provided in Appendix I.

[4] Spurious actuation of plant components (of the same type or combinations of different types of component) has the potential to place a given plant into an unsafe operating condition that might not be bounded by the plant's safety analyses.

RECOMMENDATIONS FOR SPECIFIC INTERNAL HAZARDS

INTERNAL FIRES

General

4.1. Nuclear power plants contain a range of combustible materials, as part of the structure, equipment, fluids, cabling or miscellaneous items in storage. Fire can be assumed to occur in any plant area where combustible materials are present. Where it is not practicable to eliminate these materials, design measures for fire prevention should be applied to all the fixed and transient (temporary) fire loads. Such measures include minimization of fixed fire loads, prevention of their accumulation, and control or (preferably) elimination of sources of ignition.

4.2. The design of fire prevention measures should start in the early stages of the design process. All such measures should be fully implemented before nuclear fuel arrives on the site.

Identification and characterisation of fire hazards

4.3. A fire hazard analysis of a plant site should be undertaken to demonstrate the overall adequacy of fire protection measures. In particular, the fire hazard analysis should determine the necessary fire resistance rating of fire barriers and the necessary fire detection and extinguishing capabilities (see the detailed recommendations on fire hazard analysis in Appendix II).

4.4. The fire hazard analysis should be carried out in accordance with the recommendations in para. 3.23.

Fire prevention

4.5. Several measures should be taken in the design to minimize the likelihood of internal fires, as follows:

(a) Removal, minimization and segregation of fixed and transient fire loads, as far as practicable;
(b) Elimination of potential ignition sources to the extent practicable; otherwise, the strict control of any such sources;
(c) Segregation of ignition sources from fuel sources.

Minimizing fire loads

4.6. Paragraph 6.54 of SSR-2/1 (Rev. 1) [1] states:

> "Non-combustible or fire retardant and heat resistant materials shall be used wherever practicable throughout the plant, in particular in locations such as the containment and the control room."

4.7. In order to reduce the fire load to the extent possible thus minimizing the fire hazard, the following aspects should be considered in the plant design:

(a) The use of non-combustible construction materials (e.g. structural materials, insulation, cladding, coatings and floor materials) and plant fixtures, as far as practicable;
(b) The use of non-combustible air filters and filter frames, as far as practicable; otherwise low combustible materials could be used;
(c) The use of a protected pipe or double pipe design for lubricating oil lines and for collection of leakages;
(d) The use of hydraulic control fluids of low flammability for the control systems of steam turbines and other equipment;
(e) The selection of dry type transformers, as far as practicable;
(f) The use of non-combustible materials in electrical equipment, such as switches and circuit breakers, and in control and instrumentation cubicles, and use of flame retardant non-corrosive cables or cables with suitable qualifications;
(g) The use of non-combustible scaffolding and staging materials;
(h) Segregation and compartmentation of fire loads, as far as practicable, to reduce the likelihood of fire and other effects spreading to other SSCs important to safety.

4.8. Precautions should be taken to prevent thermal insulating materials from absorbing flammable liquids (e.g. oil). Suitable protective coverings or drip guards should be provided.

4.9. Design measures should be implemented to provide for the proper storage of transient combustible materials that arise during operation; either separated from items important to safety, or otherwise protected.

4.10. Storage allowances for flammable liquids and gases inside plant buildings should be minimized. Storage areas for bulk supplies of any flammable or combustible materials should be located in areas or buildings that do not contain items important to safety.

4.11. Suitable fire rated storage cabinets should be provided to house any small quantities of flammable liquids or gases necessary to support plant operations.

4.12. Systems containing flammable liquids or gases should be designed to have a high degree of integrity in order to prevent leaks. They should be protected from degradation effects (e.g. corrosion), destructive effects (e.g. vibration, effects of hazards) and maintained in good conditions. Safety devices, such as flow limiting, excess flow and/or automatic shut-off devices, and bunding and/or dyking devices, should be provided to limit potential spills in the event of a failure.

Minimizing ignition sources

4.13. In the design, the number of ignition sources should be minimized to the extent practicable (e.g. a resilient design for the electrical protection system could be used).

4.14. Systems that contain pressurized combustible liquids, such as hydraulic fluids and lubricating oil, should be provided with spray guards, as far as practicable. Equipment should be appropriately rated, consistent with the hazards present in the environment, to prevent it providing a source of ignition for flammable gases and ignitable sprays.

4.15. Potential ignition sources arising from plant systems and equipment should be controlled.

4.16. As far as is practicable, systems and equipment should be made safe through design, so as not to provide any ignition source. Where this is not practicable, such systems and equipment should be separated from combustible materials, or else insulated or enclosed. Equipment for dispensing flammable liquids or gases should be properly earthed. Hot pipework near combustible materials that cannot be moved elsewhere should be shielded and/or insulated.

4.17. Cables should be laid on trays or installed conduits, or placed in other acceptable structures made out of non-combustible materials; steel is often used for this purpose. The distances between power cables or cable trays should be sufficient to prevent the cables from heating up to unacceptably high temperatures. The electrical protection system should be designed so that the cables will not overheat under normal loads or transient short circuit conditions. Further recommendations are provided in IAEA Safety Standards Series No. SSG-

39, Design of Instrumentation and Control Systems for Nuclear Power Plants [6], and IAEA Safety Standards Series No. SSG-34, Design of Electrical Power Systems for Nuclear Power Plants [7].

Fire mitigation

Timely detection and extinguishing of fires

4.18. Requirement 74 of SSR-2/1 (Rev. 1) [1] states:

> **"Fire protection systems, including fire detection systems and fire extinguishing systems, fire containment barriers and smoke control systems, shall be provided throughout the nuclear power plant, with due account taken of the results of the fire hazard analysis."**

These systems and equipment should be designed to provide a timely alarm in the event of fire, and the rapid extinguishing of fires, in order to minimize adverse effects on items important to safety and on plant personnel performing actions important to safety.

4.19. Active and passive means of fire protection that are needed to protect SSCs important to safety against a fire following a different event (e.g. an earthquake) should be identified, adequately designed and qualified to resist the effects of this event.

4.20. Active and passive means of fire protection that do not need to maintain a functional capability following a postulated initiating event should be designed and qualified so that they do not fail in a way that could adversely affect safety.

4.21. The need to minimize spurious alarms and discharges of extinguishing media should be taken into account in the design of fire detection and extinguishing systems and equipment.

4.22. Paragraph 6.51 of SSR-2/1 (Rev. 1) [1] states:

> "Fire extinguishing systems should be capable of automatic actuation where appropriate. Fire extinguishing systems shall be designed and located to ensure that their rupture or spurious or inadvertent operation would not significantly impair the capability of items important to safety."

In addition, fire extinguishing systems should be designed and located so that they would not simultaneously affect redundant parts of safety groups, and thereby cause the measures taken to meet the 'single failure' criterion to become ineffective.

4.23. Fire detection systems, fire extinguishing systems and support systems, such as ventilation and drainage systems, should, as far as practicable, be independent of their counterparts in other fire compartments. The purpose of this is to maintain the operability of such systems in adjacent fire compartments.

4.24. The control of fire is achieved through a combination of fixed fire suppression and extinguishing systems and equipment and manual fire-fighting capabilities. To ensure an adequate level of protection for fire compartments, the following elements should be considered in the design of the plant:

(a) Where fire detection or extinguishing systems are credited as active elements of a fire compartment, arrangements for their design, procurement, installation, verification and periodic testing should be sufficiently stringent to ensure their permanent availability. In this case, the performance of these systems should be designed taking into account the application of the single failure criterion for the safety function they protect. The application of the single failure criterion is described in paras 5.39–5.40 of SSR-2/1 (Rev. 1) [1].

(b) Where fire detection systems or fixed fire extinguishing systems are relied upon as protection against a potential fire following a different event (e.g. from external or internal hazards), they should be designed to withstand the effects of this event.

(c) The normal or the spurious operation of fire extinguishing systems should not impair the performance of safety functions.

4.25. The reliability of fire detection and extinguishing systems should be consistent with their role in providing defence in depth, and with the recommendations provided in SSG-39 [6]. This also includes ensuring that water supplies (including mains supplied) and utility connections (fire hydrants) are maintained such that they will meet any necessary demand.

4.26. Each fire compartment should be equipped with suitable, effective and reliable fire detection and alarm features.

4.27. Paragraph 6.52 of SSR-2/1 (Rev. 1) [1] states:

> "Fire detection systems shall be designed to provide operating personnel promptly with information on the location and spread of any fires that start."

This information should be used when taking action to avoid adverse effects on SSCs important to safety.

4.28. When items such as fire pumps, water spray systems, ventilation equipment and fire dampers are controlled by fire detection systems, and where spurious operation would jeopardize safety functions, the operation of these items should be controlled by two diverse means of detection operating in series. The design should allow the operation of the system to be stopped if the actuation is found to be spurious.

4.29. Systems and equipment for fire suppression and fire extinguishing, including manual fire-fighting equipment should be of sufficient capacity to ensure that later fires caused by re-ignition (e.g. due to hot materials) are prevented.

Preventing the spread of fires

4.30. Early in the design phase, the plant buildings should be divided into fire compartments, as far as practicable, and, where that is not possible, into fire cells.

4.31. Building structures (including columns and beams) should have a suitable fire resistance rating. The fire stability rating (the mechanical load bearing capacity as well as the thermal load bearing capacity) of structural elements within a fire compartment, or that form the compartment boundaries, should not be less than the fire resistance rating of the fire compartment itself.

4.32. The plant layout should be such that combustible materials (solids, liquids and gases) are not in proximity to items important to safety, as far as practicable. The design aim should be to segregate items important to safety from high fire loads and to segregate redundant safety systems from each other. The aim of this segregation is to reduce the risk of fires spreading, to minimize secondary effects and to prevent common cause failures.

4.33. The segregation of redundant parts of a safety system ensures that a fire affecting one division[5] of a safety system would not prevent the execution of the safety function within another division. This should be achieved by locating each redundant division of a safety system in its own fire compartment or at least in its own fire cell. The number of penetrations between fire compartments of different redundant divisions should be minimized and the penetrations should be sealed in a qualified manner.

4.34. The effects of postulated fires should be analysed for all areas containing items important to safety and all other locations that constitute a fire hazard to items important to safety. In the analysis, the functional failure of all systems important to safety within the fire compartment or the fire cell in which the fire is postulated should be assumed, unless they are protected by qualified fire barriers or surrounded by casings, enclosures or encapsulations designed to (or able to) withstand the consequences of the fire. Exceptions should be justified.

Mitigation of secondary fire effects

General

4.35. The hazardous (direct and indirect) effects of fire are the production of smoke (with the consequent possibility of its spreading to other areas not affected by the originating fire); radiative and convective heat; flame, which might lead to the further spread of fire, to equipment damage, to functional failures and to possible explosive effects; the production of other fire by-products; as well as pressure build-up and reduction of oxygen levels. Effects due to fire extinguishing should also be considered.

4.36. The main objectives in mitigating the effects of a fire are as follows:

(a) To confine the flame, heat and smoke in a limited space within the plant to minimize spread of the fire and consequent effects on the surrounding plant;
(b) To provide safe escape routes and access routes for personnel;
(c) To provide access for manual firefighting, manual actuation of fixed extinguishing systems and operation by plant personnel of systems necessary to reach and maintain safe shutdown;

[5] A system or set of components can be divided into redundant 'divisions' to allow for the implementation and maintenance of physical, electrical and functional independence with respect to other redundant sets of components. (adapted from Ref. [8])

(d) To provide the means for venting of smoke and heat either during or following a fire, if necessary;
(e) To control the spread of the extinguishing agents to prevent damage to items important to safety.

Layout of buildings

4.37. The layout of buildings, equipment, plant ventilation systems, and fixed fire detection and extinguishing means should all be taken into account in considering the mitigation of fire effects.

4.38. Requirement 36 of SSR-2/1 (Rev. 1) [1] states:

> **"A nuclear power plant shall be provided with a sufficient number of escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other services essential to the safe use of these escape routes."**

Adequate access routes for the firefighting teams or field plant personnel should also be provided and these should be protected. The use of combustible materials (e.g. lighting, paints and coatings) in escape routes and access routes should be limited, as far as practicable. The layout of buildings should be arranged to prevent the propagation of fire and smoke from adjacent fire compartments or fire cells to the escape routes or access routes. Further details are given in Appendix II.

Ventilation systems

4.39. Ventilation systems should neither compromise building compartmentation nor compromise the availability of redundant divisions of safety systems. These conditions should be addressed in the fire hazard analysis.

4.40. Each fire compartment containing a redundant division of a safety system should have a ventilation system designed such that a fire in one safety fire compartment will not propagate fire effects that induce a loss of ventilation of another safety fire compartment. Parts of the ventilation system (e.g. connecting ducts, fan rooms) that are located in an adjacent fire compartment should have the same fire resistance rating as the compartment or, alternatively, the fire compartment penetration should be isolated by appropriately rated fire dampers. These should operate automatically, where appropriate.

4.41. If a ventilation system serves more than one fire compartment, provision should be made to maintain the segregation between fire compartments. Means should be provided to prevent the spread of fire, heat or smoke to other fire compartments by installing fire dampers at the boundaries of each fire compartment or by installing fire resisting duct work, as appropriate.

4.42. Charcoal filter banks contain a high fire load. These should be taken into consideration in determining recommendations for fire protection. A fire in a filter bank could lead to a radioactive release: consequently, passive and active means of protection should be provided to protect charcoal filter banks from fire. Such measures could include:

(a) Locating the filter in a fire compartment.
(b) Monitoring of the air temperature and automatic isolation of the air flow.
(c) Provision of automatic protection by means of a water sprinkler to cool the outside of the filter vessel.
(d) Provision of a suitable extinguishing system inside the charcoal vessel. In designing a water-based extinguishing system for that purpose, consideration should be given to the flow rate of the water. If it is too low, the reaction between burning charcoal at high temperature and water can result in the production of hydrogen, which might induce another fire or explosion hazard. To prevent this risk, a high water flow rate should be used. The water injected into the filter housing should be drained or considered as an additional weight in the filter design.

4.43. Where combustible filters need to be used in ventilation systems or filtration units and the subsequent malfunction or failure of these filters could result in unacceptable radioactive releases, the following precautions should be taken:

(a) Filter banks should be separated from other equipment by means of adequate fire barriers.
(b) Appropriate means (e.g. upstream and downstream dampers) should be used to protect the filters from the effects of fire.
(c) Fire detectors, carbon monoxide gas sensors and/or temperature sensors should be appropriately installed to inform the plant personnel of a fire in the filter bank.

4.44. The intakes for the fresh air supply to the fire compartments should be located at a distance from the exhaust air outlets and smoke vents of other fire compartments, to the extent

necessary to prevent the intake of smoke or combustion products and the malfunction of items important to safety.

