IAEA SAFETY STANDARDS

for protecting people and the environment

Step 5

Preparing draft

Protection against Internal and External Hazards in the Operation of Nuclear Power Plants

DS 503

DRAFT SAFETY GUIDE

Revision of NS-G-2.1and enhanced scope

FOREWORD

By Rafael Mariano Grossi

Director General

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

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

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

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

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

The physical protection of fissile and radioactive materials and of nuclear power plants as a whole is mentioned where appropriate but is not treated in detail; obligations of States in this respect should be addressed on the basis of the relevant instruments and publications developed under the auspices of the IAEA Non-radiological aspects of industrial safety and environmental protection are also not explicitly considered; it is recognized that States should fulfil their international undertakings and obligations in relation to these.

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

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

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

EDITORIAL NOTE

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

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

The English version of the text is the authoritative version.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1 This Safety Guide was prepared under the IAEA programme for establishing standards for nuclear power plants (NPPs). This publication is a revision of the IAEA Safety Guide on Fire safety in the operation of NPPs issued in 2000 as IAEA Safety Standards Series No. NS-G-2.1.

1.2 To ensure safety, it is necessary that the operating organization of a NPP recognizes that the personnel involved in should be cognizant of the demands of safety, should respond effectively to these demands, and should continuously seek better ways to maintain and improve safety. This is especially important when plant operators are challenged by the adverse impacts of internal and external hazards.

1.3. The current revision of this Safety Guide reflects lessons learned over recent years, and in particular from the international response to the Great East Japan Earthquake and Tsunami of 11 March 2011 and its effects on the Fukushima Daiichi NPPs. It also reflects the principles of the Vienna Declaration on Nuclear Safety in February 2015. Many countries have enhanced their understanding of hazards, and combinations of hazards. This includes installed provisions and additional deployable equipment that have enhanced the plants' coping and mitigation strategies and equipment availability to implement these strategies. It was identified that operational guidance should be extended to pre-planning of responses to these hazards. This understanding includes improved decision making for those hazards where a sufficient warning period may allow protective preparation measures to be taken.

1.4. This guide focuses on the operational management of internal and external hazards while other IAEA publications give either general design guidance, or specific design guidance for hazards. Specifically, IAEA Safety Standards Series No. SSG-64, Protection against Internal Hazards in the Design of Nuclear Power Plants (under publication)[1], IAEA Safety Standards Series No. SSG-XX, External Events Excluding Earthquakes in the Design of Nuclear Installations (Under revision, DS498)[2] and IAEA Safety Standards Series No. SSG-XX, Seismic Design of Nuclear Installations, IAEA Safety Standards (Under revision, DS490)[3] provide design guidance for internal and external hazards respectively.

OBJECTIVE

1.5. The objectives of this publication are to provide the operating organizations involved in design, manufacture, construction, modification, maintenance, operation, safety assessment and decommissioning for NPPs in analysis, verification and review, and in the provision of technical support, as well as regulatory body of Member States, with recommendations and guidance on:

- Measures for ensuring that adequate hazard mitigating and coping strategies against internal and external hazards are maintained throughout the lifetime of a NPP, and

- Measures to ensure that early indications of an imminent hazard lead to appropriate decisions by nuclear power plant managers and operators that will increase the likelihood of successful management of the adverse effects of the hazard.

SCOPE

1.6. This Safety Guide is developed for reactors of types in general use, such as light water reactors and heavy water reactors. The general guidance may also be applicable to a broad range of other types of nuclear reactor designs, including gas cooled reactors and other types of nuclear installations, but its detailed application will depend on the particular technology and the hazard risks.

1.7. This safety guide covers the features of an operational hazard management programme necessary to protect items important to safety in NPPs against the effects of internal and external hazards.

1.8. While hazard mitigation measures and coping strategies should address plant operating personnel required to respond and implement hazard mitigating measures and coping strategies, this safety guide does not specifically discuss conventional aspects of protection of the safety of plant operating personnel, or the protection of property, except where this could affect the safety of the NPP.

