IAEA SAFETY STANDARDS

for protecting people and the environment

Step 7a

September 2017

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

1. INTRODUCTION 3
BACKGROUND 3
OBJECTIVE 3
SCOPE 3
STRUCTURE 4

2. GENERAL CONSIDERATIONS 5

3. GENERAL DESIGN RECOMMENDATIONS 7

4. RECOMMENDATIONS FOR SPECIFIC HAZARDS 14
INTERNAL FIRES 14
General 14
Identification and characterisation of fire hazards 14
Fire prevention (prevent fire from starting) 14
Fire mitigation 17
Mitigation of secondary fire effects 20
INTERNAL EXPLOSIONS 25
General 25
Identification and characterisation of explosion hazards 25
Prevention of explosion hazards 25
Mitigation of explosions: mitigate the effects of explosions 27
Mitigation of explosions: limiting the severity of explosions 28
MISSILES 28
Identification and characterisation of missiles hazards 28
Prevention of missiles hazards 31
Mitigation of missiles hazards 33
PIPE BREAKS (pipe whip and jet effect and flooding) 35
Identification and characterisation of pipe breaks 35
Prevention of pipe breaks 40
Mitigation of consequences of pipe breaks 41
Hazard-specific considerations 41
INTERNAL FLOODS 42
Identification and characterisation of internal floods hazards 42
Prevention of internal floods hazards 44
Mitigation of internal floods hazards 45
Hazard specific considerations 46
FALLING OBJECTS / HEAVY LOAD DROP 47
Identification and characterisation of falling objects/ heavy load drop 47
Prevention of falling objects/ heavy load drop 48
Mitigation of falling objects/ heavy load drop 49
ELECTROMAGNETIC INTERFERENCE 50
Identification and characterization of EMI hazards 51
Prevention of EMI hazards 51
Mitigation of EMI hazards 52
Hazard specific considerations 53

RELEASE OF HAZARDOUS SUBSTANCES INSIDE THE PLANT 53
Identification and characterisation of hazards from releases of hazardous substances within the plant 53
Prevention of hazards from releases of hazardous substances within the plant 54
Mitigation of hazard consequences from releases of hazardous substances within the plant 55
Hazard specific considerations 56

5. APPENDIX I: HAZARD COMBINATIONS 57

6. APPENDIX II: DETAILED GUIDANCE ON INTERNAL FIRES 60
Fire Hazard Analysis 60
Fire Barriers 61
Escape and Rescue Routes 67
Protection against Electrical Cable Fires 69
Fire Detection and Alarm Systems 71
Fire Extinguishing Means 73

7. REFERENCES 85

8. CONTRIBUTORS TO DRAFTING AND REVIEW 87

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide, which supplements the Safety Requirements publication on the Safety of Nuclear Power Plants: Design [1], was prepared under the IAEA's programme for establishing Safety Requirements and Safety Guides applicable to land based stationary thermal neutron nuclear power plants.

1.2. This Safety Guide supersedes the Safety Guide on Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, published in 2004 as No. NS-G-1.11 [2], and the Safety Guide on Protection against Fires and Explosions in the Design of Nuclear Power Plants, published in 2004 as No. NS-G-1.7 [3]. This revision principally consists of updating the technical content to make it consistent with the latest Requirements. Internal hazards due to electromagnetic fields or electromagnetic interference, and those due to the release of hazardous substances inside the plant are added in the scope of this safety guide. In the revision process, it was decided to treat in a single Safety Guide all the internal hazards and to provide a single approach to the prevention and mitigation of their effects.

OBJECTIVE

1.3. The objective of this Safety Guide is to provide recommendations and guidance to regulatory bodies, nuclear power plant designers and licensees on design concepts for protection against internal hazards in nuclear power plants. This Safety Guide provides interpretation of the relevant Safety Requirements on Safety of Nuclear Power Plants: Design [1] and recommendations on how to fulfil them.

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

heating or desalination). It is recognized that for other reactor types, including innovative developments in future systems, some parts of this Safety Guide might not be applicable or might need some judgement in their interpretation.

1.5. This Safety Guide covers the design features necessary to protect items important to the nuclear safety of plants against the effects of internal hazards. The following internal hazards are reviewed in this Safety Guide: fires, explosions, missiles, pipe breaks, floods, falling objects/ heavy load drop, electromagnetic interference, and release of hazardous substances inside the plant. This Safety Guide does not cover conventional aspects of protection or the safety of plant personnel, or the protection of property.

STRUCTURE

1.6. Section 2 outlines general considerations for protection against internal hazards in nuclear power plants. Section 3 describes a general common approach for building general design recommendations against internal hazards in nuclear power plants. Section 4 highlights considerations in and provide recommendations for protection against fires, explosions, missiles, pipe breaks, floods, falling objects/ heavy load drop, electromagnetic interference, and release of hazardous substances inside the plant. Two appendices provide further guidance for protection against internal hazards in the design of nuclear power plants.

2. GENERAL CONSIDERATIONS

2.1. The requirement 17 of Ref. [1] states that "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 (PIEs) and generated loadings for use in the design of relevant items important to safety for the plant."

2.2. More specifically, Ref. [1] states in paragraph 5.16 that "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 provide general design recommendations and specific design recommendations respectively to fulfil requirement 17 of Ref. [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. Items important to safety include:

- safety systems for design basis accidents (DBA) and their supporting systems;

- safety features for design extension conditions (DEC) and their supporting systems; and

- the remaining systems important to safety used in normal operation and anticipated operational occurrences (AOO) and which are termed safety related systems.

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

2.6. The hazards caused by the different facilities at the same site are also considered to be internal.

2.7. External hazards can also generate internal hazards (e.g. an earthquake followed by an internal flood).

2.8. Credible combinations of hazards are also considered within the scope of this safety guide.

2.9. Internal hazards have the potential in particular to induce initiating events, to cause failures of equipment needed to mitigate them, and to adversely affect, directly or indirectly, the barriers for prevention of the release of radioactive materials. Internal hazards could, because of their nature, challenge simultaneously more than one level of defence-in-depth and increase, for example, the degree of dependency between the origination of initiating events and the failure of mitigation equipment.

2.10. 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).

2.11. While it is not practical or possible to prevent that an internal hazard triggers an AOO, one of the layout and design objectives is to ensure that internal hazards do not trigger an accident to the extent practicable.

2.12. The aim of considering internal hazards in the design of nuclear power plants is to ensure that the fundamental safety functions are performed in any plant state and that the plant can be brought to a safe shutdown state after any internal hazard occurrence. This implies that:

- The redundancies of the 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;
- The design of individual structures, systems and components (SSCs) is such that accidents induced by internal hazards are avoided to the extent practicable;
- The implemented segregation, separation and protection are adequate to ensure that the modelling of the system response described in the analysis of PIEs is not compromised by the effects of the internal hazard;

- The design is such that a single hazard does not lead to a common cause failure between systems designed to control design basis accidents, and safety features required in the event of accidents with core melting;
- An internal hazard occurring elsewhere in the plant does not affect the habitability of the main control room. In case the latter is not habitable, the access to the supplementary control room is to be ensured. In addition, and when necessary, plant personnel accessibility to equipment in order to perform local actions is to be possible as well.

2.13. In accordance with the defence-in-depth principle (DiD level 1), protection against internal hazards is provided in general by high quality and reliability of SSCs, by environmental qualification of the SSCs, by application of principles of redundancy, diversity, and by spatial separation, segregation, and design of appropriate barriers. Therefore, the design against effects of internal hazard is an iterative process, integrating the needs of protection of several internal hazards. Proper surveillance and in-service inspections should be implemented for early detection of internal hazard occurrences and implementation of necessary corrective actions (DiD level 2) in order to ensure protection against those internal hazards.

-

3. GENERAL DESIGN RECOMMENDATIONS

3.1. Notwithstanding actions and designs to minimize the likelihood of an internal hazard, hazards are possible and the capability of the nuclear power plant to survive internal hazards and to mitigate PIEs caused by them should be an integral part of the design of the plant.

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 important to safety against internal hazards is based on the following major steps:

a) Identification of internal hazards and the possible hazards combinations, and characterisation of the hazard effects,

b) Design for prevention of adverse effects of internal hazards,
c) Design of means for mitigation of adverse effects of internal hazards.

The approach also includes the definition of success criteria of the protections against internal hazards and the verification that these success criteria are met for all hazards of the plant.

3.3. The design of the protections against internal hazards should be conducted taking into account design recommendations for safety and security in an integrated manner in such way that safety and security measures do not compromise each other. Recommendations for security are detailed in [4].

3.4. Certain postulated hazards might be of such magnitude that providing design features to mitigate them is not practicable (e.g., excessive load drop). In this case, the focus is on prevention and an evaluation should be performed to ensure that the likelihood of such events is acceptably low. Even if they cannot be completely mitigated, design measures should be implemented to minimize the consequences of these events to the extent practicable.

Hazard Identification, Characterisation and Hazard Combinations

3.5. During plant design, internal hazards should be identified on the basis of a combination of engineering judgement, deterministic and probabilistic considerations. The identification and the characterisation include the definition of the magnitude and the likelihood of the hazards, the locations of their sources, the environmental conditions produced and the possible impacts on SSCs important to safety. The hazard identification and characterisation process should be rigorous and well documented.

3.6. Possible combinations of internal/internal and internal/external hazards and the secondary/cascading effects should be identified (for example, high energy pipe break, spray, pipe whip). The effects of combined hazards should be considered in the design of the plant.

The combinations that should be considered depend heavily on site characteristics[1] and the general plant design.

3.7. The list of the combined hazards that should be considered in the design should be developed and the screening should be justified.

3.8. As stated earlier, the identification of hazards includes assumptions about their characteristics. Bounding or conservative assumptions should be made about these characteristics in order to address uncertainty.

3.9. The design basis for items important to safety should specify the necessary capability, reliability and functionality for conditions arising from internal hazards that they need to withstand. The relevant internal hazards should be identified, and effects and environmental conditions created by these hazards have to be defined for the design and layout of the plant.