Fires and potential radioactive releases

4.45. Equipment that could release radioactive substances in the event of a fire should be identified in the fire hazard analysis. This equipment should be housed in separate fire compartments in which the designed fire loads, both fixed and transient, are minimized.

4.46. The design should provide for heat and smoke venting in fire compartments containing radioactive materials. Although venting can result in a radioactive release to the external environment, it can prevent, directly or through the improvement of conditions for fire extinguishing, the subsequent release of larger quantities of radioactive substances. Two cases should be distinguished, as follows:

(a) The possible release can be shown to be well below regulatory limits.
(b) The amount of radioactive material in the fire compartment could produce a radioactive release exceeding the regulatory limits. In this case, provisions should be made for isolating the ventilation or closing fire dampers.

In each case, monitoring of the vented air should be performed to inform operational decision making.

4.47. Design measures are required to be taken to keep the amount of radioactive material released as low as reasonably achievable: see Requirement 34 of SSR-2/1 (Rev. 1) [1] The design is required to include provisions for monitoring the condition of filters (see para. 6.63 of SSR-2/1 (Rev. 1) [1]), in order to assist plant personnel in taking operational decisions.

Layout and systems for electrical equipment

4.48. Cabling for redundant safety systems should be installed in individual specially protected routes, preferably in separate fire compartments, as far as practicable, and cables should not cross between redundant divisions of safety systems. As described in para. II.17 exceptions may be necessary in certain locations, such as control rooms and the reactor containment. In such cases, the cables should be protected by means of qualified fire rated barriers or

encapsulations (e.g. qualified cable wraps). Fire extinguishing systems or other appropriate means could be used, with justifications made in the fire hazard analysis.

4.49. All possible fire induced failures that could affect redundant systems performing safety functions should be analysed (e.g. by electrical circuit analysis, including multiple spurious actuations). Electrical circuits should be rerouted or protected by combinations of qualified fire rated barriers and fire extinguishing systems, with appropriate justifications made in the fire hazard analysis.

Special locations

4.50. The main control room of a nuclear power plant generally contains control equipment of different safety systems in close proximity. Particular care should be taken to ensure that, as far as practicable, non-combustible materials are used in electrical cabinets, the room structure itself, any fixed furnishings, and floor and wall finishes. Redundant equipment used to perform the same safety function should be housed in separate electrical cabinets. Fire barriers should be utilized to provide any necessary separation to the extent possible. Every effort should be made to keep the fire load in control rooms to a minimum.

4.51. In order to ensure their habitability, the main control room and the supplementary control room should be protected against the ingress of smoke and combustion gases and against other direct and indirect effects of fire and of the operation of extinguishing systems.

4.52. The fire protection of the supplementary control room should be similar to that of the main control room. Particular emphasis should be placed on protection from flooding and other effects of the operation of fire extinguishing systems. The supplementary control room should be located in a fire compartment separate from the one containing the main control room. The ventilation system for the supplementary control room should not be a common system shared with the main control room. The separations between the main control room and the supplementary control room should meet the design objectives in para. 2.12(e).

4.53. The reactor containment is a fire compartment in which items of equipment for redundant divisions of safety systems might be close to each other. Redundant divisions of safety systems should be located as far apart as practicable and should be protected, where possible, by passive protection measures such as partial fire enclosures and cable fire protection systems.

4.54. Reactor coolant pump motors containing a large inventory of flammable lubricating oil should be provided with fire detection systems, fixed fire extinguishing systems (normally under manual control) and oil collection systems (e.g. oil pans). The oil collection systems should be capable of collecting oil and water from all potential leakage points or discharge points and draining these to a vented container or another safe location.

4.55. Similar provision should be made for oil-filled transformers, as applicable.

4.56. The turbine building could contain items important to safety. Fire compartmentation might be difficult in some areas, and substantial fire loads are present such as large inventories of flammable materials in the lubricating, cooling and hydraulic systems of the steam turbine(s) and in the hydrogen atmosphere within the generator(s). Consequently, in addition to fire suppression systems, adequate oil collection systems (e.g. oil pans) should be provided for all equipment containing flammable liquids. The use of flammable hydrocarbon based lubricating fluids should be minimized. If flammable liquids have to be used, they should be liquids with high flashpoints, consistent with operational needs.

4.57. The safety features for design extension conditions that are needed to function in the long term under such conditions should be protected against the effects of a fire.

4.58. Equipment of the systems used for long term heat removal from the containment during severe accidents should be redundant or diverse and located in different fire compartments.

4.59. Ventilation equipment necessary in the long term during severe accidents to confine radioactive material should be redundant and located in different fire compartments. Portions of the system containing charcoal filters should be capable of being isolated and should be designed with suitable fire protection features (see para. 4.42).

INTERNAL EXPLOSIONS

General

4.60. Explosion hazards should be eliminated by design, as far as practicable. Priority should be given to design measures that prevent or limit the formation of explosive mixtures.

Identification and characterization of explosion hazards

4.61. Explosion hazards within buildings and compartments containing items important to safety, and for other locations that constitute a significant explosion hazard to these areas, should be identified. Chemical explosions (typically explosions of gas mixtures), boiling liquid expanding vapour explosions induced by fire exposure, oil mist, blast from pressure vessel failure and high energy arcing faults[6] accompanied by rapid air expansion and plasma build-up, should be considered.

4.62. Consequent effects (e.g. the rupture of pipes conveying flammable gases) should be taken into account in the identification of explosion hazards.

Prevention of explosion hazards

4.63. Flammable gases and liquids and combustible materials that could produce or contribute to explosive mixtures should be excluded from compartments (i.e. enclosed areas separated by barriers) that protect items important to safety against other internal hazards. Such flammable gases and liquids and combustible materials should also be excluded from areas adjacent to such compartments or areas connected to these compartments by ventilation systems. Wherever this is not practicable, quantities of such materials should be strictly limited and adequate storage facilities should be provided. Reactive substances, oxidizers and combustible materials should be segregated from each other.

4.64. Vessels containing compressed flammable gases should be securely stored in dedicated compounds that are located away from main plant buildings and provide appropriate protection from local environmental and hazardous conditions.

4.65. Consideration should be given to the provision of automatic systems for the detection of flammable gas releases, for isolation of the gas supply, if possible, and for automatic fire extinguishing systems to prevent a fire induced explosion from affecting items important to safety.

[6] High energy arcing faults are energetic or explosive electrical equipment faults characterized by a rapid release of energy in the form of heat, light, vaporized metal and pressure increase due to high current arcs between energized electrical conductors or between energized electrical components and neutral or ground. Such faults might also result in projectiles being ejected from the electrical component or cabinet of origin and result in fire.

4.66. Hydrogen supply vessels and their distribution manifolds should be placed in well ventilated external locations that are separated from plant areas containing items important to safety. If such equipment has to be placed indoors, it should be positioned in a location that is remote from areas containing items important to safety. Interior storage locations should be provided with a ventilation system designed to ensure that the hydrogen concentration is kept at a safe level below the lower flammability limit in the event of a leak of gas. Hydrogen detection equipment should be provided, and should be designed to give an alarm at a suitably low gas concentration.

4.67. Where turbogenerators are cooled using hydrogen, monitoring equipment should be provided to indicate the pressure and purity of the hydrogen within the cooling system. Provision should be made to purge hydrogen filled components and related systems of pipes and ducts with an inert gas such as carbon dioxide or nitrogen before filling or when draining.

4.68. Each electrical battery room that contains batteries that could generate hydrogen during operation should be provided with an adequate ventilation system such that the hydrogen concentration is kept at a safe level below the lower flammability limit. The layout of the room and the design of the ventilation system should be such as to prevent local accumulations of hydrogen, with or without an operational ventilation system.

4.69. Each electrical battery room should be provided with a hydrogen detection system and ventilation system sensors arranged to provide alarms in the main control room to indicate hydrogen levels approaching the lower flammability limit and any failure of the ventilation system. If fire dampers are installed on ventilation systems serving battery rooms, the effects of their closure on the buildup of hydrogen should be considered. In the event of an alarm, actions should be taken such as stopping the battery charging.

4.70. Consideration should be given to the use of recombinant batteries (i.e. which generate less hydrogen), but it should not be assumed that this will eliminate the risk of hydrogen production.

4.71. The risk of explosions induced by fire exposure, such as boiling liquid expanding vapour explosions, should be minimized by means of separation between potential fires and potentially explosive liquids and gases, or by active measures such as suitable fixed fire suppression systems designed to provide cooling and vapour dispersion.

4.72. The provisions of paras 4.66, 4.67 and 4.77 should be applied, as appropriate, to the storage and use of any other bulk flammable gases. This should include cylinders containing flammable gases used in maintenance and repair work.

Mitigation of the effects of explosions

4.73. Features that can resist or limit explosion effects (e.g. appropriate design or operating provisions) should be in place to minimize risks: examples are limiting the volumes of explosive gas mixtures, inerting, explosion venting (e.g. blow-out panels or other pressure relief devices) and separation of explosion sources from items important to safety. Equipment that needs to maintain its functionality following a postulated initiating event should be identified and adequately designed to withstand the effects of the event, or to be protected against such events.

4.74. Consideration should be given to the blast overpressure and missiles generated by boiling liquid expanding vapour explosions, and to the potential for the ignition of flammable gases at a location distant from the point of release, which could result in the explosion of a gas cloud. The potential for boiling liquid expanding vapour explosions should be minimized by avoiding operation above the superheat limit temperature, as far as practicable.

4.75. Some hazards (e.g. high energy arcing faults), while they are not formally explosions, they are similar to explosions in terms of the loads they impart (e.g. temperature, pressure, missiles) on nearby SSCs; therefore, similar design provisions are appropriate for mitigating the effects of such hazards.

4.76. Design provisions to limit the consequences of an explosion (overpressure, missile generation or fire) should be in place. The consequent effects of postulated explosions on items important to safety should be assessed against the design objectives in para. 2.12. Access routes and escape routes for operating personnel performing manual actions important to safety should also be assessed and special design provisions should be implemented, if necessary.

4.77. Wherever there is a potential hazard due to hydrogen in plant operations, provision should be made to control the hazard by using hydrogen monitors, recombiners, adequate ventilation and controlled hydrogen burning systems (all of which should be designed for use in an explosive atmosphere), or other appropriate means. Where inerting is used, the fire hazard during operation periods without inert gas protection (e.g. maintenance and refuelling) should

be considered, and care should be taken to ensure that gas mixtures remain within the limits of non-flammability.

INTERNAL MISSILES

4.78. Nuclear power plants contain pressurized components and rotating machinery that can fail disruptively and cause missiles. A missile is an object that has kinetic energy and has left its design location. In this Safety Guide, the term internal missile is used to describe a moving object that originated from within the site boundary.

Identification and characterization of missile hazards

4.76. Sources of possible missiles should be identified, and the likelihood, possible kinetic energy, size and trajectory of missiles should be estimated. The possible targets and the effects of missiles on items important to safety should be assessed.

4.77. Analyses of missile hazards are usually performed by a combination of deterministic and probabilistic methods. Some missiles are postulated on a deterministic basis and their effects on SSCs in terms of strikes and damage are also evaluated. A formal description of the deterministic aspects of safety assessment should be presented, even in cases where all aspects of the missile hazard — initiation, strike and damage — are treated probabilistically.

4.78. The potential for secondary missiles that could damage SSCs important to safety should also be evaluated. This evaluation should include consideration of potential fragment ricochet effects, if considered credible on the basis of expert judgement (e.g. the residual energy of the missile following impact can be judged sufficient to induce damage by ricochet when the robustness of targets in the vicinity is considered).

Failure of pressure vessels

4.79. In nuclear power plants, pressure vessels important to safety are designed and constructed by means of extremely comprehensive and thorough practices to ensure their safe operation. Analysis is performed to demonstrate that levels of stress are acceptable under all design conditions. All phases of design, construction, installation and testing should be monitored in accordance with approved procedures to verify that all work is carried out in accordance with the design specifications and that the final quality of the vessel is acceptable. A surveillance

programme during commissioning and operation, as well as a reliable system for overpressure protection should be used to determine whether the vessels remain within their design limits. The gross failure of pressure vessels, such as the reactor pressure vessel or other high quality vessels designed with large margins, is, therefore, generally believed to be sufficiently improbable that consideration of the rupture of these vessels as an internal hazard is not necessary: see IAEA Safety Standards Series No. SSG-56, Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants [9]. Failures of other vessels containing fluids of high internal energy should be evaluated, as they could become sources of missiles and other consequent hazards if they rupture.

4.80. As far as practicable, pressure vessels should be designed to fail in a ductile manner or in such a way that missiles and fragment hazards are reduced. If pressure vessels can possibly fail in a brittle manner, a range of missile sizes and shapes to cover the range of possibilities should be postulated and analysed to identify the missiles that determine the design basis of protective systems or structures. Alternatively, a simplified conservative approach is an acceptable way of determining the missiles to be considered.

Failures of valves

4.81. Valves in fluid systems that operate with a high internal energy should be evaluated as potential sources of missiles.

4.82. Valve bodies are usually designed, constructed and maintained in such a manner that they are substantially stronger than the connected piping. For this reason, it is generally accepted that the generation of missiles resulting from the failure of the valve body itself is sufficiently unlikely and that this need not be considered in the design and/or evaluation of the plant.

4.83. The removable parts of a valve (e.g. stem, valve bonnet, motor) present the most significant potential for failures leading to the production of a missile that should be taken into consideration.

Ejection of a control rod

4.84. For reactor designs in which there is significant fluid pressure in the reactor vessel, it has been customary to postulate the ejection of a control rod due to the driving forces of the fluid. Depending on the particular reactor design, this postulated missile could have the potential to

cause significant primary or secondary damage. Typical concerns include the possible damage to adjacent control rods, to safety systems and to containment structures.

Failure of high speed rotating equipment

4.85. The failure of the main turbine generator set, the steam turbines, large pumps (such as the main coolant pump) and their motors, or flywheels can result in the generation of missiles. Such failures can arise either from defects in the rotating parts or from excessive stresses due to overspeed. Typical missiles include:

(a) Fan blades;
(b) Turbine disc fragments or blades;
(c) Pump impellers;
(d) Fly wheels;
(e) Coupling bolts.

4.86. Rotating machinery usually has a structure surrounding the rotating parts, and consideration should be given to the energy loss after failure due to the energy absorbing characteristics of the surrounding structure or casing. To the extent practicable, the calculation of the energy losses should be based on empirical data from tests of similar structures. For the sake of simplicity, an approach considering the interception of detached rotating parts by the casing could be applied based on operating experience feedback and manufacturer justifications. Alternatively, a conservative approach could be used in which it is assumed that no energy is lost in the interaction of the missile and the casing of rotating machinery.