1.9. This safety guide is targeted primarily at new nuclear power plants. For plants designed with earlier standards, it is expected that in the safety assessments of such designs a comparison will be made with the current standards, to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements: see para. 1.3 of SSR-2/1 (Rev. 1) [8]. Nevertheless, this Safety Guide provides the operating organizations of existing plants the latest practices for their continuous improvement of their hazard management programmes.

1.10. In this safety guide, internal and external hazard initiators caused by human actions are considered to be of accidental origin. Initiators caused by wilful or malicious actions either by on-site personnel or by third parties (e.g. terrorist incursions) are outside the scope of this document, and guidance on these are covered by IAEA guidance for nuclear security.

1.11. This safety guide is focused on safety issues with possible interfaces between nuclear safety and nuclear security. Safety measures and security measures have in common the aim of protecting human life and health, society and the environment. Safety measures and security measures must be designed and applied in an integrated manner, and as far as possible in a complementary manner, so that security measures do not compromise safety and safety measures do not compromise security. In dealing with interfaces between nuclear safety and nuclear security, it must be borne in mind that nuclear safety and nuclear security are likewise important, and measures to be taken must be mutually acceptable in both areas. Guidance on nuclear security is issued in the IAEA Nuclear Security Series.

STRUCTURE

1.12. Section 2 provides general considerations for protection against hazards in the operation of NPPs. Section 3 focuses on the organization and responsibilities of a hazard management programme. Section 4 provides recommendations for applying Defence in Depth principles. Section 5 provides recommendations for ensuring safety for internal hazards while Section 6 does the same for external hazards. Section 7 provides guidance for the combination of internal and external hazards. Section 8 provides recommendations on periodically updating the hazard management programme. Section 9 provides guidance on material control and housekeeping on the hazard management programme. Section 10 provides recommendations for the maintenance and testing of equipment required for hazard mitigation and coping. Section 11 provides guidance on training of personnel within the hazard management programme. Additional information is given in three appendices to aid understanding of aspects of the safety guide; Appendix A gives more detailed recommendations relevant to internal hazards, Appendix B gives more detailed recommendations relevant to external hazards and Appendix C provides assistance in identifying an approach towards combinations of hazards when developing an operational hazard management programme.

2. GENERAL CONSIDERATIONS

2.1. Internal hazards are those hazards to the plant that originate within the site boundary and are associated with failures of facilities and activities that are in the control of the operating organization. External hazards are those natural or human induced events that originate external to both the site and the processes of the operating organization, and which the operating organization may have very little or no control. Such events are unconnected with the operation of the NPP site or conduct of an activity on the site but could have an adverse effect on the safety of the NPP site or activity. Throughout this safety guide, the word “hazard” implies both internal and external hazards unless where specifically noted.

2.2. This safety guide provides recommendations and guidance for the operational management aspects of preparing for, mitigating and coping with hazards at aNPP, to fulfil the relevant requirements of IAEA Safety Standards Series No. SSR-2/2(Rev.1) [6], Safety of Nuclear Power Plants: Commissioning and Operation [6], and in particular Requirements 22, 23, 28, 31, 32, and 33.

23. The above requirements of SSR-2/2 (Rev.1) [6] are of particular interest in the operational management of nuclear power plants for hazards. The requirements are as follows:

Requirement 22: Fire safety

“The operating organization shall make arrangements for ensuring fire safety.”

The recommendations for specific hazard mitigating measures and coping strategies in this safety guide is developed upon this requirement. Specific applicable paragraphs is para 5.21, 5.22 and 5.23.

Requirement 23: Non-radiation-related safety

“The operating organization shall establish and implement a programme to ensure that safety related risks associated with non-radiation-related hazards to personnel involved in activities at the plant are kept as low as reasonably achievable.”

The hazard mitigating measures and coping strategies are implemented by personnel involved in activities at the plant. Therefore, the hazard management programme should include personnel and industrial safety. Specific applicable paragraph is para 5.26.

Requirement 28: Material conditions and housekeeping

"The operating organization shall develop and implement programmes to maintain a high standard of material conditions, housekeeping and cleanliness in all working areas."