3.10. More details on hazard combinations are provided in Appendix I.

Prevention of the effects of the hazards

3.11. A few hazards may be eliminated either because they are physically impossible (e.g., heavy load drop if there is no lifting equipment) or by a very high quality design (e.g., double ended guillotine break if the pipe is designed for 'leak before break').

3.12. Measures, including administrative ones, should be implemented to reduce the frequency and potential magnitude of the hazards and their effects on SSCs. This objective is mainly achieved by reducing as much as practicable the potential sources of hazards (e.g., limitation of use of combustible materials and presence of ignition sources) and by location and layout (e.g., orientation of fast rotating machines), surveillance and in-service inspections.

[1] For example, some combined 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.

Mitigation of the effects of the 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 depend on the type of hazard and on the specific technical solutions of the design. In general, the mitigation also includes specific measures for detection of occurrence of respective hazard.

3.14. The design features for protection from the effects of internal hazards should be safety classified in accordance with IAEA Specific Safety Guide SSG-30 [5]. The safety classification of protective design features should be commensurate with the consequences of their failure.

3.15. Mitigation measures can be passive, active or by procedure implementation. Passive design solutions – without moving parts and external energy supply – are generally considered to be preferable compared to the active measures or procedure implementation.

3.16. Active protective features can be used. When applicable, the worst single failure should be assumed for these active protective features.

3.17. The consideration of failure of a passive component is not necessary, provided that it is justified that its failure is very unlikely.

3.18. If it is feasible, the early detection of the occurrence of internal hazards is an effective measure for mitigation of the possible consequences.

3.19. Mitigation (including limitation) 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 on the level of:

- plant layout, separating for example the emergency diesel generators, or

- building layout, reducing for example the missile hazard by proper orientation;.

- rooms and compartments, separating the high-energy systems by barriers, forming of fire compartments or cells, and on the level of SSCs, separating for example cables of different safety trains.

3.20. Qualitatively, the layout and design provisions that are protecting the relevant SSCs important to safety from the effects of internal hazards should be such that the objectives of paragraph 2.12 are met.

3.21. The reliability of internal hazards detection and mitigation means should be consistent with their role in providing defence-in-depth.

Assessment, verification and success criteria

3.22. For the judgement on the adequacy of the design, qualitative and/or quantitative success criteria should be defined in consistence with the objectives of paragraph 2.12.

3.23. An assessment is made to demonstrate that those internal hazards relevant to the design of the nuclear power plant are considered, that provisions for prevention and mitigation are designed with sufficient safety margins to cover the uncertainties in the identification and characterisation of internal hazard effects, as well as for avoidance of cliff-edge effects.

3.24. It should be a goal of the design that a single internal hazard does not trigger an accident, unless it can be considered by itself as a postulated accident (pipe rupture for instance); if that cannot be achieved, the designer should justify that the boundary conditions of 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 DECs should be designed for the loads, conditions and durations necessary in these scenarios (e.g., effects of hydrogen combustion). These design features should be protected against the consequences of an internal hazard occurring before DEC has been completely mitigated[2]. Best estimate design loads, conditions and durations can be used for the design of these protective features.

3.26. Deterministic safety analyses, supplemented if applicable by probabilistic analyses, should be performed for the justification of the adequacy of the design of the protection

[2] In some Member States, an independent fire is postulated to break out at least two weeks after a DEC

against internal hazards. The design should be an iterative process accounting for the results of safety analyses.

3.27. Internal hazards considered in the deterministic safety analyses, for a specified location in the NPP, could be classified in four categories associated to three approaches in the hazard assessment (see Appendix I):

- internal hazards independent of AOO and accidents;

- internal hazards which could trigger an AOO;

- internal hazards resulting from an accident without significant fuel degradation;

- internal hazards resulting from a DEC with core melting.

3.28. In the case of an internal hazard independent of AOO and accidents, the assessment should demonstrate that the plant can be brought to, and maintained in, a safe shutdown state in spite of a single failure and equipment unavailability due to preventive maintenance. In practice, a functional analysis is needed to demonstrate that enough redundant systems remain available to reach and maintain that safe shutdown state.

3.29. The assessment of internal hazards which could trigger an AOO should be performed to demonstrate that the plant can be brought to, and maintained in, a safe shutdown state in spite of a single failure and equipment unavailability due to preventive maintenance. However, a specific transient analysis is not needed as this is provided by the corresponding AOO analysis. The analysis of the internal hazard is, in this case, limited to a functional analysis which should demonstrate that an adequate number of functions is provided by the design to control the AOO.

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 the systems credited in the accident analysis, are not affected by the considered internal hazard. The rules applied to DBA and the rules considered for DEC without significant fuel degradation [6] should be applied in the assessment of internal hazards resulting from DBA and from DEC without significant fuel degradation respectively.

3.31. For the deterministic assessment of an internal hazard triggered by a DEC with core melting, it should be demonstrated by using the corresponding rules [6] that the boundary conditions, in particular the systems credited in the accident analysis, are not affected by the considered internal hazard. In practice, it should be demonstrated that the SSCs needed to maintain the containment integrity are not affected by the hazard.

Specific aspects (e.g., multi-unit sites)

3.32. In the construction or operation of a multi-unit and/or multi-source power plant, steps should be taken to ensure that an internal hazard in a unit and/or radioactive source under construction or in operation would not have any safety consequences for a neighbouring operating unit or source (e.g., spent fuel pool). Temporary separations should be used if necessary to protect the operating units.

3.33. The main control rooms should be adequately separated from possible sites of internal hazards as far as applicable. Consideration should be given to the possibility of internal hazards involving facilities shared between units (para. 5.63 of Ref. [1]).

3.34. 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.

3.35. Additional guidance on assessment and verification of specific internal hazards is given in Section 4.

4. RECOMMENDATIONS FOR SPECIFIC 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. Since fire can be assumed to occur in any plant area where combustible materials are present, design measures for fire prevention should be applied to all the fixed and transient fire loads. Such measures include minimization of fixed fire loads, prevention of accumulation of transient combustible materials and control or (preferably) elimination of sources of ignition.

4.2. The design of fire prevention measures should commence 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 (FHA) of a plant site should be carried out to demonstrate that the overall safety objectives are met. In particular, the fire hazard analysis should determine the necessary fire resistance rating of fire barriers and the fire detection and extinguishing capabilities (see detailed recommendations in Appendix II).

4.4. The fire hazard analysis should be carried out early in the design phase and documented. It should be updated before initial loading of the reactor fuel and kept up to date during plant operation.

Fire prevention (prevent fire from starting)

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

a) Minimization of fixed and transient (temporary) fire loads as far as reasonably practicable, and

b) Elimination of potential ignition sources to the extent practicable or their strict control.

Minimize fire loads

4.6. In order to reduce the fire load to the extent possible and minimize 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 air filters and filter frames of non-combustible or low combustible construction materials;

c) The use of a protected pipe or double pipe design for lubricating oil lines and 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 reasonably practicable.

f) The use of non-combustible materials in electrical equipment such as switches and circuit breakers, and in control and instrumentation cubicles;

g) The use of non-combustible scaffolding and staging materials.

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

4.8. 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.

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

4.10. Systems containing flammable liquids or gases should be designed with a high degree of integrity in order to prevent leaks. They should be protected from vibration and other destructive effects. 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.

Minimize ignition sources

4.11. The number of ignition sources should be minimized in the design to the extent possible.

4.12. 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.

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

4.14. Systems and equipment should be made safe through design so as not to provide any ignition source as far as reasonably practical, separated from combustible materials, insulated or enclosed. For example, electrical equipment should be selected and classified for occupancy conditions. 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.

4.15. Cables should be laid on trays, installed conduits or placed in other structurally acceptable made out of non-combustible materials, for example steel that 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 [7, 8].

Fire mitigation

Fire mitigation: detect and extinguish quickly those fires that do start

4.16. Fire detection and fire extinguishing means should be provided, with the necessary systems and equipment being defined by the fire hazard analysis. These systems and equipment should be designed to provide a timely alarm in the event of fire, and/or its speedy extinguishing in order to minimize the adverse effects on items important to safety and to plant personnel.

4.17. Active and passive fire protection means that need to maintain a functional capability (their integrity and/or their functional capability and/or their operability after a postulated initiating event) despite the effects of the postulated initiating event should be identified, adequately designed and qualified.

4.18. Active and passive fire protection means that do not need to maintain a functional capability following a postulated initiating event should be designed and qualified such as not to fail in a way that threatens nuclear safety.

4.19. Stationary (fixed) fire extinguishing systems should be automatically actuated where necessary, and systems should be designed and located so as to ensure that their rupture or spurious operation does not significantly impair the capability of SSCs important to safety to fulfill their required safety function, and does not simultaneously affect redundant parts of safety groups, thereby rendering ineffective the measures taken to meet the ‘single failure’ criterion.

4.20. 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.

4.21. The control of fire is achieved through a combination of fixed fire suppression and extinguishing systems 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 performances of those systems should be designed taking into account the single failure criterion. The application of the single failure criterion is described in paras 5.39–5.40 of Ref. [1].

(b) Where fire detection systems or fixed fire extinguishing systems are relied upon as protection against a potential fire following another 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 inadmissibly impair the required safety functions.

4.22. The reliability of fire detection and extinguishing systems should be consistent with their role in providing defence-in-depth and with the recommendations given in Ref. [7].

4.23. 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.

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

4.25. There should be annunciation of the actuation of any automatically actuated fire extinguishing system to avoid adverse effects on the function of those SSCs important to safety required after a fire.

4.26. 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 be detrimental to the plant, operation 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.

Fire mitigation: prevent the spread of those fires which have not been extinguished

4.27. Early in the design phase, the plant buildings should be subdivided into fire compartments as far as reasonably practicable and, where that is not possible, at least into fire cells.

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

4.29. Non-combustible construction materials should as far as reasonably practicable used throughout the plant and in particular in locations such as in the reactor containment and the control room. If that is not possible, at least fire retardant and heat resistant materials should be used.

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

4.31. The concept of sufficient segregation of redundant parts of safety systems ensures that a fire affecting one division of a safety system would not prevent the execution of the safety function by 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 should be minimized and qualified.