4.87. Missiles from the failure of rotating machinery should be characterized on the basis of their potential for damage and should be included in the evaluation of possible primary and secondary effects. Having identified the missiles to study, the potential direction of missiles should be characterized in terms of potential targets, taking into account the following:

(f) The maximum range of the missiles will be limited by the available energy and mass.
(g) Consideration of the directions in which missiles could be ejected should help in locating potential targets so as to avoid missile strikes, especially if the missiles are unidirectional (e.g. as for valve stems).
(h) In other cases, there could be a probable plane or angular sector for ejection of missiles, as is the case for rotating machines. There is evidence from failures of rotating machines that

energetic missiles are usually ejected within a very narrow angle of the plane of rotation unless they are deflected by a barrier or stopped by the casing. However, there is also evidence that a small number of missiles could land in a wider angle from the plane of rotation. Therefore, sensitivity studies in relation to the direction of internal missiles, and the effect in terms of the site layout, might be necessary.

Prevention of missile hazards

Prevention of failure of pressure vessels

4.88. Measures to prevent the failure of pressure vessels includes general considerations of the first level of defence in depth, including conservative design and material choices, high quality in construction, and surveillance both in construction and operation. Regarding overpressure, specific measures relevant to pressure vessels include a reliable system for protection (e.g. safety relief valves, and the design of vessel anchors or supports).

Prevention of failure of valves or bolted connections

4.89. Valves should be designed in such a way to prevent removable parts from becoming missiles in the event of their failure.

4.90. As a design rule, no failure of a single bolt should lead to the generation of a missile other than the bolt itself. This recommendation applies to valves, pressure vessels and other bolted components with a high energy content.

4.91. Consideration should be given to the potential for multiple bolt failures due to corrosion or stress corrosion in the event of the leakage of fluid contents past gasketed joints.

4.92. Unless this is precluded by other considerations, removable valve parts should be installed in such a manner that their ejection would not result in an impact of a missile on critical targets.

Prevention of control rod ejection

4.93. The likelihood of a control rod being ejected should be reduced by providing special design features. This should be confirmed by a rigorous development programme to demonstrate that these features have the capability to retain the control rod and the drive assembly in the event of a failure of the travel housing for a control rod.

Prevention of failure of rotating machinery

4.94. Proper orientation of rotating machinery should be considered as a preventative measure for major items such as the main turbine generator, both in terms of the orientation of the main shaft and the overall plant layout. The layout of the main turbine generator should be such that potential critical targets lie within the area least susceptible to direct strikes from missiles generated by turbine failure; that is, within a cone with its axis along the axis of the turbine shaft. This arrangement takes account of the fact that large sections of rotors, if ejected, will tend to be expelled in a direction perpendicular to the rotating shaft. A cone of ejection of 25 degrees either side of perpendicular to the axis has generally been used as there is evidence that the majority of missiles are ejected within this cone; however, the designer should justify any such claim. The arrangement does not eliminate the possibility of such missiles hitting a critical target, but it significantly reduces the probability of a direct strike.

4.95. The following approach should be taken to prevent the failure of rotating machinery:

(a) Careful selection of materials, speed control features and stress margins for all plant states considered in the design basis.
(b) Non-destructive examination and other testing to detect possible defects, and quality control measures to ensure that the equipment as installed meets all specifications.
(c) Evaluation of the reliability of the means of preventing destructive overspeed. This should include equipment for the detection and prevention of overspeed, associated power supply equipment and instrumentation and control equipment, as well as the procedures involved in the periodic calibration and readiness testing of this equipment.

4.96. Additional redundant means of limiting the rotational speed should be provided by such features as governors, clutches and brakes, and by a combination of systems for instrumentation, control and valving to ensure that the likelihood of overspeed occurring is acceptably low.

4.97. Although engineering solutions are available to limit speed and to prevent missiles due to excessive overspeed, these provisions by themselves might not make the probability of missiles being generated from rotating equipment acceptably low. In addition to the failure caused by overspeed there is also the possibility of a flaw in the rotor resulting in missiles being generated at or below normal running speed. These missiles should be addressed by other means, such as conservative design, high quality manufacturing, careful operation, appropriate

monitoring of parameters (such as vibration) and comprehensive in-service inspection. Rotating plant equipment should be maintained and replaced in accordance with manufacturer's instructions. When all these means are properly used, the probability of missiles being generated through the failure of rotating machines can be significantly reduced.

Mitigation of the effects of missile hazards

4.98. Features that can retain energetic missiles resulting from the failure of equipment, or that will deflect such missiles towards a harmless direction, should be considered in the design.

4.99. To control missiles close to their potential source, valves, pumps, motor generators and high pressure gas containers should be located in areas with barriers such as an adequately strong concrete structure. Targets can also be protected by barriers. Barriers are also used to reduce certain secondary effects such as scabbing or the ejection of concrete blocks from concrete targets.

4.100. Usually, missile barriers consist of reinforced concrete slabs or of steel plates. However, other means such as woven steel mats or missile deflectors can also be used.

4.101. In the design of barriers, both local and general effects of missiles on the barriers should be considered, as follows:

(a) Concrete and reinforced concrete barriers:
   (i) The design of concrete barriers should ensure that the barriers will not collapse under the missile impact. Therefore, the thickness and the strength of the barriers should be conservatively defined, consistent with the possible mass, kinetic energy, location of impact and type of missiles (hard missile, soft missile).
   (ii) Elastoplastic, ductile behaviour of the barrier is allowed.
   (iii) The design of the barriers should ensure that hard missiles will not penetrate the barrier.
   (iv) There should be an analysis to ensure that missiles will not cause scabbing or spalling at the safe side of the barrier, and that concrete fragments will not impact SSCs important to safety.
   (v) The generation of secondary missiles from concrete barrier fragments should be avoided by multi-layer or composite barriers.
   (vi) Analysis of the penetration depth, spalling and scabbing phenomena can be performed using empirical formulas or other analytical models as appropriate.

(b) Steel and multi-layer composite barriers:

(i) The design of these barriers should be based on empirical formulas for penetration or other analytical models as appropriate.

(ii) The overall deformation of steel or composite barriers should not result in the loss of barrier function, and the deformed barrier should not impact on the SSCs to be protected.

(c) Vibratory effect:

(i) This vibratory response of the barrier to missile impact should be considered as a secondary effect that could have adverse effect on the SSCs to be protected.

Cases without protection by specific missile barriers

4.102. In some cases, it will not be necessary to provide specific missile barriers. For example, the missiles could be of relatively low mass and energy, and the targets could be sufficiently strong to withstand them, even without additional protection. The boundaries of existing buildings might limit missile effects on the plant. Detailed analysis of the potential impact on the target should be performed to demonstrate that the impact and its potential secondary effects do not affect SSCs important to safety. Physical separation of the redundant safety systems will also ensure that safety functions continue to be performed even if missiles damage components on one or more of the redundant safety systems.

Mitigation of the consequences of missiles due to rupture of pressure vessels

4.103. Modes of failure of a pressure vessel will depend upon a variety of parameters, including the design, the materials of construction, weld details and quality control in manufacture and operating conditions. It is highly unlikely that the vessel as a whole could become a missile especially if it is well restrained. With some vessels, dome end failure might lead to the largest potential missile. Depending on the vessel and operating conditions, a more fragmentary failure could also be possible. To develop protective measures against missiles, attention should be paid in the safety assessment to characterize potential missiles from the particular vessel and the effect of these missiles on plant and structures local to the vessel.

4.104. The provision of an unpressurized guard pipe around certain sections of piping carrying high pressure fluids could, in some cases, be useful for protection against missiles.

Two protection features are provided: protection of the surrounding structures and equipment from whipping pipes and possible secondary missiles, and protection of the inner pipe from missiles generated in the surrounding area. Consideration should be given to the potential for release of fluid from the impacted pipe and the resulting internal flood.

Mitigation of the consequences of missiles due to rupture of valves

4.105. Features that can retain energetic missiles resulting from the rupture of valves, or that will deflect such missiles towards a harmless direction, should be considered in the design. This could include walls or local missile barriers.

Mitigation of the consequences of missiles due to failure of rotating machinery

4.106. Features that can retain energetic missiles resulting from the failure of rotating machinery, or that will deflect such missiles towards a harmless direction, should be considered in the design.

PIPE BREAKS (PIPE WHIP AND JET EFFECT AND FLOODING)

Identification and characterization of pipe breaks

4.107. Depending on the characteristics of the pipes under consideration (internal parameters, diameter, stress values, fatigue factors), the following types of failure should be considered:

(a) High energy pipes[7] can suffer from circumferential rupture or longitudinal through-wall crack, or both. The high energy of the contained fluid means that dynamic effects, such as pipe whip or jet impingement, are important and should be considered.
(b) Low energy pipes can also suffer through-wall cracks, either longitudinal or circumferential, although, given the energy of the fluid, such cracks would generally be more stable than those in high energy pipes, and dynamic effects would be less significant.

[7] In some States, a high energy pipe is defined as a pipe with an internal operating pressure of more than 1.9 MPa or an operating temperature of more than 95°C in the case of water. In other States, these limits are 2.0 MPa and 100°C respectively. Other limits may apply for other fluids, for example gas at greater than atmospheric pressure.

By exception, for low energy pipes, it could be possible to justify limiting the leak size to an area significantly smaller than their inner cross section.

4.108. It may be acceptable to postulate only a limited leak (and not a break), if it can be demonstrated that the piping system considered is operated under 'high energy' parameters for a short period of time[8] (e.g. less than 2% of the total operating time). Some States have identified criteria for excluding certain pipe segments from break analysis (see para. 4.133). Alternatively, an assessment of the consequences assuming a full pipe break can be viewed as a good practice to demonstrate the robustness of the design.

4.109. Failure should be postulated at the following locations:

(a) At the terminal ends (fixed points, connections to a large pipe or to a component) and at welds and intermediate points of high stress for a piping system designed and operated in accordance with the rules applied for safety systems. Other locations of this piping system, where the piping failure would lead to bounding effects on SSCs important to safety, should be verified, possibly using realistic assumptions;
(b) In all locations for other pipes.

4.110. For small[9] diameter piping systems, which are sensitive to vibration-induced failure and to rupture due to external forces, breaks should be postulated at any location.

4.111. A circumferential pipe rupture might result from damage due to a degradation mechanism such as corrosion or fatigue (i.e. a crack growing over its critical size) or an acute overload (e.g. by water hammer or impact due to the rupture of other piping). The most probable location of such a pipe rupture is any circumferential weld between the straight pipe parts and the pipe components such as pipe bends, T intersections, reducers, valves or pumps. In general, pipe rupture should be considered at any location where there are changes in stiffness and vibration or fluid stratification caused by temperature differences.

4.112. The estimated frequency of a double ended guillotine break of high energy piping should be derived from operating experience or from fracture mechanics calculations. This

[8] This approach is considered acceptable only in some States.

[9] Some States have defined 'small' as a pipe with a nominal diameter of 50 mm or less. In other States, pipes with nominal diameter of 25 mm or less are considered small.

frequency might also be available from evaluations made for the purposes of probabilistic safety assessment.

4.113. If longitudinal welds are present in high energy piping, a large longitudinal through-wall crack resulting in a break or large leakage area should be considered.

4.114. Complete instantaneous breaks of high energy pipes should be postulated when analysing local effects on SSCs important to safety, such as direct mechanical contact (pipe whip) or jet impingement including potential blast wave load. Furthermore, the global effects[10] of breaks in these pipes, including consequences such as flooding, increases in humidity, increases in temperature, and higher radiation levels, should be taken into consideration when designing the supports, the protection means (e.g. pipe restraints) and the relevant SSCs important to safety.

4.115. Pipe failures could have an impact on SSCs important to safety by means of the local and global effects described in para. 4.114. All these possible effects should be analysed and considered in the plant design, in particular for protective and mitigatory measures.

4.116. Three main phenomena that could be induced by pipe failures are pipe whip, jet effects and flooding. The first two phenomena are addressed in paras 4.117–4.141, and internal flooding is addressed in paras 4.142–4.169. Secondary effects such as failure-induced missiles and the environmental effects of the break (e.g. local increase in temperature and pressure) are also addressed.

Pipe whip

4.117. Pipe whip in its usual form occurs as a consequence of a double ended guillotine type pipe break in high energy piping. As the free cross sections of the broken pipe are propelled by the forces of the discharging high energy fluid, they are accelerated, which tends to move them from their installed configuration. In the case of sufficiently large movement of the pipe branch, the increasing bending moment could cause plastic deformation and the formation of a plastic hinge at the nearest pipe whip restraint or at a rigid (or sufficiently stiff) support. This defines the length of the pipe branch that rotates coherently about this point during the phase of free pipe whip movement.

[10] In the context of this Safety Guide, 'global effects', refers to possible effects across the entire site.

4.118. For assumed breaks where the full lengths of both pipe segments are at the same elevation, the pipe whip should be assumed to occur only at the same elevation; otherwise, motion in all directions (i.e. a sphere centred on the plastic hinge) should be assumed.

4.119. In the case of a large longitudinal through-wall crack in high energy piping, no classical pipe whip occurs in the vicinity of this break since there is no separation of the pipe. However, large displacements should be considered, on the basis of the assumption that the piping forms a V shape with three plastic hinges and has the potential to affect other nearby equipment.

4.120. The whipping pipe branches should be analysed geometrically to determine possible directions of motion that might endanger target SSCs. In addition, the analysis should include an assessment of the effectiveness of the pipe whip restraints, demonstrating that pipe deflections would be limited by the physical restraints. In the case of terminal end breaks, consideration should be given to the secondary effects on the remaining terminal ends.

4.121. For the analysis of the consequences of an impact, it should be assumed that any impact of a whipping pipe onto a pipe of similar design but smaller diameter results in damage (a break) to the target pipe. Subject to justification, impacted target pipes of a diameter equal to or larger than the impacting pipe need not be assumed to lose their integrity. However, if an additional mass (such as a valve or an orifice plate) is present on the whipping branch, the kinetic energy of the motion is increased. Additionally, the stiffness of the pipe — and therefore its capacity to damage a larger pipe — might increase if there is a change in pipe shape (e.g. an elbow) near the end of the pipe. In these cases, the target pipe could be broken even if it is larger than the whipping pipe. Cables and cable trays and different types of structure and instrumentation should be considered as possible targets if they support systems or components important to safety.

4.122. In the investigation of the whipping pipe, consideration should be given to the potential for a subsequent break after an impact on a target, with the ejection of secondary missiles. Sources of missiles could be single concentrated masses within or attached to a pipe branch, such as valves and pumps. If these components have separate supports that are designed to prevent such breaks and the formation of secondary missiles, the analysis should be extended to these anchor points. Attention should also be paid to instrumentation wells and similar attachments to the pipe as further possible sources of missiles.