The management and control of materials and housekeeping on a routine basis can have a great impact on the progression of hazards and their consequences. Some of actions are of particular importance at times when an external hazard is forecast, but proper housekeeping should be in effect at all times. Specific applicable paragraphs are para 7.10. and 7.11.

Requirement 31: Maintenance, testing, surveillance, and inspection programmes

"The operating organization shall ensure that effective programmes for maintenance, testing, surveillance and inspection are established and implemented."In the activities of maintenance, testing, surveillance and inspection, risk caused by hazards may increase. Enhanced protection against hazards should be put into place during these activities. It is also important to identify and include these activities for hazard protection and mitigation measures in hazard management programmes. Specific applicable paragraphs are 8.1-8.7, 8.13, 8.14 and 8.14A.

Requirement 32: Outage management

"The operating organization shall establish and implement arrangements to ensure the effective performance, planning and control of work activities during outages."

In the outages including shutdown operation, risk caused by hazards may increase. Enhanced preparing for mitigating and coping with hazards should be put into place during the outages. Specific applicable paragraphs are Para 8.19, 8.20, 8.21 and 8.22.

Requirement 33: Preparation for decommissioning

"The operating organization shall prepare a decommissioning plan and shall maintain it throughout the lifetime of the plant, unless otherwise approved by the regulatory body, to demonstrate that decommissioning can be accomplished safely and in such a way as to meet the specified end state."

Provisions that ensure plant safety in the event of hazards should be maintained for each stage of decommissioning. Specific applicable paragraphs are Para 9.1, 9.2, 9.3, 9.4, and 9.6.

2.4. This safety guide should be used with DS494 [1], DS498 [2], and DS490 [3] as applicable. These safety guides provide recommendations on protection against hazards respectively in the design of NPPs, as required in IAEA Safety Standards Series No.SSR-2/1(Rev. 1), Safety of Nuclear Power Plants: Design [8]. These safety guides should be used to ensure that all design aspects related to a particular hazard are maintained and upgraded based upon periodic reviews.

2.5. Provisions that ensure plant safety in the event of hazards should be maintained for each stage of plant life, from design to construction and commissioning, plant operation and through decommissioning.

2.6. Hazards caused by (or occurring at) different NPPs at the same site should be considered hazards depending upon which is the operating organization of the different NPPs.

2.7. Hazards have the potential to induce initiating events; to cause failures of equipment that is necessary to mitigate hazards; and to adversely affect, directly or indirectly, the barriers for prevention of release of radioactive materials. Additionally, hazards can simultaneously challenge more than one level of defence in depth and increase the dependency between the origination of initiating events and the failures of mitigation equipment. The following should be considered:

- External hazards can generate internal hazards (e.g. an earthquake followed by an internal flood)
- 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). The mitigation of one hazard can cause the initiation of another hazard. (e.g. the use of water to extinguish an internal fire may cause internal flooding)
- Credible combinations of hazards are considered in DS494 [1], DS498 [2], and DS490 [3]. Section 7 and Appendix C gives additional guidance on combined hazards.

2.8. While it may not be practical or possible to prevent an hazard from triggering an anticipated operational occurrence (AOO), one of the objectives of an operational hazard management program is to ensure that hazards do not trigger an accident whenever practicable. (e.g. avoidance of Station Black Out caused by a seismic hazard)

2.9. The aim of considering hazards in the design and operation of NPPs is to ensure that the fundamental safety functions are fulfilled in any plant state and that the plant can be brought to and maintained in a safe shutdown state after any hazard occurrence. This implies that:

(a) The redundancies of the systems are segregated to the extent possible or adequately designed and maintained as necessary to prevent the loss of the safety function performed by the systems;

(b) The design and operation of individual structures, systems and components (SSCs) is such that design basis accidents or design extension conditions induced by hazards are avoided to the extent practicable;

(c) An internal or external hazard occurring does not affect the habitability of the main control room. In case the latter is not habitable, access to the supplementary control room is to be ensured. In addition, and when necessary, plant personnel should be able to access equipment in order to perform local actions.