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

Mitigation of secondary fire effects

General

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

4.34. The main objectives in mitigating the effects of a fire are therefore:

- To confine the flame, heat and smoke in a limited space within the plant to minimize spread of the fire and consequential effects on the surrounding plant;
- To provide safe escape and access routes for personnel;
- 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;
- To provide the means for venting of smoke and heat either during or following a fire, if necessary;
- To control the spread of the extinguishing agents to prevent damage to items important to safety.

Layout of buildings

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

4.36. Adequate escape and rescue routes for the firefighting teams or field plant personnel should be provided and these should be protected. The routes should be free from combustible materials. The layout of buildings should be arranged to prevent the propagation

of fire and smoke from adjacent fire compartments or cells to the escape or access routes. Details are given in Appendix II.

Ventilation systems

4.37. 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.

4.38. Each fire compartment containing a redundant division of a safety system should have an independent and fully separated ventilation system. Parts of the ventilation system (e.g., connecting ducts, fan rooms and filters) that are situated outside the fire compartment should have the same fire resistance rating as the compartment or, alternatively, the fire compartment penetration should be isolated by rated fire dampers.

4.39. 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.

4.40. 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 the release of radioactive materials. Passive and active means of protection should be provided to protect charcoal filter banks from fire. Such measures could include:

- Locating the filter in a fire compartment.

- Monitoring of the air temperature and automatic isolation of the air flow.

- Provision of automatic protection by means of a water sprinkler to cool the outside of the filter vessel (see Appendix II).

- Provision of a suitable extinguishing system inside the charcoal vessel. In designing a water-based extinguishing system for that purpose, it should be recognized that if the flow rate of the water is too low, the reaction between overheated charcoal 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.

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

- Filter banks should be separated from other equipment by means of adequate fire barriers.
- Appropriate means (e.g., upstream and downstream dampers) should be used to protect the filters from the effects of fire.
- Fire detectors, carbon monoxide gas sensors (preferably after the filters) or temperature sensors (before the filters) should be installed inside the ducts before and after the filter bank.

4.42. The intakes for the fresh air supply to the fire compartments should be located in 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

4.43. 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 where the designed fire loads, fixed or transient, are minimized.

4.44. Consistent with safety, the design should provide for fire venting in fire compartments containing radioactive materials. Although venting can result in the release of radioactive material to the outside environment, it can prevent, directly or through the improvement of conditions for fire extinguishing, the ultimate release of larger quantities of radioactive material. Two cases should be distinguished:

(1) The possible release can be shown to be well below the acceptable doses defined by the regulatory body.

(2) The amount of radioactive material in the fire compartment can make possible a release exceeding the acceptable limits as defined by the regulatory body. In this case a provision should be made for isolating the ventilation or closing fire dampers. In each case monitoring of the vented air should be performed.

4.45. Design measures should be taken to keep the amount of radioactive material released as low as reasonably achievable. The design should include provisions for monitoring the condition of filters in order to assist plant personnel in taking operational decisions.

Layout and systems for electrical equipment

4.46. Cabling for redundant safety systems should be run in individual specially protected routes, preferably in separate fire compartments, and cables should not cross between redundant divisions of safety systems. As outlined in Appendix II, para. II.20, 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.

4.47. All possible fire induced failures that could affect redundant systems performing safety functions should be analysed by electrical circuit analysis, including multiple spurious actuation. Electrical circuit should be rerouted or protected by combinations of qualified fire rated barriers, fire extinguishing systems with justifications made in the fire hazard analysis.

Special locations

4.48. The main control room of a nuclear power plant could contain the equipment of different safety systems in close proximity. Particular care should be taken to ensure that non-combustible material is used in control rooms for all 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. Additional compensatory protection means should be provided as appropriate.

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

4.50. 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 placed in a fire compartment separate from the one containing the main control room, and its ventilation system should not be a common system shared with the main control room. The separations between the main control room, the supplementary control room and their associated ventilation systems should be such as to meet the intent of para. 2.12 after any postulated initiating event such as a fire or explosion.

4.51. 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.

4.52. 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. The oil collection systems should be capable of collecting oil and water from all potential leakage points or discharge points and draining them to a vented container or another safe location.

4.53. 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 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 the operational requirements.

4.54. The safety features for DEC necessary in the long term should be protected against the effects of a fire, as it is a rather frequent event.

4.55. Equipment sensitive to fire of the systems used for extracting in the long term the heat from the containment during severe accidents should be redundant and located in different fire compartments.

4.56. The equipment of the ventilation systems used in the long term during severe accidents to confine radioactive material should be redundant and located in different fire compartments. Their charcoals should be isolatable and a suitable extinguishing system inside their vessel should be available.

INTERNAL EXPLOSIONS

General

4.57. 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 atmospheres.

Identification and characterisation of explosion hazards

4.58. Explosion hazards should be identified within buildings and compartments separating redundant items important to safety, and for other locations that constitute a significant explosion hazard to these areas. Chemical explosions (typically explosions of gas mixtures), explosions induced by fire exposure and high energy arcing faults (HEAF) accompanied by rapid air expansion and plasma build-up should be considered.

4.59. Consequential effects or consequential events (e.g., the rupture of pipes conveying flammable gases) should be taken into account in the identification of explosion hazards.

Prevention of explosion hazards

4.60. 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) protecting items important to safety against other internal hazards and also from areas adjacent to them or connected to them by ventilation systems. Wherever this is not practicable, quantities of such materials should be strictly limited, adequate storage

facilities should be provided and reactive substances, oxidizers and combustible materials should be segregated from each other.

4.61. Cylinders of 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.

4.62. Consideration should be given to the provision of automatic systems for the detection of fire and flammable gases and of automatic fire extinguishing systems to prevent a fire induced explosion from affecting items important to safety in other buildings.

4.63. Hydrogen supply cylinders or special containers for hydrogen and their distribution manifolds should be placed in well ventilated external locations separated from the plant area containing items important to safety. If placed indoors, the equipment should be positioned on an outside wall and separated from areas containing items important to safety. Interior storage locations should be provided with a ventilation system designed to maintain the hydrogen concentration to values significantly below the lower flammable limit in the event of a leak of gas. Hydrogen detection equipment should be provided to give an alarm at suitably low gas concentration levels.

4.64. 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.

4.65. Each electrical battery room that contains batteries which could generate hydrogen during operation should be provided with a separate ventilation exhaust arranged to discharge directly to the outside of the building so 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.

4.66. The electrical battery room should be provided with a hydrogen detection system and ventilation system sensors arranged to provide alarms in the 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.

4.67. Consideration should be given to the use of recombinant batteries to replace lead acid cells. Recombinant batteries generate less hydrogen, but it should not be assumed that this will eliminate the risk of hydrogen production.

4.68. The provisions of paras 4.69–4.70 and 4.73 should be applied, as appropriate, to the storage and use of any other bulk flammable gases used in plant operation. This should include cylinders containing such flammable gases that might be used in maintenance and repair work.

Mitigation of explosions: mitigate the effects of explosions

4.69. If an explosive atmosphere cannot be avoided, appropriate design or operating provisions should be in place to minimize the risks: the limitation of the volumes of explosive gases, the elimination of ignition sources, adequate ventilation rates, the appropriate choice of electrical equipment designed for use in an explosive atmosphere, inerting, explosion venting (e.g., blow-out panels or other pressure relief devices) and separation from items important to safety. Equipment that needs to maintain its functionality following a postulated initiating event should be identified and adequately designed and qualified.

4.70. The risk of explosions induced by fire exposure such as boiling liquid expanding vapour explosions (BLEVEs) should be minimized by means of separation between potential fire exposures and potentially explosive liquids and gases, or by active measures such as suitable fixed fire suppression systems designed to provide cooling and vapour dispersion. Consideration should be given to the blast overpressure and missiles generated by BLEVEs, 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.

4.71. Some hazards (e.g., HEAF) do not meet the formal definition of an “explosion” yet they act like explosions in terms of the loads they impart on nearby SSCs (e.g., temperature, pressure, missiles); therefore, similar design provisions are appropriate for mitigating them.

Mitigation of explosions: limiting the severity of explosions

4.72. Design provisions to limit the consequences of an explosion (overpressure, missile generation or fire) should be in place. The consequential effects of postulated explosions on items important to safety should be assessed against the objectives of para. 2.12. Escape and rescue routes for operating personnel should also be assessed. Special design provisions should be made if necessary.

4.73. Wherever there is a potential hazard due to hydrogen in plant operations, provisions should be made to control the hazard by the use of hydrogen monitors, recombiners, adequate ventilation, controlled hydrogen burning systems, equipment designed for use in an explosive atmosphere or other appropriate means. Where inerting is used, fire hazards arising during non-inert gas protected operation periods (maintenance and refuelling) should be considered, and care should be taken to ensure that gas mixtures remain within the limits of non-flammability.

MISSILES

4.74. Nuclear power plants contain pressurized components (e.g., pipe work, valves, pressure vessels and housing of control rods) and rotating machinery (e.g., turbine-generators, diesel generators, pumps, fans, blowers, compressors etc.) that can fail disruptively and cause missiles with destructive kinetic energy for the surrounding SSCs.

Identification and characterisation of missiles hazards

4.75. Sources of possible missiles should be identified; the frequency, the possible magnitude of kinetic energy and the likely size and trajectory of missiles should be estimated. The possible targets and their effects on items important to safety should be assessed.

4.76. 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 the SSCs in terms of strikes and damage are also evaluated. A narrative form of the deterministic aspects of safety cases should be presented even in cases when all aspects of the missile hazard — initiation, strike and damage — are treated probabilistically.

4.77. The potential for secondary missiles should also be evaluated.

Failure of pressure vessels

4.78. In nuclear power plants, pressure vessels important to safety are designed and constructed by means of extremely comprehensive and thorough practices. 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 such vessels (including the reactor pressure vessel) is therefore generally assumed to be sufficiently improbable that the rupture of these vessels is ruled out from the design [9].

4.79. Failures of other (non-safety related) vessels containing fluids of high internal energy should be evaluated, as they could become sources of missiles if they rupture.

4.80. If the vessel 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 acceptable in order to determine the missiles to be considered.