Jet effects

4.123. A jet is a stream of fluid ejected from a leak or break in a pressure retaining system, in a particular direction and with a significantly high velocity.

4.124. Jets usually originate from a broken component, such as a pipe or vessel, containing high energy pressurized fluid. Jets can be excluded from consideration for low energy systems.

4.125. The origin of the jet is usually assumed to be a circumferential or longitudinal break of a vessel or pipe. The resulting jet is then limited to a particular direction. In the case of circumferential breaks, the jet is assumed to be orientated axially with respect to the pipe. In the case of longitudinal breaks, the jet is assumed to be oriented radially.

4.126. Other possible sources of jets should be considered, where appropriate. An example of such a source is a jet of gas (the possible effects of the ignition of this gas are considered in paras 4.1–4.77).

4.127. For each postulated location and size of break, the jet geometry (shape and direction) and its physical parameters (e.g. pressure, temperature and density) should be evaluated as a function of time and space.

4.128. If the break generates more than one jet, the possible interference of the jets should be taken into account. This is the case for a double ended break of a pipe without restraints, in which two jets could be generated, one from each of the broken ends of the pipe.

4.129. The effect of the motion of the jet's source (such as a whipping pipe) on the jet's geometry should be taken into account, as well as other possible effects (such as due to objects in the vicinity of the jet's trajectory).

4.130. A conservative analysis, using either an appropriate and verified computer model or a simplified approximation on the basis of experimental data, or other appropriate and justified conservative assumptions, can be used for the analysis of the jet's shape and other properties.

4.131. The following effects of jets on targets should be taken into account: mechanical load (pressure, impact), thermal load (temperature, including thermal stresses and shocks where appropriate) and properties of fluids (such as possible short circuits in electric equipment due to the conductivity of liquid water). Possible chemical effects should also be evaluated, particularly if the fluid ejected is not water.

4.132. It might be necessary to analyse the effects of jets on targets that are not SSCs important to safety if their damage might lead to significant secondary consequences. A typical example is damage to pipe insulation inside containment. Although the insulation itself is not important to safety, debris from insulation material could block the emergency core cooling or containment spray sump strainers during recirculation cooling. Relevant recommendations are provided in paras 4.84 and 4.85 of IAEA Safety Standards Series No. SSG-53, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants [10].

Prevention of pipe breaks

4.133. In some States, it has been judged that the application of very high quality standards for high energy piping, similar to those for vessels, could reduce the risk of pipe breaks to such a low level that it can be effectively excluded from further consideration. Some States have identified criteria for excluding certain pipe segments from break analysis (see, for example, Ref. [11]).

4.134. For locations where break preclusion criteria are met, a leak (rather than a complete rupture) may be assumed.[11] To determine the leak size, a fracture mechanics analysis should be performed. Alternatively, a crack corresponding to a leak size of 10% of the flow cross section should be postulated. The leak detection system should be shown to have a sensitivity that is adequate to detect the minimum leakage from a crack of this size.

4.135. For all piping, the likelihood of a pipe break can be reduced significantly if safety measures are applied, notably for design, manufacturing, construction and surveillance (increased in-service inspections or monitoring for leakage, vibration and fatigue, water chemistry, loose parts, displacements, and erosion and corrosion).

[11] This is applicable in States where the leak-before-break concept has been accepted.

Mitigation of the consequences of pipe breaks

Mitigation of the consequences of pipe whip

4.136. The likelihood of a severe pipe rupture in the piping systems of a nuclear power plant is generally accepted to be low; however, pipe restraints should be used to restrict the motion of pipes that, if broken, could impact SSCs important to safety.

Mitigation of the consequences of jets

4.137. If a high energy pipe does break, the generation of a jet cannot be avoided; the only way to prevent the generation of a jet is to prevent the break itself. However, means of limiting the jet in time and/or space should be considered. For example, valves installed upstream and check valves installed downstream of the point of failure can stop the jet soon after it is initiated. Robust barriers (e.g. concrete walls) around the failed pipe should be used to limit the range of the jet.

4.138. To the extent practicable, coatings and insulation materials that are resistant to jet impingement should be used to limit the amount of debris that is generated by the jet (since this debris can challenge the performance of safety systems under certain conditions).

Specific jet hazard considerations

4.139. In addition to the direct impingement of a jet onto targets (local effects), the release of fluid from a leak or break could also have a significant effect on the general environmental conditions in a room. The effects will depend, among other things, on the time duration and the parameters of the jet and on the dimensions of the room. If this is a concern, then the general environmental parameters and their influence on SSC functionality should also be analysed and included in the environmental qualification process.

4.140. The effect of a differential pressure across a structure or portion of a structure (e.g. a wall), for example due to the steam released by a break, should be considered when designing the plant. Blow-out panels and doors that open when subjected to a certain pressure or temperature are examples of measures that can be used to mitigate this effect.

4.141. Protection against direct jet impingement is similar to protection against missiles. Protective measures should be designed in such a way as to cope with both missiles and jets, or generally with as many internal hazards as practicable.

INTERNAL FLOODING

Identification and characterization of internal flooding hazards

4.142. Internal flooding can be caused by any event that results in the release of a liquid (usually water[12]) that exceeds the drainage capacity in a given area. Flooding can affect multiple SSCs, i.e. that are not designed to withstand being submerged or exposed to spray. Although the guidance in this subsection is limited to internal flooding, external events (e.g. earthquake, external flooding) can cause or exacerbate internal flooding.

4.143. Flooding means not only the formation of pools of water on the floor of a room but also the collection of water in higher locations. For example, water (arising from sprays or condensed steam) could collect in cable trays even if they are located well above the floor level. Equipment located in such a place should then be considered to be subject to flooding. In addition, water from these trays might be drained to other locations where its presence is also undesirable.

4.144. Actions undertaken by plant personnel (e.g. maintenance activities) that can lead to flooding should be considered.

4.145. Examples of events that could cause a flood include the following:

(a) A leak or break of the primary or secondary system;
(b) A leak or break of the emergency core cooling system;
(c) A leak or break of the service water system;
(d) A leak, break, or spurious operation of the fire extinguishing system;
(e) Human error during maintenance (e.g. leaving a valve, an access hole or a flange open by mistake);

[12]This subsection addresses water-based flooding; however, the same considerations apply to other liquids on the site if they exist in sufficient quantities and locations that could cause a flood. Possible examples include fuel, chemicals and fire extinguishing materials.

(f) A leak in piping systems such as domestic water, circulating water, condensate, external backwater through drains.

4.146. All possible flooding hazards should be systematically identified. One approach is to list SSCs and then to identify all the possible sources of water (including sources in other rooms) and systematically identify the flood propagation pathways. This identification should be supported by design drawings and room walk-downs for verification. A three-dimensional model could also be used for verification and validation purposes.

4.147. For all possible flood scenarios, the water level as a function of time should be determined, not only for the room or plant area containing the source of the water but also for all rooms or plant areas to which the water could spread. This should take into account the overall source inventory, discharge rates and means of isolation. Possible inexhaustible water supplies should also be considered. Typical pathways that flood water could traverse include pipe conduits, drains, or openings in walls or floors, stairwells, vents and elevators. Doors are also an important flood propagation pathway.

4.148. Flood water might travel under doors or might damage (e.g. buckle) doors until they fail, if they are not designed to withstand the hydrostatic pressure and/or hydrodynamic loads that might occur. Failure of doors should be modelled in a conservative manner.[13]

4.149. Operating experience has shown that ventilation ducts can drain water to lower levels. Thus, the propagation of water by ventilation ducts should be considered in the design. Examples of effects include water spray on electrical equipment or the submerging of equipment in rooms where there is a ventilation outlet or a low point that might fail.

4.150. In the case of breaks in pipes connected to tanks or pools, siphoning effects, which can increase the amount of water drained, should be considered.

4.151. Possible blocking of drain holes by debris should be taken into account if this would lead to more severe conditions. In determining the water level using a volume–height relationship, the as-built status of the room (including the volume of equipment in the room) should be used.

[13] 'Conservative' depends on whether failure of the door would be advantageous (e.g. by allowing water to flow away from SSCs important to safety) or disadvantageous, (e.g. by allowing water to flow toward SSCs important to safety).

4.152. If the liquid is water, flooding is usually considered to be of concern mainly for electrical devices, which should be assumed to fail if submerged or subjected to spray, unless qualified for these conditions. Cables are generally assumed to be unaffected by being submerged; however, the connection points (e.g. splices) should be assumed to fail when exposed to water unless they are specially qualified.

4.153. Some mechanical equipment might be resistant to the direct effects of water, but relies on electrical support equipment (e.g. for power, instrumentation, control). In such cases, the effects of flooding on this support equipment should be considered. Additionally, the effect of buoyancy should be considered since mechanical equipment might not be designed to withstand an upward force.

Prevention of internal flooding hazards

4.154. Flooding can be caused by the leaking or breaking of a vessel, tank or pipe; therefore, design provisions intended to reduce the likelihood of a leak or a break (see paras 4.133–4.135) should be used to reduce the likelihood of flooding.

4.155. The reduction of human error should be considered as an important way of reducing the likelihood of flooding.

4.156. Engineered features (e.g. sensors) that prevent the overfilling of tanks should be used, where practicable, to limit the likelihood of internal flooding caused by tank overflow.

4.157. Cable trays should be designed in a manner that limits flood propagation. Examples of design features include drainage holes and water tight penetrations.

4.158. To the extent practicable, water tight penetrations should be manufactured from material that is resistant to material degradation, and should be installed in locations that facilitate inspection and maintenance.

4.159. Seals and gaskets whose failure could lead to a flooding event (e.g. condenser seals) should be fabricated from a material that is resistant to material degradation and is robust enough to withstand anticipated loads (e.g. water hammer, seismic events, fire, hydraulic loads). The flow rate from a seal or gasket failure should be conservatively determined on a case-by-case basis.

4.160. The operation of design features such as containment spray systems, fire extinguishing systems, or (if in-vessel melt retention is credited reactor cavity flooding systems, could produce flooding. Such flooding should be given full consideration in the design (e.g. some components of instrumentation and control systems should be accordingly qualified for containment sprays, and some doors and walls should be qualified as waterproof for fire extinguishing sprays). Such intentional flooding might not generally be considered an internal hazard; however, owing to its similar nature, it should be included in the set of internal flooding hazards being analysed.

Mitigation of internal flooding and the effects of internal flooding

4.161. Mitigation of internal flooding should be achieved in part by design choices with respect to the layout of the plant. This includes physical separation of redundant SSCs important to safety, and locating SSCs vulnerable to flooding at elevations higher than the assumed flood levels. For example, SSCs can be located on a pedestal that is higher than the maximum assumed flooding level. If this is not possible, a barrier (either a wall around the component or a complete enclosure) can be used. It should also be ensured (by all available means) that accidental flooding is mitigated as soon as possible, and that the unfavourable spreading of flooding to other areas is prevented (e.g. by means of suitable thresholds). Means that can be used to mitigate flooding include the following:

(a) Appropriate design (e.g. passive flood protection features, isolation valves on drains, pumps and water-tight doors, and on potentially hazardous pipes);
(b) Detection systems (e.g. flood alarms);
(c) Adequate procedures (operational and/or emergency procedures).

4.162. If actions by plant personnel are assumed (e.g. isolation of the source of flooding) the time needed to detect, diagnose and mitigate the consequences of the event should be determined. The environmental conditions in areas where actions are necessary should be evaluated and factored into any assumptions about timing. These considerations should also be factored in when determining human error probabilities. In the deterministic approach, the most limiting single failure should be assumed for detection, diagnosis or mitigatory action (e.g. isolation), and conservative times for plant personnel to complete these actions should be assumed, considering the environmental conditions due to flooding.

4.163. Because some means of flood detection (e.g. sump level) do not offer an indication of the precise location of the leak or break, design features should be implemented to assist plant personnel in identifying the source of internal flooding and/or to automatically mitigate the flooding. Examples include valves that automatically close if environmental conditions indicative of a flood are detected (e.g. elevated room temperature, excessive flow rate), and closed circuit television to allow visual monitoring of flooding conditions. Appropriate, procedures and training should be provided for plant personnel.

4.164. The possible formation and effects of internal flood waves should be taken into account and analysed, if flooding is fast enough (such as in the event of a total breach of a large tank). A wave could increase the local water level significantly above the estimated steady state water level and therefore, a dynamic analysis should be performed. This analysis should evaluate the mechanical loads imposed on SSCs by waves and the potential effects of floating debris on SSCs.

4.165. Drains are an important protective feature against flooding because they limit the rate that water rises during a flood, which provides time for the plant personnel to take appropriate actions. The drain system should be designed with a capacity (i.e. drainage rate) suitable for the internal flooding sources in each plant area. To the extent practicable, the drainage system should be designed in a manner that facilitates inspection and maintenance to limit the likelihood of clogging. Portions of redundant drainage should be independent and not drain into common headers. Administrative controls should be used to ensure that temporary equipment that could clog drains (e.g. plastic sheeting) is not stored in a location in which it could be transported to drains if a flood were to occur. Design provisions (e.g. drains equipped with check valves) should be used to ensure that flood water from one area does not flow backwards causing a flood in another area, thus compromising the segregation of SSCs important to safety.

Specific flooding hazard considerations

4.166. In addition to the direct impacts of flooding (e.g. spray, submergence) as described in this section, the release of water into a room might also have a significant effect on the general environmental conditions. Such effects (e.g. increase in humidity, radiation levels, temperature) should be considered in the qualification process for equipment. Special

consideration should be given to potential releases of dissolved hydrogen in water and to fluids other than water (e.g. chemicals used for fire suppression).

4.167. The design should take into account that water present during an internal flood could impose a hydrostatic load on those SSCs in contact with the water (e.g. doors, walls, floors, penetrations). If not properly accounted for, this could lead to structural failures and damage from falling objects or heavy load drop. It could also lead to failure of barriers and doors important to safety.

4.168. The design of the plant should ensure that potentially contaminated water released during a flooding event does not propagate into the site surface and/or groundwater. One method of achieving this is to ensure that those portions of the building that are below the assumed maximum flood level are leaktight.

4.169. Leakages from systems used in the long term for extracting heat from the containment during severe accidents should be accounted for. These systems should be capable of being isolated, and any radioactive water and gas released should be confined by appropriate means; in particular, a ventilation system qualified to the corresponding ambient conditions should be available.

HEAVY LOAD DROP

4.170. The collapse of structures, or objects falling from heights can be secondary effects either of an internal hazard or of an external hazard such as an earthquake or high winds. They need to be assessed as potential consequences of the initiating internal or external hazards. In turn, falling objects can cause consequent internal hazards; guidance on these combined sequential hazards is given in Appendix I. Paragraphs 4.171–4.183 concentrate on heavy load drop in which no other initiating hazard is necessary.