2.10. In accordance with the concept of defence in depth (the first level of defence in depth), protection against hazards is provided in general by ensuring quality and reliability of SSCs. This should be done by environmental qualification of the SSCs, by application of principles of redundancy, diversity, by physical separation, functional independence, and through design of appropriate barriers. Therefore, the protection against the effects of hazards is an iterative process, integrating the needs of protection against several hazards. Proper surveillance and in-service inspections should be implemented for coping (and, if possible, detecting) with hazards.

2.11. An appropriate management system should be applied to all hazard protection and mitigation features, including those that were not ordinally installed or designed as safety systems or features, such as embankments, spillways, in order to reduce the potential for common cause failure and thus pose a threat to safety. Throughout this safety guide, the word hazard protection and mitigation features imply these items unless where specifically noted.

3. ORGANIZATION AND RESPONSIBILITIES

3.1. Responsibilities of site staff involved in the establishment, implementation, and management of the operational hazard management programme should be identified and documented. Requirements and guidance on Leadership and Management are given in other IAEA Safety Standards, including IAEA Safety Standards Series No. GSR Part 2, Leadership and Management for Safety, IAEA Safety (2016) [9] and IAEA Safety Standards Series GS-G-3.5, The Management System for Nuclear (2009) [10].

3.2. The arrangements for delegation of responsibilities should be included in the operational hazard management programme. This documentation identifies the organizational structures, processes, specific responsibilities, level of authority, and interfaces of personnel involved in hazard management including their relationship with internal and external organizations. The external organizations featured in the operational hazard management programme should be developed accounting for differences in site challenges, plant design aspects and local and national governance.

3.3. Responsibilities for deploying protective measures should be realized by plant management and plant operating personnel in a timely manner when a hazard is predicted (e.g, severe storm). The operating organization should identify and establish staffing levels and capabilities, and organise them appropriately, in the period prior to the event, to mitigate and cope with the hazard.

OPERATIONAL HAZARD MANAGEMENT PROGRAMME

3.4. The plant operating organization should establish an operational hazard management programme to ensure that the plant can be protected from, mitigate the impact of, and cope with the consequences of hazards or credible combinations thereof. Specifically, the operating organization should be able to maintain the fundamental safety functions of the NPP during and after the impact from hazards or a credible combination of these.

3.5. The operational hazard management programme and its decision making should be harmonized with the requirements, guidance, and actions provided in the plant's emergency plan, for mitigating and coping with the event progress from internal or external hazards to a nuclear or radiological emergency. Requirements and guidance on preparedness for a nuclear or radiological emergency are given in other IAEA Safety Standards, including IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [11] and GS-G-2.1 [7].

3.6. The operational hazard management programme should consider and include:

- The prevention of avoidable hazards that can affect nuclear safety,
- Mitigation measures for hazards or credible combinations of hazards, and
- Hazard coping strategies.

3.7. The operational hazard management programme should include a combination of personnel from the various site sections or organizations such as engineering design, operations, maintenance, and emergency response. These personnel perform activities to ensure the plant is protected by proper design and maintenance and operated to mitigate and cope with the impacts of hazards.

3.8. For hazard impacts that are of sufficient duration (e.g., heavy snow fall, hurricane, etc.), the operating organization should utilize all available resources to cope with the hazard impact and not allow the impact of the hazard to propagate, become more severe, or jeopardize the fundamental safety functions.

3.9. The operational hazard management programme should be maintained applicable and relevant throughout the entire plant lifetime. This includes implementation of design modifications, lessons learned, and best practices from industry operating experiences.

3.10. Hazard coping strategies within the operational hazard management programme should be developed accounting for the physical and social infrastructure around the plant. The strategies should account for the local road and rail infrastructure, electrical grid interfaces, presence of sources of water and proximity to water ways, local population centres and local industries, especially those that may present hazard challenges to the site. The programme should also identify relevant external organizations, such as local government and emergency services, and specify the amount of support local external organizations can be relied on for.

3.11. The hazard management programme should include personnel and industrial safety for those personnel responsible for implementing hazard mitigating measures and coping strategies.

3.12 Defined roles and responsibilities of site staff involved in the establishment, implementation, and administration of the operational hazard management programme should be documented and maintained current.

3.13. The operating organization should include a response team with the appropriate qualifications, skills and training in the use of hazard mitigation and coping equipment (See section 11).