Failures of valves

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

4.82. Valve bodies are usually constructed 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 in most cases and that it need not therefore be considered in the design and/or evaluation of the plant.

4.83. The removable parts present the most significant potential for failures that lead to the production of a missile that should be taken into consideration.

Ejection of a control rod

4.84. For reactor designs in which significant fluid pressure is contained by the reactor vessel, it has been customary to postulate, the ejection of the control rod due to the driving

forces of the fluid contained. This postulated missile could, depending on the particular reactor design, have the potential for causing significant primary or secondary damage. For example, typical matters of concern include the possible damage to adjacent control rods, to safety systems and to the containment structures.

Failure of high speed rotating equipment

4.85. The main turbine generator set, the steam turbines, large pumps (such as the main coolant pump) and their motors, and flywheels in the event of their failure can be converted into translational kinetic energy of rotor fragments. Such failures can arise either from defects in the rotating parts or from excessive stresses due to overspeed.

4.86. Since rotating machinery usually has a structure surrounding the rotating parts, some 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 relationships developed in tests of similar, carefully defined structures. For the sake of simplicity, a conservative approach is often 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 doing damage and should be included in the evaluation of possible primary and secondary effects.

4.88. Typical missiles postulated to be caused by the failure of high speed rotating equipment should include:
(a) Fan blades;
(b) Turbine disc fragments or blades;
(c) Pump impellers;
(d) Fly wheels;
(e) Coupling bolts.

4.89. Having identified the missiles to study, the potential direction of missiles should be characterised by potential targets identified.

- The maximum range of the missiles is limited by the available energy and mass.

- Consideration of the directions in which missiles from a particular source could be ejected should help in locating potential targets so as to avoid missile strikes-especially if the missiles are unidirectional, as for valve stems.
- In other cases there could be a most probable plane or angular sector, as is the case for missiles from 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 of some kind (e.g., casing) at the source.

Prevention of missiles hazards

Prevention of failure of pressure vessels

4.90. Prevention of failure of pressure vessels include the general considerations of Level 1 of the defence-in-depth scheme, including conservative design and material choices, high quality in construction, and surveillance both in construction and operation. Specific measures relevant to pressure vessels include a reliable system for overpressure protection (e.g., safety relief valves, and the design of vessel anchors or supports).

Prevention of failure of valves

4.91. Valve stems should be designed with features to prevent valve stems from becoming missiles in the event of their failure.

4.92. 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.

4.93. 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 gasketted joints.

4.94. Unless this is precluded by other considerations, valve stems should be installed in such a manner that the ejection of the stem or of related parts would not result in an impact of a missile on critical targets.

Prevention of control rod ejection

4.95. The likelihood of a control rod being ejected should be reduced by providing special

design features. These features should be confirmed by a rigorous development programme to demonstrate that they have the capability to retain the control rod and drive assembly in the event of a failure of the travel housing for a control rod.

Prevention of failure of rotating machinery

4.96. Proper orientation of rotating machinery should be considered as a preventative measure for major items of rotating machinery 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 the turbine; 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 close to the normal to the rotating shaft[3]. The arrangement does not eliminate the possibility of their hitting a critical target, but it significantly reduces the probability of a direct strike.

4.97. The following approach should be taken to prevent failure of rotating machinery:
(a) Selection of materials, speed control features and stress margins for all plant states considered in the design basis;
(b) Nondestructive examination and other testing to detect possible defects, and for the adequacy of the quality control measures taken to ensure that the equipment as installed meets all specifications;
(c) Means of preventing destructive overspeed should be evaluated for reliability. 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 all these.

4.98. 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 reduce the probability of overspeed occurring to an acceptable level.

[3] Historically, a cone of ejection of 25 degree either side of the normal to the axis has been used as there is evidence that the vast majority of missiles are ejected in this cone but the designer should justify any such claim.

4.99. It should be noted that while 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. Besides the failure caused by overspeed there is the possibility of a flaw in the rotor resulting in missiles being generated at or below normal running speed. These missiles should be dealt with by other means, such as conservative design, high quality manufacturing, careful operation, appropriate monitoring of parameters (such as vibration) and comprehensive in-service inspection. 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 missiles hazards

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

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

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

4.103. Design of barriers requires the consideration of both local and general effects of missiles on the barrier.

- *Concrete/reinforced concrete barriers*
    - Design of the 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 according to the possible mass, kinetic energy, location of impact and type of missiles (hard missile, soft missile).
    - Elastoplastic, ductile behavior of the barrier is allowed.
    - The design of the barriers should ensure that the hard type missile will not penetrate the barrier.

- It should be analyzed and ensured that the missile will not cause scabbing at the safe side of the barrier and the concrete fragments will not impact SSCs important to safety.
- Generation of the secondary missiles from concrete barrier fragments should be avoided by multi-layer or composite barriers.
- Analysis of the penetration depth, spalling and scabbing phenomena can be performed using empirical formulas.

- *Steel and composite barriers*
  - Steel and multi-layer composite barriers are also applicable. The design of these barriers should be based on the empirical formulas for penetration.
  - The overall deformation of the 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.
- *Vibratory effect*
  - The impact of the missile at the barrier causes vibratory response of the barrier structure. This vibratory response of the barrier should be considered as secondary effect that could have adverse effect on the SSCs to be protected.

Cases without protection by specific missile barriers

4.104. 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 intervening protection. The boundaries of existing buildings might limit missile effects to local 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 prevent the safety requirements from being met. Physical separation of the redundant safety systems will also ensure that the general safety requirements are met even if missiles damage components on one or more of the redundant safety systems.

Mitigation of missile consequences due to rupture of pressure vessels

4.105. Modes of failure of a pressure vessel will depend upon a variety of parameters including the design, the materials of construction, weld details, quality control in

manufacture, etc. 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 most massive potential missile. Depending on the vessel and operating conditions, more fragmentary failure could also be possible. To develop a safety case against missiles, attention should be paid to characterize potential missiles from the particular vessel and the effect of the missiles on plant and structures local to the vessel.

4.106. 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 obtained: 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 relapse of fluid from the impacted pipe and the resulting internal flood.

Mitigation of missile consequences due to rupture of valves

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

Mitigation of missile consequences due to rupture of rotating machinery

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

PIPE BREAKS (PIPE WHIP AND JET EFFECT AND FLOODING)

Identification and characterisation of pipe breaks

4.109. 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) For high energy pipes (except for those qualified for break preclusion) circumferential rupture or longitudinal through-wall crack.

(b) By exception, for low energy pipes[4], it could be possible to justify limiting the break size to that of a leak with limited area.

4.110. It is 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 (e.g., less than 2% of the total operating time) or if its nominal stress is reasonably low (e.g., a pressure of less than 50 MPa).

4.111. 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 according to the rules applied for safety systems;

(b) In all locations for other pipes.

4.112. For small[5] diameter piping systems, breaks should be postulated at all locations because they are sensitive to vibration-induced failure.

4.113. A circumferential pipe rupture might result from damage by a degradation failure mechanism such as corrosion or fatigue (i.e., a crack growing over its critical size) or an acute stress such as 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, where there are changes in stiffness and vibration or fluid stratification caused by temperature differences.

---

[4] A low energy pipe is defined as a pipe with an internal operating pressure of less than 2.0 MPa or an operating temperature of less than 100°C in the case of water. Other limits could apply for other fluids, for example gas at greater than atmospheric pressure.

[5] Some member states have defined "small" as a pipe with a nominal diameter of 50 mm or less.

4.114. The frequency of a double ended guillotine break of high energy piping should be derived from operating experience or fracture mechanics calculations. This frequency might also be available from evaluations made for the purposes of probabilistic safety assessment.

4.115. A large longitudinal through-wall crack in high energy piping resulting in a break or large leakage area should be considered if longitudinal welds are present.

4.116. Complete instantaneous breaks of high energy pipes should be postulated. The consequences of breaks in these pipes include flooding and increases in pressure, humidity, temperature, radiation, and debris generation. These effects should be taken into consideration when designing relevant SSCs important to safety.

4.117. Pipe failures could have an impact on SSCs important to safety by means of local effects, such as direct mechanical contact (pipe whip) or jet impingement, as well as global effects, such as flooding, increases in humidity, increases in temperature, asphyxiant effects and higher radiation levels. These possible effects should be analysed.

4.118. Three main phenomena that could be induced by pipe failures — pipe whip, jet effects and flooding — are discussed in the following sections. Secondary effects such as failure-induced missiles and the environmental effects of the break (e.g., local increase in temperature and pressure) are also discussed.

Phenomenon of pipe whip

4.119. The phenomenon of pipe whip in its classical form can occur only 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.

4.120. For assumed breaks where 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 centered on the plastic hinge) should be assumed.

4.121. 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.

4.122. 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.

4.123. 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 than the impacting pipe in general results in damage (a break) to the target pipe. 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 should be considered as possible targets if they support systems or components important to safety.

4.124. 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 or heavy form parts. If these components have separate supports by design 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.

Phenomenon of jet effects

4.125. 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.

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

4.127. The jet's origin 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.

4.128. 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 its burning are considered in the section on internal fire).

4.129. For each postulated location and size of a break, the jet geometry (shape and direction) and its physical parameters (pressure and temperature) should be evaluated as a function of time and space[6].

4.130. If the break generates more than one jet, the possible interference of the jets should be taken into account. An example of this situation is the 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.

4.131. 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 objects in the vicinity of the jet's trajectory).

4.132. 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 properties.

---

[6] One example of this approach is ANSI/ANS-58-2-1988

4.133. 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 other than water.

4.134. It might be necessary to analyse the effects of jets on targets that are not SSCs if their damage might lead to significant secondary consequences. A typical example is damage to pipe insulation inside containment. Although the insulation could not itself be 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 paragraphs 4.81 and 4.82 of Ref. [10].

Prevention of pipe breaks

Preclusion and prevention of pipe breaks

4.135. Very high quality standards for high energy piping should be applied in order to reduce the likelihood of pipe failures. Some member states have identified criteria for excluding certain pipe segments from break analysis[7].

4.136. For locations where break preclusion criteria are met, a leak (rather than a complete rupture) may be assumed. To determine the leak size, a fracture mechanics analysis should be performed. Alternatively, a subcritical 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 that is just subcritical.