Identification and characterization of heavy load drop

4.171. Drops are more likely to occur from the handling of plant equipment for maintenance or from fuel handling lifts. If heavy items of plant equipment are located at significant heights, an evaluation should be made of the possible hazards associated with dropping such equipment (i.e. unless the probability of such an event is negligible). The consequences of heavy load

drops should be assessed; these consequences could present a risk to safety in several ways, for example:

(a) As an impact on the fuel (resulting in a risk of radioactive release and potentially a risk of criticality);

(b) As an impact on components of safety systems (risk of failure of systems);

(c) As an impact on structures important to safety (for example, risk of loss of integrity of fuel pools and of release of radioactive material).

4.172. IAEA Safety Standards Series No. DS440, Design of Auxiliary Systems and Supporting Systems for Nuclear Power Plants [12], and IAEA Safety Standards Series No. DS487, Design of Fuel Handling and Storage Systems for Nuclear Power Plants [13] provide recommendations on the design of overhead lifting equipment and fuel handling equipment respectively. Furthermore, IAEA Safety Standards Series No. NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants [14], and IAEA Safety Standards Series No. NS-G-2.6 Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants [15], provide recommendations on seismic design and qualification, and on maintenance, surveillance and in-service inspection, respectively, that together will lead to high integrity lifting systems in operation. Following the recommendations of these publications will reduce the likelihood of dropping heavy equipment as a result of internally initiated events.

4.173. The nature of the object and the cause of the drop should be analysed in order to characterize the possible direction (e.g. from drop, tilting or swinging), size, shape and energy of the falling object and the possible consequences for safety.[14]

4.174. For the purpose of determining the potential consequences, dropped loads associated with fuel handling could be considered in categories such as casks or lids, transfer cask and multipurpose sealed baskets or canisters, fuel and fuel storage racks, and power and hand operated tools. Fuel handling drops constitute a large variety of different scenarios, and each

[14] The following cases are assessed in some States with realistic assumptions: drop of the reactor pressure vessel closure head on the reactor pressure vessel; drop of the reactor cavity cover slab on the reactor pressure vessel closure head (when the slabs above the vessel are removed); and drop of a reactor cavity cover slab on the reactor cavity floor slab.

needs to be considered in the context of the potential radiological consequences and the potential effect on SSCs.

4.175. Another potential category of dropped loads is associated with the movement of containers for radioactive waste. In general, these are likely to contain materials with lower activity levels than fuel casks, but the containers are also less substantial. The general principles of prevention of drops and limiting consequence should also be followed, i.e. in the quality of lifting equipment, the choice of routes and controls to prevent incorrect operation.

Prevention of heavy load drop

4.176. Functional design requirements often govern the physical location of equipment in this category. Where it is functionally necessary to tolerate proximity between heavy equipment and critical targets, it is possible to provide sufficient design measures such as redundant cables on cranes or interlocks to reduce the probability of failure. Guidance on the design of high integrity and single-failure proof cranes is available in Refs [16–19].

4.177. Where practicable, plant layout should facilitate the safe movement of the overhead lifting equipment and of items being transported. In some cases, it might be necessary to handle plant equipment in areas where the layout precludes separation from SSCs important to safety; in such cases, additional care should be taken in the handling of heavy loads in the vicinity of SSCs.

4.178. Measures to prevent dropped loads should include the classification of lifting devices, design measures and administrative measures, as follows:

(a) Classification of lifting devices in accordance with the results of a hazard analysis that evaluates the consequences of a postulated dropped load.

(b) Design measures:

    (i) The general considerations of the first level of defence in depth, including conservative design and material choices, high quality in construction, and surveillance both in construction and operation.

    (ii) Crane zoning and protection schemes, as appropriate, including load cells to monitor lift weights, and interlocks and trips.

(c) Administrative measures:

(i) Procedural controls prevent the lifting of excessive loads, or the inadvertent mishandling of loads (e.g. load snagging, load hold-up, swinging loads).

(ii) Appropriate controls related to the identification of appropriate lift heights and lift routes, and administrative controls to enforce these (e.g. additional supervision). There could also be advantages in local control of a lift such that plant personnel can confirm that there are no snags or holds up and that clearances are adequate for the lift.

(iii) Periodic inspection and maintenance of cranes (e.g. their interlocks, cables and brakes) and associated lifting equipment (nooses and slings, straps and shackles, and related items).

4.179. Prevention of dropped loads in fuel handling is mostly achieved through conservative design measures and appropriate administrative measures. Fuel handling layout and lift routes should be designed to avoid potential drops on SSCs important to safety.

4.180. An additional design objective for the plant layout should be to protect stored fuel or other items important to safety from the drop of heavy equipment or other equipment handled in specific situations that might induce large consequences.

Mitigation of the effects of heavy load drop

4.181. A significant mitigation of risks from dropped loads is provided by scheduling load movements and lifts only in specified modes of plant operation (such as shutdown modes). Such scheduling could be also used as a preventive measure.

4.182. The consequences of heavy load drops can in some cases be reduced by adopting a stepped approach so that the lift is made over intermediate points, by using load following platforms, or by deploying deformable structures at the point of the lift. Protective dampers installed on heavy load could be also used. For example, such protective dampers are used for fuel casks.

4.183. For crane loads associated with fuel handling, such as fuel shipping casks, attention should be paid to the fuel casks since they are massive and the possible consequences of drops affecting the fuel storage pool should be controlled. The impact of concern might be either the fall into the pool, or onto the slabs surrounding the fuel storage pool. This impact should be assessed as potentially compromising the integrity or leak tightness of the storage pools.

Another layout practice that should be considered is to restrict the handling of fuel casks to an area remote from the pool itself and remote from other critical target areas (see DS487 [13]).

ELECTROMAGNETIC INTERFERENCE

4.184. Electromagnetic interference is a term used to describe a number of potential disturbance mechanisms with the potential to affect electrical or electronic devices caused either by electromagnetic conduction or by electromagnetic radiation. If the disturbance is in the high or radio frequency ranges, it is sometimes referred to as radio frequency interference ; in the context of this Safety Guide, electromagnetic interference is used as the generic term.

4.185. Electromagnetic interference hazards can be categorized as internal hazards (for example, caused by induction or radiation from installed equipment, either in normal operation or in fault), or as external hazards (for example, lightning, radiation from solar flares, or from equipment outside the site boundary and operated by other bodies). This Safety Guide addresses internal electromagnetic interference hazards only.

4.186. In many cases, both prevention of the sources of electromagnetic interference and the ability of equipment to withstand electromagnetic interference is addressed by the standards for design and construction of equipment. Further recommendations on these aspects are provided in IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [6], and IAEA Safety Standards Series No. SSG-34, Design of Electrical Power Systems for Nuclear Power Plants [7].

Identification and characterization of electromagnetic interference hazards

4.187. The potential sources of electromagnetic interference should be identified and possible effects from them should be assessed. Significant sources of electromagnetic interference within the control of the operating organisation include motor and generator brush assemblies, and fault current clearance from the operation of switchgears, circuit breakers or fuses; there can also be electric fields caused by radio transmitters. Even flash photography has occasionally affected sensitive control and protection equipment. There is considerable operating experience feedback available that will help designers identify potential electromagnetic interference mechanisms or similar faults. Further recommendations are provided in SSG-39 [6].

4.188. Other potential sources include some maintenance or construction activities, for example portable arc welding equipment and portable radio communications brought into the nuclear plant, and ground penetrating radar used for ground surveys. These potential sources of electromagnetic interference should also be identified and possible effects from these sources should be considered.

4.189. Identification of potential electromagnetic interference hazards should take into account potential sources arising from faults, for example electrical faults from cables with insulation degradation or from transformer bushing insulator breakdown faults.

4.190. The identification process should, where possible, also include the location of sources of electromagnetic interference. This will be relevant when assessing the effects of the interference on the plant.

Prevention of electromagnetic interference hazards

4.191. The nuclear power plant design should include preventative and/or protective measures against the effects of electromagnetic interference. An assessment should be made to determine whether any source of electromagnetic interference on the site could cause malfunction in, or damage to, the nuclear power plant's systems and components, particularly instrumentation. During the plant's operating lifetime, both the presence of new sources and changes in existing sources of electromagnetic interference should be monitored and analysed.

4.192. Electromagnetic interference should be limited such that the functioning of equipment is ensured. Recommendations on minimizing the effects of electromagnetic interference on instrumentation and control components or systems are provided in SSG-39 [6]. This includes a number of techniques, such as the following:

(a) Suppression of electromagnetic noise at the source;
(b) Separation and isolation of instrumentation and control signal cables from power cables;
(c) Shielding of equipment and cables from external sources of magnetic and electromagnetic radiation;
(d) Filtering of electromagnetic noise before it can couple to sensitive electronic circuits;
(e) Neutralization or isolation of electronic equipment from ground potential differences;
(f) Proper grounding of electrical and instrumentation and control equipment, raceways, cabinets, components and cable shields.

Adoption of these techniques can ensure a good level of compatibility between instrumentation and control systems and the sources of electromagnetic interference in the local environment.

4.193. If testing is to be carried out to demonstrate the effectiveness of the protection against electromagnetic interference provided by the design, the equipment under test should be in a state that if it were to operate incorrectly this does not adversely affect safety. The tests should be performed using typical operating parameters (e.g. input signal, output signal, ambient conditions, auxiliary power supply, electrical characteristics).

4.194. Portable sources close to sensitive equipment should be controlled in such a way that SSCs important to safety will not be adversely affected by these sources. This could include a number of measures, such as exclusion zones[15] or other administrative controls. Exclusion zones should be reinforced by physical controls (for example electromagnetic interference detection devices), by administrative controls (such as access arrangements, warning notices, work control systems) and by good safety culture (training, awareness, self-checking, questioning attitude). The choice of approaches to enforce exclusion zones will depend upon the level of reliability that is needed.

Mitigation of the effects of electromagnetic interference hazards

4.195. The consequences of individual component failures on the overall performance of systems or on the overall safety function should be understood.

4.196. As with other internal hazards, good design principles such as redundancy and diversity, separation and segregation should be adopted as they can have a significant effect on reducing the pervasiveness of the electromagnetic interference hazard. In many cases, care in the design over the location of systems or subsystems can have a major effect on the potential overall consequences to system functionality and hence to the performance of safety functions.

Specific electromagnetic interference hazard considerations

4.197. This Safety Guide considers only the 'prompt' effects of electromagnetic interference as an internal hazard. It is possible that standing electromagnetic interference has longer term

[15] An exclusion zone is defined by the minimum distance permitted between the point of installation and where portable emitters of electromagnetic radiation are allowed to be activated.

effects, in terms of induced vibrations and fatigue or galvanic corrosion through eddy current effects. These might have an effect on longer term component or system integrity, but it is assumed that these would be managed by processes intended to maintain the condition of the plant.

RELEASE OF HAZARDOUS SUBSTANCES INSIDE THE PLANT

4.198. Hazardous substances have the potential to disable plant items or systems or to affect personnel carrying out actions important to safety. The potential to release stored hazardous substances or to generate them within the site boundaries is considered as an internal hazard within this safety guide. The release of hazardous material from outside the site or outside the control of the operating organisation should be considered as an external hazard (e.g. chlorine release from road tanker accident). However, some of the recommendations in this Safety Guide could also be relevant.

4.199. The effects of hazardous chemical substances that should be considered in the safety analysis should include the effects due to physicochemical properties (e.g. explosive, oxidizing, flammable) and health-threatening properties (e.g. toxic, irritant, corrosive, anoxic, high temperature).

Identification and characterization of hazards from releases of hazardous substances within the plant

4.200. The inventory of hazardous materials (i.e. quantity, physical and chemical form, type, storage arrangements) within the site boundary should be reviewed to determine what materials, if released, could either affect components of systems important to safety, or cause adverse effects on personnel that might affect their ability to carry out actions important to safety.

4.201. A list of the hazardous substances that could be potentially released should be established by a hazard identification process. These potential releases could come from a variety of differing sources, for example: bulk stored gases, bottled gases, volatile liquids, chemicals used in water chemistry, and releases of chemicals that could mix and form a secondary product, for example as a cloud.

4.202. The list of hazardous substances should be complete and should include any such substances that are brought onto site by sub-contracting companies for maintenance purposes.

4.203. Potential effects of the hazard on plant personnel should be considered. These could include toxic and asphyxiation effects with the potential to disable or otherwise impair plant personnel. Care should be taken to ensure that the release of hazardous substances would not prevent actions by plant personnel to control the incident or to safely shutdown the plant and maintain it in a safe state.

4.204. Potential effects of the hazard on the plant should also be considered. Examples include deposition causing shorting at electrical contacts for instrumentation and control equipment, and the intake of non-combustible gases by diesel generators that might cause them to fail to run. In addition, some plant systems could be affected by the cooling effects of gas clouds. Prompt or short-term potential corrosion effects should be also identified.

Prevention of hazards from releases of hazardous substances within the plant

4.205. Measures to prevent releases of hazardous substances in the first instance include the general considerations of the first level of defence in depth with respect to minimizing the likelihood of a release, including conservative design and material choices, high quality in construction, and surveillance both in construction and operation. Specific measures relevant to releases of hazardous substances will include design of storage tanks, distribution systems and their in-service maintenance.

4.206. Where plant systems or components need to be resilient to the presence of a gas or vapour cloud, the same approach should be followed, i.e. conservative design and material choices, high quality in construction, and surveillance both in construction and operation. In such cases, cabling and electrical control cabinets close to potential releases should be designed and located so as to minimize (consistent with other safety requirements) damage due to the release of gas, water, steam, smoke or hazardous substances.

4.207. As with other internal hazards, adoption of good design principles such as redundancy and diversity, separation and segregation can have a significant effect on the development of hazards from releases of hazardous substances. In some cases, scenarios of concern can be largely eliminated by carefully locating safety systems, i.e. relative to the storage arrangements for hazardous materials.

4.208. Where necessary, the prevention of hazards from releases of hazardous substances should include controls for ventilation systems for plant areas where actions to fulfil safety functions are needed, in particular in control rooms. Control systems should close ventilation intakes, putting the area into a recirculation mode and therefore preventing incapacitating effects on plant personnel performing actions important to safety. Recommendations on the design of the ventilation systems are provided in DS440 [12].

4.209. In the case of releases of chemicals that could mix and form a secondary hazardous product, the preventative measures should include administrative controls over the receipt and storage of such chemicals, and engineering provisions, for example, different hose couplings for acid and alkaline supplies.

Mitigation of the consequences of hazards associated with releases of hazardous substances within the plant

4.210. The design principles of redundancy and diversity, separation and segregation of SSCs important to safety should also mitigate the effects of hazards associated with releases of hazardous substances. Systems that include redundant capability with good segregation or separation should have sufficient redundant subsystems unaffected by the release that their safety functions will be successfully fulfilled even with failures in some of the system components.