4.137. For all piping the probability of a pipe break can be reduced significantly if additional safety orientated measures are applied, such as surveillance measures (increased in-service inspections or monitoring for leakage, vibration and fatigue, water chemistry, loose parts, displacements, and erosion and corrosion).

[7] see, for example, NUREG-0800, U.S. NRC Branch Technical Position 3-4.

Mitigation of consequences of pipe breaks

Mitigation of consequences of pipe whip

4.138. 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

4.139. Once a high energy pipe or vessel has broken, 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.

4.140. 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 safety system performance under certain conditions).

Hazard-specific considerations

4.141. 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.

4.142. The effect of a differential pressure across a structure or portion of a structure (e.g., a wall) due to the steam released by a break should be considered when designing the plant. Blow-out panels or fusible doors (i.e., a normally shut door that opens when subjected to a certain pressure or temperature) are examples of measures that can be used to mitigate this effect.

4.143. 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 possible.

INTERNAL FLOODS

Identification and characterisation of internal floods hazards

4.144. Internal flooding can be caused by any event that results in the release of a liquid, usually water[8] that exceeds the capacity of the evacuation in a given area. Flooding is a concern because it can simultaneously disable multiple SSCs that are not designed to be submerged or exposed to spray. Although the guidance in this section is limited to internal flooding, it should be recognized that external events (e.g., earthquake, external flooding) can cause or exacerbate internal flooding.

4.145. In a general sense, 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 undesired locations.

4.146. Plant personnel actions (e.g., maintenance activities) that can lead to flooding should be considered.

4.147. Examples of events that could cause a flood include but are not limited to:

(a) A leak or break of the primary or secondary system;

(b) A leak or break of the emergency core cooling system;

[8] This section discusses water-based flooding but the same considerations apply to other materials on site if they exist in sufficient quantities and locations that could cause a flood. Possible examples include but are not limited to fuel tanks, chemical tanks, and fire extinguishing materials

(c) A leak or break of the service water system;

(d) A leak, break, or spurious operation of the fire water system;

(e) Human error during maintenance (e.g., leaving a valve, an access hole or a flange open by mistake).

4.148. All possible flood 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. This identification should be supported by room walk-downs for verification.

4.149. For all possible flood scenarios, a water level as a function of time should be determined not only for the room or plant area with the source of the water but also for all rooms or plant areas to which the water could spread. Typical pathways that flood water could traverse include pipe conduits, drains, or openings in walls or floors, stairwells, vents, elevators. Doors are also an important flood propagation pathway.

4.150. Flood water might travel under doors or might fail (buckle) doors if they are not designed to withstand the hydrostatic pressure present. Failure of doors should be modeled in a conservative manner. “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).

4.151. 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.

4.152. 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.

4.153. 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 relation, the as-built status of the room (including the volume of equipment in the room) should be used.

4.154. 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 subject to spray, unless

qualified for these conditions. Cables are generally assumed to be unaffected by submergence; however, the connection points (e.g., splices) should be assumed to fail when exposed to water unless they are specially qualified.

4.155. Mechanical equipment could not be directly affected by water but often relies on electrical support equipment (e.g., power, instrumentation, control) and the effect 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 floods hazards

4.156. 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 (as discussed in paragraphs 4.136-4.138) should be used to reduce the likelihood of flooding.

4.157. The reduction of human error is another important way to reduce the likelihood of flooding.

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

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

4.160. To the extent practicable, penetrations that are required to be water tight should be designed out of material that is resistant to material degradation and should be installed in locations that facilitate inspection and maintenance.

4.161. 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 event, fire, hydraulic loads). The flow rate from a seal or gasket failure should be conservatively determined on a case-by-case basis.

4.162. Sometimes intentional flooding is a design feature, and flooding phenomena should

then be given full consideration in the design.

Mitigation of internal floods hazards

4.163. Mitigation of internal flooding should be achieved in part by design choices with respect to the plant's layout. This includes physical separation of redundant SSCs important to safety and by 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 spreading to unfavourable regions is prevented (e.g., by means of suitable thresholds). Means that can be used to mitigate flooding include:

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

4.164. If plant personnel actions are assumed (e.g., isolation of the flood source) the required time to detect and diagnose and mitigate the event should be determined. If ex-control room actions are required, the environmental conditions in areas where actions are needed should be evaluated and factored into any assumptions about timing. These considerations should be factored in when determining human error probabilities (HEPs). In the deterministic approach, the most limiting single failure should be assumed for detection or isolation and conservative plant personnel action times should be assumed.

4.165. Because some flood detection means (e.g., sump level) do not offer indication as to the precise location of the leak or break, design features should be implemented to assist plant personnel in identifying the source of internal flood and/or to automatically mitigate the flood. 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 TV to allow visual identification of flooding conditions. Procedures and training should be provided to plant personnel.

4.166. The possible formation of 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 value predicted on a steady state basis and therefore, a dynamic analysis should be performed. This analysis should also evaluate the mechanical loads imposed on SSCs by waves.

4.167. Drains are an important protective feature against flooding because they limit the rate that water rises during a flood, which provides time to 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. Administrative controls should be used to ensure that temporary equipment that could clog drains (e.g., plastic sheeting) is not stored in a location that could transport to drains were a flood to occur. Check valves should be used to ensure that flood water from one area does not travel backwards through a drain, causing a flood in another area.

Hazard specific considerations

4.168. 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, temperature) should be considered in the qualification process for equipment.

4.169. The design should account for the fact 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 materials. It could also lead to failure of barriers and doors important to hazard protection.

4.170. The design of the plant should ensure that potentially contaminated water released during a flooding event does not propagate into the site groundwater. One method of achieving this goal is to ensure that those portions of the building that are below the assumed maximum flood level are leak-tight.

4.171. Leakages of the systems used for extracting in the long term the heat from the containment during severe accidents should be accounted for. They should be isolatable and the 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.

FALLING OBJECTS / HEAVY LOAD DROP

4.172. Falling objects or structure elements caused by external events such as earthquakes or high winds will be covered under the relevant external hazards. The potential for consequential internal hazards following these drops will follow the guidance given for combined consequential hazards in Appendix I of this guide.

Identification and characterisation of falling objects/ heavy load drop

4.173. 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, if the probability of this event is not negligible. The consequences of load drops should be assessed, and these could present a risk for the safety in several ways:

a. as an impact on the fuel (risk of release of radioactive material and potentially of criticality),

b. as an impact on components of safety systems (risk of failure of systems),

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

4.174. References [11] and [12] provide recommendations on the design of overhead lifting equipment and fuel handling equipment respectively. References [13] and [14] give guidance on seismic design and qualification and on maintenance, surveillance and in-service inspection which together will lead to high integrity systems lifting in operation. Following the recommendations of these documents will reduce the likelihood of dropping heavy equipment as a result of internally initiated events.

4.175. The nature of the object and the cause of its dropping should be analysed in order to

characterize the possible direction, size, shape and energy of the falling object and their possible consequences for safety[9].

4.176. 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 basket or canister, fuel and fuel storage racks, and power and hand operated tools. Fuel handling drops constitute a large variety of different scenarios, and each needs to be considered in the context of the potential radiological consequences and the potential effect on SSCs.

4.177. Another potential category of dropped loads would be associated with the movement of radioactive waste containers. In general these are likely to contain materials with lower specific 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 over mal-operation.

Prevention of falling objects/ heavy load drop

4.178. 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. There is international guidance on design of high integrity and single-failure proof cranes[10] .

4.179. Where practicable, plant layout should permit 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 layout precluded separation from SSCs, additional care should then be taken in the handling of heavy loads in the vicinity of SSCs.

4.180. Prevention of dropped loads should include the classification of lifting devices,

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

[10] For example, ASME NOG-1, NUREG-0554, NUREG-0612

design measures and administrative measures:

- Classification of lifting devices according to the results of a hazard analysis that evaluates the consequences of a postulated dropped load from the considered lifting device.
- Design:
    - The general considerations of Level 1 of the defence-in-depth scheme, including conservative design and material choices, high quality in construction, and surveillance both in construction and operation.
    - Crane zoning and protection schemes, as appropriate, including load cells to monitor lift weights and interlocks/trips.
- Administrative measures:
    - Controls over lifts to prevent the lifting of excessive loads, or the inadvertent mishandling of loads (e.g., load snagging, load hold-up, swinging loads).
    - Appropriate controls over lifts related to the identification of appropriate lift heights and lift routes. Administrative controls to enforce these (e.g., additional supervision or "banksman"). There could also be advantages in local control of a lift such that the plant personnel can confirm that there are no snags or holds up and that clearances are adequate for the lift.
    - Attention should be paid to the periodic inspection and maintenance of cranes (e.g., their interlocks, cables and brakes) and associated lifting equipment (nooses/slings, straps and shackles, and related items).

4.181. Prevention of dropped loads in fuel handling is largely down to conservative design measures and appropriate administrative measures. Fuel handling layout and lift routes should be designed to avoid potential drops on SSCs related to key safety functions.

Mitigation of falling objects/ heavy load drop

4.182. A significant mitigation of risks from dropped or falling loads is by scheduling load movements and lifts only in specified plant states such as shutdown states.

4.183. Large drops can in some cases be reduced in consequence by adopting a stepped

approach so that the lift is over intermediate points, by load following platforms, or by deformable structures at the point of the lift.

4.184. In the particular case 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 pools 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.

4.185. An additional design objective for plant layout should be and to protect stored fuel or other safety related items from any dropped loads.

ELECTROMAGNETIC INTERFERENCE

4.186. Electromagnetic Interference (EMI) is a term to describe a number of potential disturbance mechanisms with the potential to affect electrical or electronic devices caused either by electromagnetic induction or by electromagnetic radiation. If the disturbance is in the high or radio frequency ranges, it is sometimes referred to as Radio Frequency Interference (RFI), but in the context of this document, EMI is used as the generic term.

4.187. EMI hazards can be categorised as internal hazards (for example, caused by induction or radiation from installed equipment, either in normal operation or in fault), or as external hazard (for example, radiation from solar flares, or from equipment outside the site boundary and operated by other bodies). There are also potential security related aspects (deliberate introduction of high energy sources of radiation or electromagnetic induction). This document only addresses the internal hazards aspect of EMI.