4.211. For some plants, the effects of locating the plant within buildings could mean that gas clouds have blown past or reduced in density before significant ingress into the building that might affect the local environment for equipment such as cables and cubicles.

4.212. Accident management might necessitate the provision of personal protective equipment, either to allow plant personnel to escape from environments that are in danger of becoming uninhabitable, or to access plant areas in which important actions have to be carried out, or to continue performing other actions at an endangered location (e.g. for plant personnel in the main control room).

Specific considerations for releases of hazardous substances

4.213. This Safety Guide considers only the 'prompt effects' of the release of hazardous material within the plant. It is possible that smaller continuing releases could cause longer term

effects, for example, in terms of corrosion effects. These might have an effect on longer term component or system integrity, but it is assumed that these would be managed by processes intended to maintain the condition of the plant.

APPENDIX I: HAZARD COMBINATIONS

I.1. Both internal hazards and external hazards can cause other hazards. For example, a seismic event (external hazard) could result in the rupture of a pipe or cause a fire by damaging electrical equipment (internal hazards). Similarly, the drop of a heavy load (internal hazard) might cause an internal flood (another internal hazard) by breaking a pipe or it might generate missiles (internal hazard) by damaging mechanical equipment.

I.2. The effects of these combined hazards (i.e. two or more hazards occurring as a consequence of an initial event, including a hazard) should be considered in the plant's design. The combinations that should be considered depend on the location of the site and the general plant design. Combinations involving a variety of external hazards (natural hazards such as tsunami, blizzard, sand storm, and also human induced ones, such as explosion pressure waves) are not applicable to all sites. Therefore, it is not feasible or necessary to identify a set of hazard combinations that are applicable to all plants.

I.3. A performance-based approach[16] is recommended. This approach, irrespective of the specific methods or criteria being used, should be comprehensive and systematic. The objective is to identify which hazard combinations need to be considered and which design features are necessary to address these combinations. The basis for screening a hazard combination for further consideration, as well as for screening out combinations of hazards, should be clearly defined and documented.

I.4. In principle, three types of hazard combination could be considered:

(a) Consequent (subsequent) events: An initial event, e.g. an external or internal hazard, results in another event, e.g. an internal hazard. Examples are a seismic event and subsequent internal explosion, and internal fire and subsequent internal flooding.

[16] A performance-based approach does not prescribe specific steps that have to be taken, but rather defines a desired outcome and clear, objective, and measurable criteria to determine whether that outcome has been reached. Various methods could be used, provided the desired outcome is reached.

(b) Correlated events: Two or more events, at least one of them representing an internal hazard, which occur as a result of a common cause. The common cause can be any anticipated event including an external hazard, or might be due to an unanticipated dependency. The two or more events connected by this common cause could occur simultaneously[17]. Examples include a tsunami as the common cause for external flooding, internal flooding and internal fire as three potential correlated events, and electromagnetic interference as the common cause for station blackout and internal fire as the two correlated events.

(c) Unrelated (independent) events: An initial event, e.g. an external or internal hazard, occurs independently from (but simultaneously with) an internal hazard without any common cause. Examples are external flooding and an independent internal explosion, and a seismic event and an independent internal fire.

I.5. A hazard combination sequence should be used to determine the loading and magnitude of the hazard, the duration it is applied, and the sequencing of the occurrence of other hazards. For unrelated (independent) events, an identification process should be adopted to include all foreseeable independently occurring hazards, where the second is sufficiently probable that it could occur before the effects of the previous hazard have been completely mitigated. Correlated hazards result from the same basic failure, or other common cause initiator, and the frequencies are related to the cause. Consequent hazards could occur at the same frequency as the initial hazard, or at a lower frequency, depending on the progression of events leading to the subsequent hazards.

I.6. Hazard identification processes could produce a long list of potential combinations; therefore, pragmatic approaches should be used. While combinations involving two (or even more) simultaneous hazards could be postulated, screening criteria should be developed to ensure that the list represents a credible and reasonable set of plant challenges. The screening criteria can be deterministic or probabilistic, or a combination of both. Examples of screening criteria include the following:

(a) The event combination is not credible;

[17] 'Simultaneously' in this case does not mean that the hazards occur exactly at the same time but rather that the second hazard occurs before the effects of the previous hazard have been completely mitigated.

(b) The event combination, even if credible, would not lead to conditions beyond what have already been assumed in the design.

I.7. The desired outcome of this process is a clear understanding of any unique effects of hazard combinations that should be accounted for in the design of the plant. For example, in the case of internal flooding, if the maximum flood level in a room caused by a load drop or missile impact exceeds the assumed flood level caused by a pipe break, additional design measures could be necessary. On the other hand, if analysis shows that existing hazard analysis (based on pipe rupture) predicts a flood level greater than what could be caused by a missile or load drop, no additional design measures would be necessary.

I.8. For each identified hazard combination sequence, the analysis should also consider any deterioration or damage to SSCs important to safety (including hazard barriers) after being subjected to each of the various hazards. For example, for a pipe failure that leads to a missile and a subsequent flood, the analysis of the capability of a hazard barrier to withstand the hydrostatic loads from flooding will need to take account of any damage caused by successive or simultaneous hazards (e.g. the failure of pressurized parts, which could lead to pipe whip, jets, and steam pressure effects on barriers or other SSCs important to safety).

I.9. When considering the likelihood of a hazard combination, it should be noted that the initial hazard might put the plant into a state where the second hazard is more likely than its assumed normal frequency.

I.10. Combined hazards can create unique challenges, even if the hazards occur at different areas of the plant or at slightly different times. For example, a fire in a switchgear room could disable flood isolation equipment: this would create a challenge even if the flood were to occur at a later time or in a different room.

I.11. Following screening, some hazard combinations could be selected to be credible but will still need to be assessed against specific acceptance criteria.

APPENDIX II: DETAILED GUIDANCE ON INTERNAL FIRES

FIRE HAZARD ANALYSIS

II.1. The fire hazard analysis should be developed on a deterministic basis, with the following assumptions:

(a) A fire is postulated wherever fixed or transient combustible material could be present;
(b) Only one fire is postulated to occur at any one time; consequent fire spread should be considered as part of this single event, if necessary;
(c) The fire is postulated whatever the normal operating status of the plant, whether at power or during shutdown.

II.2. The fire hazard analysis should take into account any credible combinations of fire and other events, as described in Appendix I.

II.3. Simultaneous unrelated fires occurring in different fire compartments, in particular, if occurring at a multiple unit site need not be considered in the design of fire protection means; however, the possibility of a fire spreading from one unit to another unit or to another installation on the site, should be taken into account in the fire hazard analysis.

II.4. The fire hazard analysis should have the following purposes:

(a) To identify the type and amount, as well as the location and distribution, of fire loads (fixed and transient) and potential ignition sources over the room or plant area.

(b) To identify the relevant items important to safety and to establish the locations of individual components (e.g. control or power cables) in fire compartments.

(c) To analyse the anticipated growth and the consequences of a fire with respect to the items important to safety. Assumptions and limitations applicable to the methods of analysis should be clearly stated.

(d) To determine the necessary fire resistance rating of fire barriers. In particular, the fire hazard analysis should be used to determine the necessary fire resistance rating of the boundaries of the fire compartments.

(e) To determine the passive and active fire protection means necessary to achieve safety against fire.

(f) To identify cases in which additional fire separation or fire protection is necessary, in particular for common cause failures, so as to ensure that the necessary functions of items important to safety after a fire are not impaired during and following a credible fire. Moreover, in those plant areas where it is not possible to have fire compartments, the fire hazard analysis should be used for determining the extent of the passive and active protection means necessary to separate the fire cells (the fire influence approach).

II.5. The secondary effects of fires and of fire suppression should be evaluated in order to ensure that these effects would not have any adverse effect on safety.

II.6. Detailed guidance on the preparation of a fire hazard analysis is given in Ref. [20].

II.7. The fire hazard analysis should be complemented by fire probabilistic safety assessment, which has been used in many nuclear power plants to identify and rank the risks of fire. Probabilistic safety assessment could also be used in the design phase to support decision making in the deterministic design of plant layout and fire protection systems. Recommendations on the use of probabilistic safety assessment are provided in IAEA Safety Standards Series No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [21].

FIRE BARRIERS

II.8. The overall purpose of fire barriers in nuclear power plants is to provide a boundary around a space (e.g. a fire compartment) with a demonstrated capability to withstand and contain an expected fire without allowing the fire to propagate across to, or otherwise cause direct or indirect damage to, materials or items on the side of the fire barrier not exposed to the fire. The fire barrier is expected to perform this function independently of any fire extinguishing action.

II.9. The fire resistance of fire barriers is characterized by stability, integrity and insulation under fire conditions. The corresponding physical criteria are as follows:

(a) Mechanical resistance;

(b) Capacity to withstand flames, hot gases and flammable gases;

(c) Thermal insulation that is considered satisfactory when the temperature of the unexposed face remains below a prescribed value (e.g. 140°C on average, and 180°C at any one point) over a defined period of time.

The absence of relevant emissions of flammable gases from the face unexposed to the fire should also be verified.

II.10. Passive fire protection systems can be categorized against three performance criteria, depending on their specific function and their potential role in a fire, as follows:

(a) Load bearing capability (stability): The ability of a specimen of a load bearing element to support its test load, where appropriate, without exceeding specified criteria for the extent of deformation, the rate of deformation, or both.

(b) Integrity: The ability of a specimen of a separating element to contain a fire with regard to specified criteria for collapse, freedom from holes, cracks and fissures, and sustained flaming on the unexposed face.

(c) Insulation: The ability of a specimen of a separating element to restrict the temperature rise of the unexposed face to below specified levels.

II.11. Within each of the categories in para. II.10, the fire classification of the components is expressed as a 'rating' (in minutes or hours) corresponding to the period of time for which the components continue to perform their function when subjected to a thermal test programme in accordance with the standards of the International Organization for Standardization (see Ref. [22]) or other relevant standards.

II.12. The specific functions (load bearing capacity, integrity and insulation) and ratings (e.g. 90 min, 120 min, 180 min) of fire barrier elements (e.g. walls, ceilings, floors, doors, dampers, penetration seals) should be specified in the fire hazard analysis.

Fire containment approach

II.13. A fire compartment is a building or part of a building that is completely surrounded by fire resistant barriers: all walls, the floor and the ceiling. The fire resistance rating of the barriers

should be sufficiently high that total combustion of the fire load in the compartment can occur (i.e. total burnout) without breaching the fire barriers.

II.14. Redundant items important to safety should be located in separate fire compartments, in order to implement the concept of segregation, as described in Section 4, and to separate them from high fire loads and other fire hazards. This preferred method is referred to as the 'fire containment approach'. Confinement of the fire within the fire compartment should prevent the spread of fire and its (direct and indirect) effects from one fire compartment to another, and thus to prevent the failure of redundant items important to safety. The separation provided by fire barriers should not be compromised by the effects of fire or fire by-products, or by pressure effects of fires on common building elements such as building services or ventilation systems.

II.15. Since any penetration of a barrier can reduce its overall effectiveness and reliability, such penetrations should be minimized, in particular between different redundant divisions. The fire resistance rating of any devices for closing passages, such as doors, ductwork, hatches, and pipe and cable entryway seals that form part of a fire barrier and a fire compartment boundary should be at least equal to the fire resistance necessary for the fire barrier itself.

II.16. By following the fire containment approach, the provision of fire extinguishing systems to meet the requirements stated in paras 2.1 and 2.2 is not necessary (see also paras 4.30–4.34). Nevertheless, such provisions should be installed where there is a high fire load, as determined by the fire hazard analysis, in order to confine a fire as soon as possible.

II.17. Other design requirements might prevent the full adoption of the fire containment approach throughout the design of a nuclear power plant. This might be the case, for example, in the following areas:

(a) In areas such as the reactor containment and in control rooms of certain designs, where redundant divisions of safety systems could be located close to each other in the same fire compartment;
(b) In areas where the use of structures to form fire barriers could unduly interfere with normal plant functions such as plant maintenance, access to equipment and in-service inspection.

In areas for which individual fire compartments cannot be utilized to separate items important to safety, protection can be provided by locating the items in separate fire cells. This is known

as the ‘fire influence approach’. Figure 1 illustrates applications of the fire containment approach and the fire influence approach.

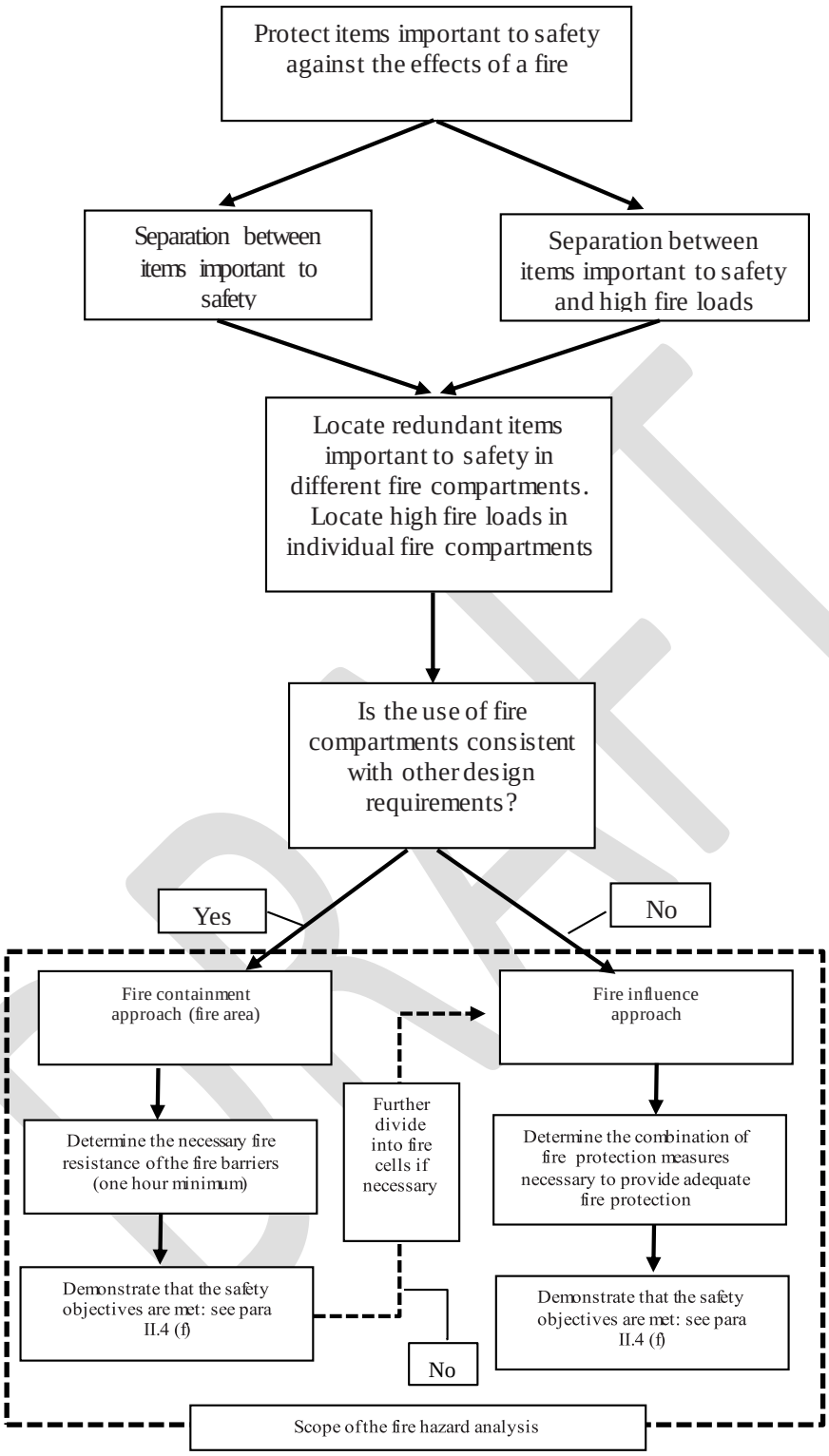

FIG 1 Application of the fire containment approach and the fire influence approach

Fire influence approach

II.18. Fire cells are separate areas in which redundant items important to safety are located. Since fire cells might not be completely surrounded by fire barriers, spreading of fire between cells should be prevented by other means of protection. These means include the following:

(a) The limitation of combustible materials;
(b) The separation of equipment by distance, without intervening combustible materials;
(c) The provision of local passive qualified fire protection such as fire shields or cable wraps;
(d) The provision of fire detection and extinguishing systems.

II.19 Combinations of active and passive means could be used to achieve a satisfactory level of protection; for example, the use of fire barriers (walls, ceilings, floors, doors, dampers, penetration seals and cable wraps) and their fire rating should be specified in the fire hazard analysis together with an extinguishing system.

II.20. The fire hazard analysis should demonstrate that protection measures are sufficient to prevent the failure of redundant items important to safety that are located in separate fire cells.

II.21. Where separation by distance is the sole means of protection between fire cells, the fire hazard analysis should demonstrate that neither radiative nor convective heat transfer effects nor fire by-products would jeopardize the separation.

ACCESS ROUTES AND ESCAPE ROUTES

II.22. Adequate access and escape routes for personnel need to be provided, with account taken of the requirements of national building codes, fire protection regulations and rules for accident prevention, as well as the recommendations of this Safety Guide. Ideally, a minimum of two escape routes from every building should be provided. For each route the following general conditions should be met:

(a) Access routes and escape routes should be protected from the effects of fire and fire by-products. Protected access routes and escape routes comprise staircases and passageways leading to an external exit from the building.

(b) Access routes and escape routes should be kept clear of any stored material.

(c) Fire extinguishers should be placed at appropriate locations along the access routes and escape routes, as required by national regulations.

(d) Access and escape routes should be clearly and permanently marked and should be easy to recognize. The markings of access routes and escape routes and should show the shortest possible safe routes.

(e) The floor level or number should be clearly marked on all staircases.

(f) Emergency lighting needs to be provided on access routes and escape routes.

(g) Appropriate means for raising the alarm (e.g. fire call points) should be available at all places that have been defined in a hazard analysis (i.e. fire hazard analysis), and on all escape routes and building exits.

(h) Access and escape routes should have the capability to be ventilated, by either mechanical or other means, to prevent smoke accumulating and to facilitate access.

(i) Staircases that serve as access routes and escape routes should be kept free of all combustible materials. Overpressure ventilation could be necessary in order to keep the staircase free of smoke. It is advisable to make provision for smoke removal from corridors and rooms leading to staircases. For high multi-storey staircases, consideration should be given to subdividing the staircase.

(j) Doors leading onto staircases or access routes and escape routes should be of the self-closing and latching type and should open in the direction of escape.

(k) Means should be provided to allow quick evacuation of the reactor containment through airlocks. The measures should be adequate to deal with the largest number of personnel expected to be present during maintenance periods and outages.

(l) A reliable communication system should be provided for all access routes and escape routes.

(m) All emergency lighting systems should be energized at all times and should be provided with non-interruptible emergency power supplies.

PROTECTION AGAINST ELECTRICAL CABLE FIRES

II.23. The large inventories of organic insulated electrical cable constitute a significant source of combustible material in nuclear power plants. The impact of electrical cable fires on items important to safety should be determined in the fire hazard analysis.

II.24. Various design approaches have been taken to limit the significant impact of cable fires. Among these approaches are the following:

(a) Protecting electrical circuits against overload and short circuit conditions;
(b) Limiting the total inventory of combustible material in cable installations;
(c) Reducing the relative combustibility of cable insulation;
(d) Providing fire protection to limit fire propagation;
(e) Providing separation between cables from redundant divisions of safety systems, and between power supply cables and control cables.

II.25. Design approaches should be taken to limit the significant impact of cable fires as follows:

(a) Providing fire protection to limit fire propagation;
(b) Providing segregation between cables from redundant divisions of safety systems;
(c) Providing segregation between power supply cables and control cables, as far as practicable. Where segregation is not possible, separation may be appropriate.

II.26. Care should be taken to ensure that cables serving items important to safety are not routed over designated storage areas or other areas of high fire hazard.

Control of cable fires

II.27. Controls should be imposed on the quantities of combustible cable insulation (e.g. polymer insulation) installed on cable trays and within cable routes. These controls are necessary to prevent the fire load exceeding the rated resistance of compartment fire barriers and to minimize the rate of spread of fire along cable trays. The controls should include limits on the numbers and sizes of cable trays and/or the loading of insulation upon them, and should correspond to the combustion characteristics of the cables used.

Cable fire testing

II.28. The qualification tests for fire retardant electrical cables vary across different national standards; however, large scale flame propagation tests for cables often involve vertical or horizontal cable samples exposed to a flaming ignition source. Among the important variable factors associated with cable fire tests are:

(a) The cable inventory as an ignition source;
(b) Cable layout, in particular configurations with multiple cable trays;
(c) Resistance to ignition;
(d) Extent of fire propagation;
(e) Air flow rate;
(f) Thermal isolation of the enclosure;
(g) Toxicity and corrosiveness associated with smoke formation.

Cable fire protection

II.29. In some circumstances, specific passive protection measures should be provided to protect electrical cables from fire. Such measures include:

(a) Cable coatings to reduce the potential for ignition and to delay flame propagation;
(b) Cable wraps to provide segregation from other fire loads and from other systems and/or items important to safety;
(c) Fire stops to limit flame propagation.

Since these measures can lead to overheating of the cable and derating of the current load, these factors should be taken into account in determining the choice of materials to be used.

II.30. The potential impact of cable fires can be reduced by providing suitable segregation using the fire containment approach (see paras II.13–II.17).

II.31. In some cases, physical separation with no intervening combustible materials (alone or in conjunction with fire safety measures) can provide sufficient separation to preclude damage to redundant items important to safety due to a single credible fire. It is not possible to specify a single minimum distance that would provide adequate safe separation for all circumstances,

but rather the adequacy of the separation should be determined by making a careful analysis of the particular situation.

II.32. The preferred approach for the separation of redundant divisions of a safety system should be the fire containment approach.

FIRE DETECTION AND ALARM SYSTEMS

II.33. The nature of the fire detection and alarm systems, their layout, the necessary response time and the characteristics of their detectors, including their diversification, should be determined by the fire hazard analysis or system design requirements.

II.34. The fire detection and alarm systems should provide information in the control room about the location and spread of a fire by means of audible and visual alarms. Local audible and visual alarms, as appropriate, should also be provided in plant areas that are normally occupied. Fire alarms should be distinctive to prevent them being confused with any other alarms in the plant.

II.35. Detection and alarm systems should be functional at all times and should be provided with non-interruptible emergency power supplies, including fire resistant supply cables where necessary. Recommendations on emergency power supplies are provided in SSG-34 [7].

II.36. Individual detectors should be sited so that the flow of air due to ventilation or pressure differences provided for contamination control will not cause smoke or heat energy to flow away from the detectors and thus unduly delay actuation of the detector alarm. Fire detectors should also be placed in such a way as to avoid spurious signals due to air currents generated by the operation of the ventilation system. This should be verified by in situ testing where feasible.

II.37. In the selection and installation of fire detection equipment, account should be taken of the environment in which the equipment will function (e.g. in terms of radiation fields, humidity, temperature and air flow). If the environment does not allow detectors to be placed in the immediate area to be protected (e.g. owing to increased radiation levels or high temperatures), alternative methods should be considered, such as the sampling of the atmosphere from the protected area for analysis by remote detectors with automatic operation.

II.38. Wiring for fire detection systems, alarm systems or actuation systems should be:

(a) Protected from the effects of fire by a suitable choice of cable type, by proper routing, by a looped configuration or by other means;
(b) Protected from mechanical damage;
(c) Constantly monitored for integrity and functionality.

Selection and location of detectors

II.39. The types of fire detector to be installed should be carefully selected, as should their location and positioning, to ensure that the detectors will actuate as expected in response to a fire. Numerous factors affect the response of fire detectors to the growth of a fire, including the following:

(a) Burning rate;
(b) Rate of change of the burning rate;
(c) Characteristics of the burning materials;
(d) Ceiling height;
(e) Positions and locations of detectors;
(f) Locations of walls;
(g) Positions of any obstructions to gas flow;
(h) Room ventilation;
(i) Response characteristics of the detector.

II.40. Analyses should be performed to evaluate the effectiveness of the selected type and locations of the fire detectors.

Fire extinguishing means

Fixed provisions for fire extinguishing

II.41. Nuclear power plants should be provided with fixed fire extinguishing equipment. This should include provisions for manual firefighting, such as fire hydrants and fire standpipes.

II.42. The fire hazard analysis should determine the need to provide automatic extinguishing systems such as sprinklers, spray systems, foam, water mist or gaseous systems, or dry

chemical systems. The design criteria for fire extinguishing systems should be based on the findings of the fire hazard analysis, so as to ensure that the design is appropriate for each fire hazard that is being protected against.

II.43. Fire extinguishing systems need to be designed and located to ensure that their intentional nor their spurious operation does not jeopardize the function of SSCs important to safety (including safety features for design extension conditions).

II.44. Consideration should be given in the design to the potential for errors in the operation of extinguishing systems. Consideration should also be given to the effects of discharges from systems in locations adjacent to the fire compartment where the fire started.

II.45. In the selection of the type of extinguishing system to be installed, consideration should be given to the necessary response time, the characteristics regarding its capability for extinguishing a fire (e.g. thermal shock) and the consequences of operation of the system for plant personnel and for items important to safety, as established by the fire hazard analysis.

II.46. In general, water systems should be preferred in areas containing high fire loads, where there is a possibility of firmly established fires, and where cooling is necessary. Automatic sprinklers, water mist systems, water spray and deluge systems as well as water based foam systems should be used in cable spreading rooms and storage areas, and to protect equipment containing large quantities of oil, such as turbogenerators and oil cooled transformers. Water mist and foam systems are more complex. Water mist has the advantage of discharging smaller quantities of water to achieve control. Gaseous extinguishing systems are usually used in locations containing control cabinets and other electrical equipment susceptible to water damage.

II.47. For prompt operation and availability at the time of a fire, automatic extinguishing systems are preferred. However, provision should be made for the manual actuation of automatic systems. Provision should also be made for manual shut-off of automatic systems, to permit the termination of spurious discharges or the control of water runoff or other side effects.

II.48. The exclusive use of manually operated extinguishing systems should only be acceptable if the evaluation in the fire hazard analysis demonstrates that the anticipated delay in manual actuation would not result in unacceptable damage.

II.49. Any fixed extinguishing system that is solely manually actuated should be designed to withstand fires for a sufficient period of time to allow for the manual actuation.

II.50. All parts, except for the detection devices themselves, of any electrical activation system or electrical supplies for fire extinguishing systems should be protected from fire or should be located outside the fire compartments protected by the systems. Failure of the electrical supply should give rise to an alarm.

II.51. For all fire extinguishing systems, an operational test is usually necessary in commissioning, either by means of actual discharge tests or by the use of equivalent methods.

II.52. A formal maintenance, testing and inspection programme should be established in order to provide assurance that fire protection systems and components function correctly and meet the design requirements. Further recommendations on the implementation of this programme are provided in IAEA Safety Standards Series No. NS-G-2.1, Fire Safety in the Operation of Nuclear Power Plants [23].

Water based extinguishing systems

II.53. Water based extinguishing systems should be permanently connected to a reliable and adequate supply of fire extinguishing water.

II.54. Water based automatic fire extinguishing systems include automatic sprinklers, water spray, deluge, foam and water mist systems. Subject to the findings of a fire hazard analysis, automatic protection should be provided at all locations where one of the following factors applies:

(a) A high fire load is present;
(b) A potential for rapid spread of fire exists;
(c) A fire could compromise redundant items important to safety;
(d) An unacceptable hazard for fire fighters could be created;

(e) An uncontrolled fire would make access for firefighting difficult.

II.55. If the fire hazard analysis indicates that water alone might not be suitable for successfully coping with the hazard (e.g. in the case of application to flammable liquids), consideration should be given to systems using fire extinguishing foam.

II.56. In addition to the expected fire exposure as determined in the fire hazard analysis, various factors should be addressed in the design of water sprinkler systems, such as adequate type and location of sprinkler heads or spray nozzles.

II.57. The component parts of water based systems should be constructed from compatible materials in order to avoid galvanic corrosion.

II.58. Where water based extinguishing systems are used, means should be provided to confine potentially contaminated water, and adequate drains should be provided with arrangements to prevent any uncontrolled release of radioactive material to the environment.

Fire hydrant, standpipe and hose systems

II.59. Reactor buildings should be provided with a fire standpipe and hose system (dry risers).

II.60. The fire hydrant system for the reactor building should have provisions for local or remote actuation.

II.61. The distribution loop for fire hydrants should adequately provide for exterior firefighting operations on all building. Internal standpipes with a sufficient number of fire hoses of sufficient length, and with connections and accessories adequate for the hazard, should be provided to cover all interior areas of the plant, unless duly justified by the fire hazard analysis.

II.62. Each hydrant hose and standpipe riser should have connections that are compatible with on-site and off-site firefighting equipment.

II.63. Suitable accessories such as fire hoses, adapters, foam mixing devices and nozzles should be provided at strategically located points throughout the plant, as identified in the fire hazard analysis. The accessories should be compatible with those of external fire services.

II.64. The fire extinguishing water supply system to each separate building should be provided with no fewer than two independent hydrant points. Each building supply should be provided with an indicating shut-off valve.