4.188. In many cases, both prevention of the sources of EMI and the ability of equipment to withstand EMI is addressed by the standards for design and construction of equipment. Further guidance on these aspects is given in [7, 8].

Identification and characterization of EMI hazards

4.189. The potential sources of EMI should be identified. Significant sources of electromagnetic interference within the control of the operating organisation include fault current clearance from the operation of switchgears, circuit breakers or fuses; there could also be electric fields caused by radio transmitters[11]. There is considerable operating experience feedback available which will help designers identify potential EMI mechanisms. Further information is available in [7].

4.190. Other potential sources include some maintenance or construction activities, for examples portable arc welding equipment, portable radio communications or telephony brought into the nuclear plant, and ground penetrating radar used for ground surveys.

4.191. Identification of potential EMI hazards should account for potential sources during maintenance or faults, for example electrical faults from cables with insulation degradation or from transformer insulator breakdown faults.

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

Prevention of EMI hazards

4.193. 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 either on-site or off-site could cause malfunction in, or damage to, the nuclear power plant's systems and components, particularly instrumentation.

4.194. Guidance is available for minimising the effects of EMI on I&C components or systems [7]. This includes a number of techniques such as:

[11] Natural sources such as lightning strike or solar storms; and other human induced sources external to the plant are considered as external hazards

- Suppression of electromagnetic noise at the source;
- Separation and isolation of I&C signal cables from power cables;
- Shielding of equipment and cables from external sources of magnetic and electromagnetic radiation;
- Filtering of electromagnetic noise before it can couple to sensitive electronic circuits;
- Neutralization or isolation of electronic equipment from ground potential differences;
- Proper grounding of electrical and I&C equipment, raceways, cabinets, components and cable shields.

Adoption of these techniques has the potential to give a good level of compatibility between I&C systems and the potential EMI sources in their local environment.

4.195. If testing is to be carried out to demonstrate the efficacy of the protection against EMI provided by the design, the equipment under test needs to be in a state that if it were to mal-operate this does not result in a threat to nuclear safety.

4.196. Portable sources close to sensitive equipment should be controlled. This could include a number of measures, such as exclusion zones or other administrative controls. Exclusion zones should be reinforced by physical controls (for example EMI 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 required level of reliability.

Mitigation of EMI hazards

4.197. The consequences of individual component failures on the overall success or failure of the system or on the overall safety function should be understood.

4.198. 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 EMI hazard. In many cases, care in design over choice of the location of systems or subsystems can have a major effect on the potential overall consequences to system functionality and hence to the nuclear safety risks.

Hazard specific considerations

4.199. This safety guide only considers the "prompt" effects of EMI as an internal hazard on the overall safety case for the nuclear power plant. It is possible that standing EMI has longer term 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 plant.

RELEASE OF HAZARDOUS SUBSTANCES INSIDE THE PLANT

4.200. Toxic and corrosive materials and gases 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.

4.201. Release of hazardous material affecting the plant originating from outside the site or the control of the operating organisation is considered as an external hazard. However some of the considerations in this safety guide could also be relevant. Examples of these external hazards would include gas clouds from facilities operated by other companies neighbouring the site, or for example, chlorine release from a road tanker accident on neighbouring roads.

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

4.202. Identification of the materials holdings (i.e. quantity, physical and chemical form, type, storage arrangements) within the site boundary should be performed 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. The identification needs to account for material storage locations, and the routes followed by distribution means and delivery vehicles, as the location of potential releases will be important to an understanding of the subsequent hazard.

4.203. These potential releases could come from a variety of differing sources, for example:

- Bulk stored gases which might be part of the normal water chemistry or used for specific plant protection purposes. Examples of these could be nitrogen, hydrogen, chlorine, CO2, depending on the nuclear plant design, and should be confirmed by hazard identification processes.
- Bottled gases, if stored in sufficient quantities such that a release could cause a hazard to plant or personnel carrying out actions important to safety.
- Releases of volatile liquids that could generate a vapour cloud, either under ambient conditions or if they have the potential to come into contact with plant items with elevated temperatures.
- Examples could include chemicals used in water chemistry such as hydrazine, glycol, dimethyl amine, and should be confirmed by hazard identification processes.
- Releases of chemicals which could accidentally mix and form a secondary product as a cloud.

4.204. The list of hazardous substances should be complete and should include material which is brought onto site by sub-contracting companies for maintenance purposes.

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

4.206. Potential hazard effects on plant should also be considered. Examples could include deposition causing shorting at electrical contacts for I&C equipment, and ingestion of gases by diesel generators which might cause them to fail to run; also some other plant systems could be affected by the cooling effects of gas clouds.

Prevention of hazards from releases of hazardous substances within the plant

4.207. Prevention of releases of hazardous substances in the first instance include the general considerations of Level 1 of the defence in depth scheme with respect to minimising

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.

4.208. Where plant systems or components are recognised as needing to be resilient to the presence of a gas or vapour cloud the same approach is followed, i.e., conservative design and material choices, high quality in construction, and surveillance both in construction and operation. In this case, cabling and electrical control cabinets close to potential releases should be designed and located so as to minimise, consistent with other safety requirements, damage due to the release of gas, water, steam, smoke or any other noxious substance.

4.209. 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 care over the location of systems relative to the storage arrangements for hazardous material.

4.210. Engineering provisions preventing the hazard consequences from releases of hazardous substances should include controls for ventilation systems for plant areas or control rooms. Control systems should close ventilation intakes putting the area into a recirculation mode and therefore preventing the immediate effects on the plant personnel. Relevant guidance for the design of the ventilation systems are provided in [11].

4.211. In the case of releases from chemicals which could accidentally mix and form a secondary product as a cloud, the preventative measures should include administrative controls over the receipt and storage of such chemicals, and some engineering provisions, for example different hose couplings for acid and alkaline supplies.

Mitigation of hazard consequences from releases of hazardous substances within the plant

4.212. The design principles of redundancy and diversity, separation and segregation should be used to assist in the mitigation of hazards from releases of hazardous substances. Systems that include redundant capability with good segregation or separation could have

sufficient redundant subsystems unaffected by the release that their safety functions will be successfully achieved even with failures in some of the system components.

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

4.214. Accident management might need the provision of self-air sets either to allow plant personnel to escape from environments that are in danger of becoming untenable, or to access plant areas in which important actions must be carried out.

Hazard specific considerations

4.215. This safety guide only considers the "prompt" effects of the release of hazardous material within the plant internal hazard on the overall safety case for the nuclear power plant. It is possible that smaller continuing releases have 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 plant.

4.216. Some releases are associated with failure of pressurized components such as tanks. The missile effects are discussed elsewhere in this safety guide.

5. APPENDIX I: HAZARD COMBINATIONS

I.1. Both internal and external hazards could - by their nature - 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 hazards) should be considered in the plant's design. The combinations that should be considered depend heavily on the location of the site and the general plant design. Clearly, combinations involving a variety of external hazards, (natural hazards such as tsunami, blizzard, sand storm, but 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 priori a set of hazard combinations applicable to all plants.

I.3. Instead, a performance-based[12] approach is recommended. This approach, regardless 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 what design features are necessary to address them. The basis for screening a hazard combination from further consideration should be clearly defined and documented.

I.4. In principle, three types of hazard combinations should be considered:

- Consequential/Subsequent events: An internal hazard induces one or more additional internal hazards.
- Correlated events: A common event (including external hazards) results in multiple internal hazard(s), which even could occur simultaneously[13].

[12] A performance-based approach does not prescribe specific steps that must 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.

[13] "Simultaneous" in this case does not mean that the hazards occur exactly at the same time but rather that the second hazard occurs before the previous hazard has been completely mitigated.

- Unrelated (independent) events: An initiating event (including hazards) occurs independently from but simultaneously with an internal hazard.

I.5. 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. Examples of screening criteria include:

a. The event combination is not credible
b. The event combination, even if credible, would not lead to conditions beyond what has already been assumed in the design.

I.6. 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. Consider internal flooding as an example. 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 needed. 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 then no additional design measures would be necessary.

I.7. 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.8. Attention should also be paid to the fact that 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.9. Following screening, some hazard combinations could be determined to be credible but need to be assessed against specific acceptance criteria.

I.10. In practice, four categories of internal hazards are considered in the deterministic assessment in a given location:

- internal hazards independent of AOO and accidents;

- internal hazards which could trigger an AOO (e.g., a fire which could trigger a loss of off-site power);
- internal hazards resulting from an accident without significant fuel degradation (e.g., a flooding resulting from a loss of coolant accident);
- internal hazards resulting from a DEC with core melting (e.g., fire from hydrogen combustion).

6. 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; consequential 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 including internal and external hazards likely to occur independently of a fire.

II.3. Simultaneous unrelated fires occurring not in the same fire compartment, in particular, if occurring at multi-unit, multi-source sites, should not have to be considered in the design of fire protection means; however the possibility of a fire spreading, even from one unit to another unit or source, should be taken into account in the fire hazard analysis.

II.4. The fire hazard analysis has the following purposes:

(a) To identify type and amount as well as location in and distribution of fire loads 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 in fire compartments;

(c) To analyze 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 functions of items important to safety required after a fire are not inadmissibly 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 either redundant items important to safety from each other or from inadmissible fire consequences.

II.5. Secondary effects of fires and of fire suppression should be evaluated in the frame of the fire hazard analysis in order to ensure that these secondary effects would not have any adverse effect on nuclear safety.

II.6. Detailed guidance on the preparation of a fire hazard analysis is given in Ref. [15]. Detailed guidance on the evaluation of a fire hazard analysis is given in Ref. [16].

II.7. Fire hazard analysis should be complemented by fire probabilistic safety analysis (Fire PSA). PSA has been used in many power plants to identify and rank the risks of fire. PSA could be used in the design phase to support decision making in the deterministic design of plant layout and fire protection systems. The use of PSA is discussed in Ref. [17].

Fire Barriers

II.8. The overall purpose of fire barriers in nuclear power plants is to provide a passive 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:

- Mechanical resistance;
- Flame proof capacity and hot or flammable gas proof capacity;
- Thermal insulation, which 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).

II.10. The absence of any emission of flammable gases from the face unexposed to the fire should also be verified.

II.11. Passive fire protection systems could be categorized against three performance criteria, depending on their specific function and their potential role in a fire:

- 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 with regard to either the extent or the rate of deformation or both.

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

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

II.12. Within each category, 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 or role when subjected to a thermal test program according to the standards of the International Organization for Standardization (ISO) or other standards.

II.13. The specific functions (load bearing capacity, integrity and insulation) and ratings (e.g., 90 min) of components used as fire barriers (walls, ceilings, floors, dampers, penetration seals and cable wraps) should be specified in the fire hazard analysis.

Fire compartment approach

II.14. Redundant items important to safety should be located in separate fire compartments, in order to implement the concept of segregation and to separate them from high fire loads and other fire hazards.

II.15. 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.16. Confinement of the fire within the fire compartment is intended to 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 relevant.

II.17. The separation provided by fire barriers should not be compromised by fire and fire by-products effects or pressure effects of fires on common building elements such as building services or ventilation systems.

II.18. Since any penetration of a barrier can reduce its overall effectiveness and reliability, such penetrations should be minimized. 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.19. The fire compartment approach does not require the provision of fire extinguishing systems to meet the considerations stated in para. 4.1. 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.20. Conflicts between requirements for fire protection and other plant requirements might prevent the full adoption of the fire compartment approach throughout the design of a nuclear power plant. For example:

- 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;

- 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.

II.21. In situations such as those described in Appendix II, paragraph II.20., 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 cell approach'. Figure II.1. illustrates applications of the fire containment approach and the fire cell approach.

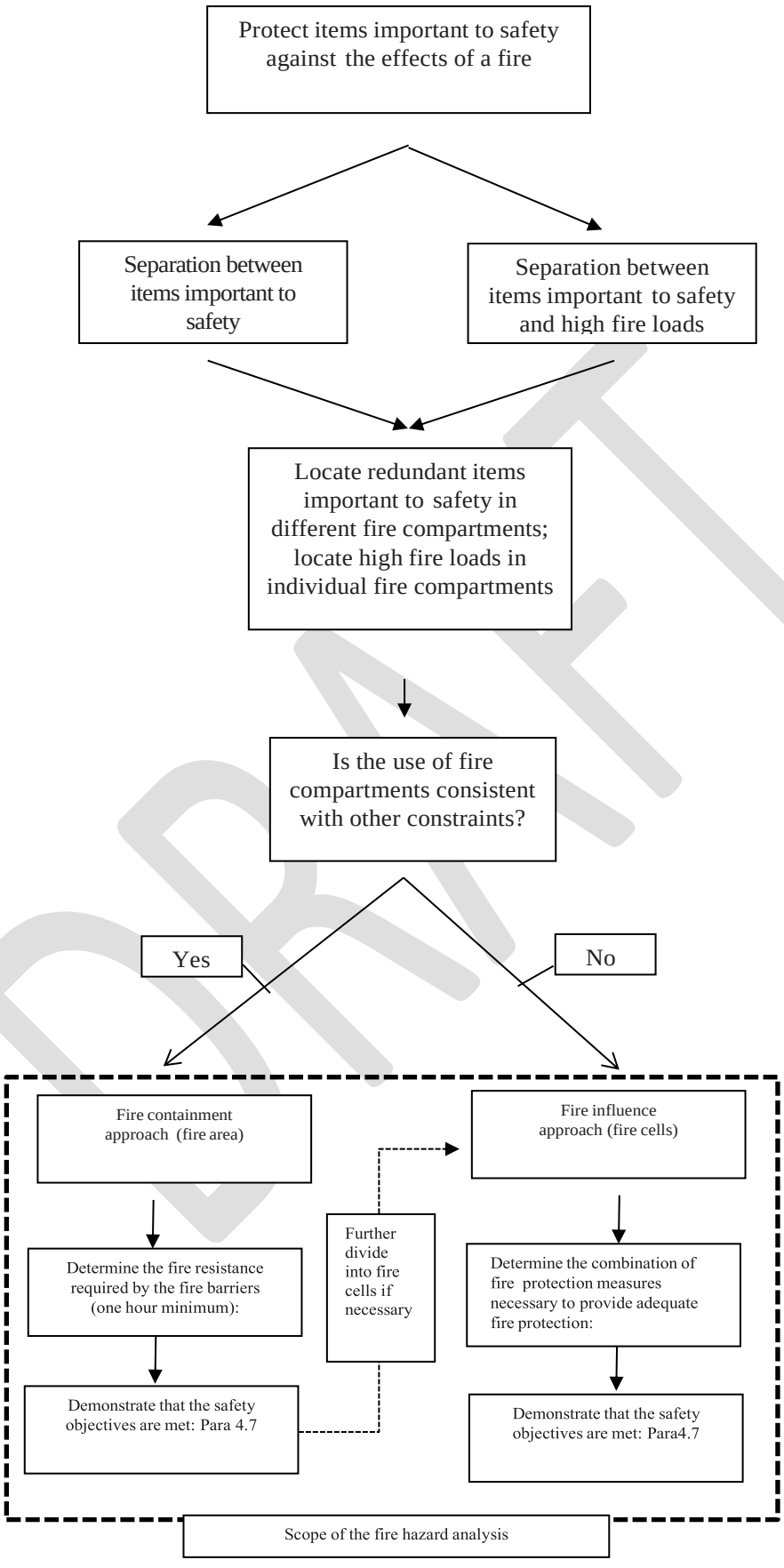
Protect items important to safety against the effects of a fire
Separation between items important to safety
Separation between items important to safety and high fire loads
Locate redundant items important to safety in different fire compartments; locate high fire loads in individual fire compartments
Is the use of fire compartments consistent with other constraints?
Yes
No
Fire containment approach (fire area)
Fire influence approach (fire cells)
Determine the fire resistance required by the fire barriers (one hour minimum):
Further divide into fire cells if necessary
Determine the combination of fire protection measures necessary to provide adequate fire protection:
Demonstrate that the safety objectives are met: Para 4.7
Demonstrate that the safety objectives are met: Para4.7
Scope of the fire hazard analysis

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

Fire cell approach

II.22. 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 protection means. These means include:

- the limitation of combustible materials;
- the separation of equipment by distance, without intervening combustible materials;
- the provision of local passive qualified fire protection such as fire shields or cable wraps;
- the provision of fire detection and extinguishing systems.

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) should be specified in the fire hazard analysis together with an extinguishing system.

II.23. 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 in the same fire compartment.

II.24. Where separation by distance alone is claimed as the protection between fire cells within a fire compartment, the fire hazard analysis should demonstrate that neither radioactive nor convective heat transfer effects would jeopardize the claimed separation.

Escape and Rescue Routes

II.25. Adequate escape and rescue routes for personnel should 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. A minimum of two escape routes from every building should be provided. For each route the following general conditions should be met:

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

(b) Escape and rescue routes should be kept clear of any stored material.

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

(d) Escape and rescue routes should be clearly and permanently marked and should be easy to recognize. The markings should show the shortest possible safe routes.

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

(f) Emergency lighting should be provided on escape and rescue 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) Escape and rescue 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 escape and rescue 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 multistorey staircases, consideration should be given to subdividing the staircase.

(j) Doors leading onto staircases or escape and rescue 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 escape and rescue 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.26. Together with liquid hydrocarbons used as fuel and as lubricating and insulating fluids, 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.27. Various design approaches have been taken to limit the significant impact of cable fires. Among these approaches are: protecting electrical circuits against overload and short circuit conditions; limiting the total inventory of combustible material in cable installations; reducing the relative combustibility of cable insulation; providing fire protection to limit fire propagation; and providing separation between cables from redundant divisions of safety systems, and between power supply cables and control cables.

II.28. Design approaches should be taken to limit the significant impact of cable fires as follows:

- providing fire protection to limit fire propagation; and
- providing separation between cables from redundant divisions of safety systems, and between power supply cables and control cables.

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

Control of cable fires

II.29. Controls should be imposed on the quantities of polymer insulated cables 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.30. While details of qualification tests for fire retardant electrical cables vary according to national standards, large scale flame propagation tests for cables often involve vertical cable samples exposed to a flaming ignition source. Among the important variable factors associated with cable fire tests are:

- The cable inventory as an ignition source,
- Cable layout,
- Resistance to ignition,
- The extent of fire propagation,
- Air flow rate,
- The thermal isolation of the enclosure,
- The toxicity and corrodibility associated with smoke formation.

Cable fire protection

II.31. In some circumstances, specific passive protection measures might be necessary to protect electrical cables from fire. Such measures include:

- Cable coatings to reduce the potential for ignition and flame propagation;

- Cable wraps to provide segregation from other fire loads and from other systems and/or items important to safety;

- 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.32. The potential impact of cable fires can be reduced by providing suitable separation by the fire compartment approach.

II.33. In some cases, spatial separation with no intervening combustible materials used, 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 particular situations.

II.34. The preferred approach for the separation of redundant divisions of a safety system should be fire compartment approach.

Fire Detection and Alarm Systems

II.35. The nature of the fire detection and alarm systems, its layout, the necessary response time and the characteristics of its detectors, including their diversification, should be determined by the fire hazard analysis.

II.36. The fire detection and alarm systems should provide detailed annunciation in the control room about the location of the 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 and should not be capable of being confused with any other alarms in the plant.

II.37 All detection and alarm systems should be energized at all times and should be provided with non-interruptible emergency power supplies, including fire resistant supply cables where necessary. Guidance on emergency power supplies is provided in Refs [7, 8].

II.38. Individual detectors should be sited so that the flow of air due to ventilation or pressure differences necessitated 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.

II.39. 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 gaseous atmosphere from the protected area for analysis by remote detectors with automatic operation.

II.40. 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 be detrimental to the plant, operation 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.

II.41. Wiring for fire detection systems, alarm systems or actuation systems should be:

- protected from the effects of fire by a suitable choice of cable type, by proper routing, by a looped configuration or by other means;
- protected from mechanical damage;
- constantly monitored for integrity and functionality.