Water supply system for fire extinguishing equipment

II.65. The main loop of the water supply system for the fire extinguishing equipment should be designed to supply the anticipated demand for water: see para. II.70. The distribution of water to the fire extinguishing equipment should be through a main loop such that water can reach each connection from two directions.

II.66. Valves should be provided to isolate the water in parts of the main loop. Local visual indications of whether the valves are open or closed should be provided. Valves in the main loop should be so arranged that closure of a single valve should not cause the complete loss of capability of the fire extinguishing system in any given fire compartment, unless this is indicated by the recommendations of the fire hazard analysis. The loop valves for the fire extinguishing water should be located sufficiently far from the hazard against which they are protecting, so as to remain unaffected by a fire in that area.

II.67. The water system for the fire extinguishing system should be used only for fire extinguishing. This water system should not be connected into the piping of the service water or sanitary water systems except as a source of backup supplies of firefighting water or to perform a safety function to mitigate an accident condition. Such connections should be provided with an isolating valve that is locked in the closed position or should be provided with position monitoring during normal operation.

II.68. The fire extinguishing water main loop could serve more than one reactor at a multi-unit site, and common water supplies could be utilized for such installations.

II.69. At sites where pumping is needed to provide the necessary amount of water, fire pumps should be redundant, diverse and separated (i.e. with regard to fire protection) to ensure adequate functionality in the event of equipment failure. Fire pumps should have independent controls, automatic start and manual shut-off, diverse power supplies provided by the plant's emergency power supply and independent prime movers (see SSG-34 [7]). An indication that the pumps are running, together with alarms indicating power failure or failure of the fire

pumps, should be provided in the control room. In areas subject to freezing, a low temperature alarm should also be provided.

II.70. The water supply system for the fire extinguishing system should be designed on the basis of the highest expected flow rate at the necessary pressure for the minimum period of time needed to bring the fire under control. This flow rate, derived from the fire hazard analysis, should be based on the largest water demand for any fixed fire extinguishing system plus an adequate allowance for manual firefighting. In the design of the water supply system for the fire extinguishing system, the minimum pressure at the highest outlet in the plant should be taken into account. Any need to prevent freezing at low temperatures should be taken into account. Consideration should be given to the provision of trace heating or other measures to prevent the freezing of vulnerable pipework.

II.71. Two separate reliable water sources should be provided. If only one water source is provided, then it should be sufficiently large (e.g. a lake, pond or river) and at least two independent intakes should be provided. If only water tanks are provided, two tanks, each capable of providing the entire demand for water for the system, should be installed. The main plant water supply capacity should be sufficient to allow refilling of either tank within a sufficiently short period of time. Tanks should be capable of being interconnected so that pumps can take suction from either tank or both tanks. Each tank should be capable of being isolated in the event of a leak. Tanks should be fitted with fire pump connections.

II.72. When a common water supply is provided for fire protection and the ultimate heat sink, the following conditions should also be satisfied:

(a) The necessary capacity for the water supply for the fire protection system should be a dedicated part of the total water inventory.
(b) Failure or operation of the fire protection system should not affect the water supply for the ultimate heat sink (or vice versa), including for combinations of events.

II.73. Where appropriate, measures to prevent the blockage of the sprinklers or their nozzles by debris, biological fouling or corrosion products should be implemented (e.g. chemical treatment and additional filtration).

II.74. Provision should be made for the inspection of water supply equipment such as filters, end connections, sprinkler heads and spray nozzles. Water flows should be regularly tested by discharge to provide confidence in the continued ability of the system to perform its intended functions throughout the lifetime of the plant. Precautions should be taken to prevent water damage to electrical equipment during testing.

Gaseous extinguishing systems

II.75. Gaseous fire extinguishing systems consist of a gaseous fire suppression agent, a source of compressed gas propellant, an associated distribution network, discharge nozzles and provisions for detection and/or actuation. The systems can be either manually operated at the hazard, or remotely or automatically actuated by a detection system.

II.76. Gaseous extinguishing agents are usually termed clean agents as they leave no residue after deployment. Since they are also non-conductive, their characteristics make them suitable for protecting electrical equipment. Several types of gaseous extinguishing system are available, and more are under development. The advantages of clean agent systems are offset by the need for the concentration of the agent to be maintained, the complexity of the systems, their inability to provide cooling and the single use nature of their operation.

II.77. Carbon dioxide systems, or any other gaseous systems with the potential for causing a hazard to personnel, should never be used to protect areas that are normally occupied.

II.78. There are generally two methods of providing protection with gaseous extinguishing agents: local application, where the agent is discharged towards the hazard or a particular piece of equipment; and total flooding, where the agent is discharged into a fire compartment or into enclosed equipment such as switchgear. Some extinguishing agents are unsuitable for local application.

II.79. Considerations for gaseous fire extinguishing systems are as follows:

(a) In determining the need for gaseous extinguishing systems, consideration should be given to the type of fire, possible chemical reactions with other materials, the effects on charcoal filters, and the toxic and corrosive characteristics of the products of thermal decomposition and of the agents themselves.

(b) Gaseous fire extinguishing systems should not be used where cooling is needed, for example to extinguish firmly established fires, such as those in areas containing a high fire load of electrical cable material. When gaseous agents are used, consideration should be given to the possibility of re-ignition if the concentration of extinguishing medium falls below the minimum necessary level before any residual combustible material has cooled sufficiently.

(c) The total quantity of any gaseous extinguishing agent should be sufficient to extinguish the fire. This is usually accomplished (except for halogenated agents) by means of oxygen dilution. In determining the quantity of agent necessary, account should be taken of the leaktightness of the enclosure, the necessary extinguishing concentration for the hazard, the rate of application and the period for which the design concentration is to be maintained.

(d) To avoid overpressures that would result in structural damage or damage to equipment, the structural effects of the buildup of pressure within protected enclosures resulting from the discharge of gaseous extinguishing agents should be evaluated, and provision should be made for safe venting where necessary. Caution is necessary in selecting venting arrangements so as not to transfer the overpressure or environmental conditions into the relieving area.

(e) Consideration should be given to the potential for damage due to thermal shock when gaseous extinguishing systems are discharged directly onto equipment important to safety. This could occur during local manual applications and during automatic discharges into electrical cabinets. The design should ensure that nozzles are located to avoid fanning the flames of the fire on the initial discharge of the system.

II.80. Suitable precautions should be taken to protect persons who enter a location where the atmosphere might have become hazardous owing to the inadvertent leakage or discharge of carbon dioxide or any other hazardous gas from an extinguishing system. Such precautions include:

(a) Precautions to prevent leakage of carbon dioxide or any other hazardous extinguishing gas in dangerous concentrations to adjacent areas that might be occupied by personnel;

(b) Provision of devices to prevent automatic discharge of the system while personnel are, or could be, within the protected space;

(c) Provision for manual operation of the system from outside the protected space;

(d) Provision of a continuous alarm following the discharge of a gas within the entrances to protected enclosures until the atmosphere has been returned to normal;
(e) Continued operation of the fire detection and alarm system until the atmosphere has been returned to normal (this can help to avoid premature re-entry with the fire still ignited and can protect personnel from toxic gases);
(f) Means to ventilate protected enclosures after the discharge of the gaseous protection system. Forced ventilation is often necessary to ensure that an atmosphere hazardous to personnel is dissipated and not moved to other areas.

II.81. Total flooding applications rely on a rapid and even distribution of gas throughout the space that is flooded. This is usually achieved within 10–30 seconds of actuation by the use of special nozzles and a system designed to proprietary specifications. Rapid distribution of gas is particularly important when the gaseous agent is heavier than air, in order to minimize the stratification of gas within the space and its potentially more rapid leakage.

Dry powder and chemical extinguishing systems

II.82. Dry powder and chemical fire suppression systems consist of a stored quantity of powder or chemical suppression agent, a source of compressed gas propellant, an associated distribution network, discharge nozzles and provisions for detection and/or actuation. The systems can be either manually operated at the hazard, or remotely or automatically actuated by a detection system. These systems are usually used to protect against flammable liquid fires and certain fires involving electrical equipment. These extinguishing agents should not be used on sensitive electrical equipment since they generally leave a corrosive residue.

II.83. The type of powder or chemical agent selected should be compatible with the combustible material and/or the hazard. Special powders should be used to fight metal fires.

II.84. Careful consideration should be given to the use of dry powder systems in possibly contaminated areas, since decontamination following their discharge could be rendered more difficult owing to residues of contaminated powder. The consequential clogging of filters, e.g. ventilation system filters, should also be taken into account.

II.85. The possible adverse effects of using dry powders in conjunction with other extinguishing systems such as foam should be considered; some combinations should not be used.

II.86. Since dry powders do not provide cooling or an inerting atmosphere and only minimally secure the hazard, precautions should be taken to prevent or to reduce the possibility of re-ignition of a fire.

II.87. Dry powder systems are difficult to maintain. Precautions should be taken to ensure that the powder does not compact in its storage container and that the nozzles do not become blocked during discharge.

Portable and mobile fire extinguishing equipment

II.88. Portable and mobile fire extinguishers of a type and size suitable for the hazards being protected against should be provided for use, as necessary, in manual firefighting by plant personnel and external fire fighters. The entire plant should be equipped with a sufficient number of portable and mobile extinguishers of the appropriate type as well as spares or facilities for recharging.

II.89. Fire extinguishers should be placed close to the locations of fire hoses and along the access routes and escape routes for fire compartments. All fire extinguisher locations should be clearly indicated.

II.90. Consideration should be given to the possible adverse consequences of the use of extinguishers, such as cleaning up after the use of dry powder extinguishers.

II.91. In plant areas with potential hazards due to flammable liquids, foam concentrate for firefighting and portable equipment that is suitable for the hazard should be readily available.

II.92. Portable and mobile extinguishers filled with water or foam solution, or other extinguishing agents with a neutron moderating capability, should not be used in locations where nuclear fuel is stored, handled or passes in transit unless an assessment of the criticality hazard has demonstrated that it is safe to do so.

Provisions for manual fire fighting

II.93. Manual firefighting forms an important part of the defence in depth strategy for firefighting. The extent of reliance on on-site and off-site fire services should be established at the design stage. The location of the site and the response time of any off-site fire service will affect the necessary level of provision for manual firefighting. Recommendations on manual firefighting capabilities are provided in NS-G-2.1 [23].

II.94. The design of the plant should allow access by fire teams and off-site fire services using heavy vehicles.

II.95. Suitable emergency lighting and communications equipment should be provided for all fire compartments to support the operation of manual firefighting activities. These should be functional at all times and should be provided with non-interruptible emergency power supplies.

II.96. A fixed wired emergency communication system with a reliable power supply should be installed at preselected stations: see DS440 [12].

II.97. Alternative communication equipment such as two way radios should be provided in the control room and at selected locations throughout the plant. In addition, portable two way radios should be provided for the firefighting team.

II.98. Self-contained breathing apparatus, including spare cylinders and a facility for recharging, should be provided at appropriate locations for use by suitably trained personnel.

II.99. Arrangements for plant equipment and for its storage in the plant should be designed to facilitate access for firefighting, as far as practicable.

II.100. Detailed firefighting strategies should be developed for locations containing items important to safety.

Provisions for venting smoke and heat

II.101. An assessment should be carried out to determine the need for venting smoke and heat, including the need for dedicated smoke and heat extraction systems, to confine the

products of combustion and prevent the spread of smoke, to reduce temperatures and to facilitate manual firefighting.

II.102. In the design of a smoke and heat extraction system, the following criteria should be taken into account: fire load, smoke propagation behaviour, visibility, toxicity, fire service access, the type of fixed fire extinguishing systems used and radiological aspects.

II.103. The necessary capability of the smoke and heat extraction system should be determined from assessments of the smoke and heat released from the postulated fire for the fire compartment. The following locations should have provisions for venting smoke and heat:

(a) Areas containing a high fire load due to electrical cables;
(b) Areas containing a high fire load due to flammable liquids;
(c) Areas containing items important to safety (including safety features for design extension conditions) that are normally occupied by operating personnel (e.g. the main control room).

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, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

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

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2 (Rev. 1), IAEA, Vienna (in preparation).

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

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

[8] AFCEN, EPR Technical Code for Fire Protection, ETC-F 2013, AFCEN Paris (2013).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-56, IAEA, Vienna (in preparation).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY Design of the Reactor Containment and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-53, IAEA, Vienna (in preparation).

[11] UNITED STATES NUCLEAR REGULATORY COMMISSION, Postulated Rupture Locations in Fluid System Piping Inside and Outside Containment, Branch Technical Position 3-4, Standard Review Plan, NUREG-0800, USNRC, Washington DC (2007).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, , Design of Auxiliary Systems and Supporting Systems for Nuclear Power Plants, IAEA Safety Standards Series No. DS440, IAEA, Vienna (in preparation).

[13] 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).

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

[15] 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.)

[16] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder), ASME NOG-1, New York (2015).

[17] UNITED STATES NUCLEAR REGULATORY COMMISSION, Single-Failure-Proof Cranes for Nuclear Power Plants, Office of Standards Development, U.S. Nuclear Regulatory Commission, NUREG-0554, USNRC, Washington DC (1979).

[18] UNITED STATES NUCLEAR REGULATORY COMMISSION, Control of Heavy Loads at Nuclear Power Plants, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, NUREG-0612, USNRC, Washington DC (1980).

[19] BUNDESAMT FÜR STRAHLENSCHUTZ, Design of Lifting Equipment in Nuclear Power Plants, KTA Safety Standard KTA 3902 (2012-11 – corrected version 2014-04-08), KTA Geschäftsstelle, Bundesamt für Strahlenschutz, Salzgitter, Germany (2012).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparation of Fire Hazard Analyses for Nuclear Power Plants, Safety Reports Series No. 8, IAEA, Vienna, (1998).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna, (2010).

[22] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 3941:2007, Classification of fires, (2007).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Fire Safety in the Operation of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.1, IAEA, Vienna (2000). (A revision of this publication is in preparation.)

CONTRIBUTORS TO DRAFTING AND REVIEW

Amri, A.	International Atomic Energy Agency
Bae, Y.B.	Korea Institute of Nuclear Safety, Korea
Berg, P-H.	Federal Office for the Safety of Nuclear Waste Management (BfE), Germany
Bouscasse, M.	Institut de Radioprotection et de Sûreté Nucléaire, France
Eguchi, H.	Nuclear Regulation Authority, Japan
Fong, C.J.	Nuclear Regulatory Commission, United States of America
Kasahara, F.	Nuclear Regulation Authority, Japan
Katona, T.J.	MVM Paks Nuclear Power Plant Ltd., Hungary
Röwekamp, M.	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Germany
Williams, G.	Office for Nuclear Regulation, United Kingdom