SELECTION OF DETECTOR TYPES AND LOCATION OF DETECTORS

II.42. The selection of the types of fire detector and of the positioning and location of detectors should be made carefully to ensure that the detectors would actuate as expected in response to a fire. Numerous factors affect the response of fire detectors to the growth of a fire, among which are:

- Burning rate,
- Rate of change of the burning rate,
- Characteristics of the burning materials,
- Ceiling height,
- Positions and locations of detectors,
- Locations of walls,
- Positions of any obstructions to gas flow,

- Room ventilation,
- Response characteristics of the detector.

II.43. 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.44. 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.45. 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.46. Fire extinguishing systems should be designed and located to ensure that neither their intentional nor their spurious operation jeopardizes the required function of SSCs important to safety (including DEC conditions) in case of fire.

II.47. 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 fire compartment where the fire started.

II.48. In the selection of the type of extinguishing system to be installed, consideration should be given to the necessary response time, the suppression characteristics (e.g., thermal shock) and the consequences of operation of the system for people and for items important to safety as established by the fire hazard analysis.

II.49. In general, water systems should be preferred in areas containing high fire loads, where there is a possibility of deep seated fires and where cooling is necessary. Automatic sprinklers, water mist systems, water spray or spray water 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 systems are more complex but have 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.50. For prompt operation and availability at the time of a fire emergency, automatic extinguishing systems are preferred. 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.51. 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.52. Any fixed extinguishing system that is solely manually actuated should be designed to withstand fires for a period of time set to be sufficient to allow for the manual actuation.

II.53. 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.54. 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.55. 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. Recommendations and guidance on these activities are provided in Ref. [18].

Water based extinguishing systems

II.56. Water based extinguishing systems should be permanently connected to a reliable and adequate supply of fire extinguishing water.

II.57. 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 high fire load is present.
- A potential for rapid spread of fire exists.
- A fire could compromise redundant items important to safety.
- An unacceptable hazard for fire fighters could be created.
- An uncontrolled fire would make access for firefighting difficult.

II.58. If the fire hazard analysis indicates that water alone might not be suitable for successfully coping with the hazard, such as for applications to flammable liquids, consideration should be given to systems using fire extinguishing foam as the extinguishing medium.

II.59. 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.60. The component parts of water based systems should be constructed from compatible materials in order to avoid galvanic corrosion.

II.61. 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.62. Reactor buildings should be provided with a de-energized fire standpipe and hose system (dry risers). The fire hydrant system for the reactor building should have provisions for local or remote actuation.

II.63. The distribution loop for fire hydrants should provide exterior coverage of the 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.

II.64. Each hydrant hose and standpipe riser should have connections that are compatible with on-site and off-site firefighting equipment.

II.65. 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.66. Each branch line to a separate building should be provided with no fewer than two independent hydrant points. Each branch line should be provided with an indicating shut-off valve.

Water supply system for fire extinguishing equipment

II.67. The main loop of the water supply system for the fire extinguishing equipment should be designed to supply the anticipated demand for water. 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.68. Valves should be provided to isolate parts of the main loop for the water. 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 in contradiction to 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 as to remain unaffected by a fire in that area.

II.69. 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.70. 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.71. At sites where a pumping capability is necessary to provide the amount of water needed, fire pumps should be redundant and diverse and separated in the fire context in order 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 system and independent prime movers [8]. Alarms indicating pump running, power failure or failure of the fire pumps should be provided in the control room. In areas subject to freezing temperatures, a low temperature alarm should also be provided.

II.72. 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 required. 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 recommendations on the minimum pressure at the highest outlet in the plant should be taken into account. Any need to prevent freezing under low temperature climatic conditions 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.73. 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.74. When a common water supply is provided for fire protection and for the ultimate heat sink, the following conditions should also be satisfied:

— The capacity needed to meet the recommendations for the water supply for the fire protection system should be a dedicated part of the total water inventory.
— Failure or operation of the fire protection system should not violate the intended functions of any water supply for the ultimate heat sink, or vice versa.

II.75. The water supply for sprinkler systems might necessitate chemical treatment and additional filtration to ensure that no blockage of the sprinklers occurs from the effects of debris, biological fouling or corrosion products.

II.76. Provision should be made for the inspection of water suppression 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 any possible water damage to electrical equipment during testing.

Gaseous extinguishing systems

II.77. Gaseous fire extinguishing systems consist of a gaseous 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 fires involving electrical equipment.

II.78. Gaseous extinguishing agents are usually termed clean agents as they leave no residue upon actuation. Since they are also non-conductive, their combined characteristics make them

suitable for protecting electrical equipment. Several types of gaseous extinguishing systems 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.79. Owing to the potential for causing a severe hazard to personnel, carbon dioxide and 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.80. There are generally two methods of providing protection with gaseous extinguishing agents: (1) local application, where the agent is discharged towards the hazard or a particular piece of equipment; (2) 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.81. 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 deep seated 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 the fuel has cooled.

(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 particular hazard, the rate of application and the period for which the design concentration is to be maintained.

(d) In order to avoid overpressures that would result in structural damage or damage to equipment, the structural effects of the buildup of pressure within the 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. Moreover, the design should ensure that nozzles are sited to avoid fanning the flames of the fire on the initial discharge of the system.

(f) Carbon dioxide extinguishing systems and any other gaseous system with the potential for causing a hazard to personnel should be provided with early warning alarms for prompt evacuation of personnel from the affected area before the system discharges.

II.82. Suitable safety 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 should include:

- Provision of devices to prevent automatic discharge of the system while personnel are, or could be, within the protected space;
- Provision for manual operation of the system from outside the protected space;
- 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);
- 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.

II.83. Precautions should be taken to prevent leakage of carbon dioxide or any other hazardous extinguishing gas in dangerous concentrations to adjacent areas that might be occupied by personnel.

II.84. Means should be provided to ventilate the protected enclosure after the discharge of the gaseous protection system. Forced ventilation is often needed to ensure that an atmosphere hazardous to personnel is dissipated and not moved to other areas.

II.85. All total flooding applications need a rapid and even distribution of gas throughout the space that is flooded. This is usually achieved within 10–30 s of actuation by the use of special nozzles and an adequate 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.86. 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.87. 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.88. 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 should also be taken into account.

II.89. 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.90. 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.91. 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.92. Portable and mobile fire extinguishers of a type and size suitable for the hazards being guarded against should be provided for use in manual firefighting by plant personnel and external fire fighters, if needed.

II.93. The entire plant should be equipped with a sufficient number of portable and mobile extinguishers of the appropriate types as well as spares or facilities for recharging. All fire extinguisher locations should be clearly indicated.

II.94. Fire extinguishers should be placed close to the locations of fire hoses and along the escape and rescue routes for fire compartments.

II.95. Consideration should be given to the possible adverse consequences of the use of extinguishers, such as cleanup problems after use of dry powder extinguishers.

II.96. In plant areas with potential hazards due to flammable liquids, foam concentrate for firefighting and portable equipment that are suitable for the hazard should be readily available.

II.97. Portable and mobile extinguishers filled with water or foam solution and 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.98. 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 brigades should be established at the design stage. The location of the site and the response time of any off-site fire brigade will affect the necessary level of provision for manual firefighting. Manual firefighting capabilities are discussed in Ref. [18].

II.99. The design of the plant should allow for access by fire teams and fire brigades using heavy vehicles.

II.100. Suitable emergency lighting and communications equipment should be provided for all fire compartments to support the operation of manual firefighting activities. These should be energized at all times and should be provided with non-interruptible emergency power supplies.

II.101. A fixed wired emergency communication system with a reliable power supply should be installed at preselected stations [11].

II.102. 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. Prior to the first fuel loading, testing should be carried out to demonstrate that the frequencies and transmitter powers used will not cause spurious operation of the protection system and control devices.

II.103. Self-contained breathing apparatus, including spare cylinders and a facility for recharging, should be provided at appropriate locations for the use of the emergency response team.

II.104. Arrangements for plant equipment and for storage in the plant should be designed to facilitate access for firefighting, as far as practicable.

II.105. Detailed firefighting strategies should be developed for locations containing items important to safety.

Provisions for smoke and heat venting

II.106. An assessment should be carried out to determine the need for smoke and heat venting, 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.107. 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 brigade access, the type of fixed fire extinguishing systems used and radiological aspects.

II.108. 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 smoke and heat venting:

- Areas containing a high fire load due to electrical cables;
- Areas containing a high fire load of flammable liquids;
- Areas containing items important to safety (including those applied under DEC conditions) that are normally occupied by operating personnel (e.g., the main control room).

7. REFERENCES

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

[2] 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)

[3] 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)

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

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

[6] IAEA Safety Standards Series No. DS491, Deterministic Safety Analysis for Nuclear Power Plants, (revision of SSG-2)

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

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

[9] IAEA Safety Standards Series No. DS481, Design of Reactor Coolant System and Associated Systems in Nuclear Power Plants.

[10] IAEA Safety Standards Series No. DS482, Design of Reactor Containment Structure and Systems for Nuclear Power Plants

[11] IAEA Safety Standards Series No. DS440, Design of Auxiliary Systems and Supporting Systems for Nuclear Power Plants

[12] IAEA Safety Standards Series No. DS487, Design of Fuel Handling and Storage Systems for Nuclear Power Plants, (revision of NS-G-1.4)

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003)

[14] 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)

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

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Fire Hazard Analyses for Nuclear Power Plants, Safety Series No. 50-P-9, IAEA, Vienna, (1995)

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

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Fire Safety in the Operation of Nuclear Power Plants, Safety Standards Series No. NS-G-2.1, IAEA, Vienna (2000)

8. CONTRIBUTORS TO DRAFTING AND REVIEW

Amri, A.	IAEA
Bae, Y.B.	KINS, Korea
Berg, P-H.	BfE, Germany
Bouscasse, M.	IRSN, France
Eguchi, H.	NRA, Japan
Fong, C.J.	NRC, USA
Kasahara, F.	NRA, Japan
Katona, T.J.	Paks Nuclear Power Plant Co., Ltd., Hungary
Röwekamp, M.	GRS, Germany
Williams, G.	ONR, UK