3.14. Procedures should give clear instructions for plant operating personnel on actions in the event of precursors and indications of hazards. These actions should be primarily directed to ensuring the safety of the power plant including personnel. In some cases, shutdown or power reduction of the plant may be necessary.

3.15. The procedures should set out the roles of plant operating personnel in relation to the roles of any external organizations (e.g. local authority fire brigades).

3.16. Special attention should be paid to cases where there is a risk of release of radioactive material following the initiation of a hazard event. It should be ensured that such cases are covered in the emergency arrangements with operating organizations and external organizations.

3.17. Appropriate measures should be taken for radiation protection for personnel from external organizations (e.g. fire fighters and other staff carrying out plant response or casualty recovery).

DECISION MAKING FOR HAZARD MANAGEMENT

3.18. Operational decision makers at the plant should have a working level of understanding for safety significance of their NPP, and how nuclear safety and hazard protection and mitigation features could be threatened by hazards. This includes an understanding of hazard coping and mitigation strategies and measures to increase the plant's resilience.

3.19. The working level of understanding by operational decision makers should include the security features of the NPP that may also be affected by the impact of the hazards and the necessary mitigation measures.

3.20. When a hazard has occurred, decision making should be performed by the operating organization to ensure:

- A timely evaluation/assessment that the criteria for specific hazards are met;
- That time-sensitive actions and confirmation of actions are to be performed in order to manage the risk imposed by the hazard;
- Identification of any required support (e.g., internal organizations, external organizations, emergency support equipment, specialized personnel);
- That the fundamental safety functions required for the appropriate plant operating mode are not or will not be threatened.

3.21. The operating organizations should put in place processes to ensure that meteorological forecasts are monitored and that the appropriate actions are taken when an external hazard is predicted to occur (for example coastal flooding, tornadoes, etc). The operating organization should then prepare and activate the organization as required to minimise the effects of a predicted hazard on the NPP, and implement hazard mitigation measures and coping strategies. For these hazards that are predictable or partially predictable, the operating organization should undertake the steps listed in the paragraph above to ensure that the site is prepared in good time. In addition, all of the following should be considered and implemented:

- Cooperation with local state, and national external organizations:

  The operating organization or decision team should establish communication arrangements in advance with appropriate external organizations to allow timely predictions of potential hazards to input into their managerial decision-making process.

  There are well-established arrangements for emergencies in which a radiological release may occur, but the NPP operating organization should review what arrangements are appropriate for hazard initiator events which, if managed appropriately, will not lead to a radiological release.

  Hazard coping and mitigation strategies may require additional emergency equipment which may be stored off-site and require transport organizations to deploy them to the site. In the context of hazards, this may include equipment such as drainage pumps. Sections 5 and 6 of this safety guide give further examples.

- Security aspects

  The operational hazard management programme should be compatible with the security programme of the nuclear power plant. The operational hazard management plan should also be developed cooperatively with off-site security and/or law enforcement organizations as recommended by the plant's security staff. Guidance to be considered is given in the plant's security plan, IAEA Nuclear Security Series No. 27-G, Physical Protection of Nuclear Material and Nuclear Facilities (implementation of INFCIRC/225/Revision 5) [12], and in other relevant Nuclear Security Series documents.

- Multi-unit plant sites

  For multiple NPPs located on the same site or closely adjacent, but managed by different operating organizations, the operating organizations should consider how this site configuration affects their hazard coping and mitigation strategies, particularly for hazards with an increased predictability, and ensure appropriate cooperation.

4. APPLICATION OF DEFENCE-IN-DEPTH

4.1. Principle 8 of IAEA Safety Standards Series No. SF-1, Fundamental Safety Principles [13] ensures that the design of nuclear installations includes the appropriate application of defence in depth concept. When properly implemented, defence in depth ensures that no single technical, human, or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. Hazards have the potential to challenge multiple layers of defence in depth. Thus, hazard coping strategies and mitigation measures should be provided as part of the defence in depth concept and the operational hazard management programme to control hazard impacts.

4.2. Requirement 4 of the SSR-2/1(Rev. 1) [8] states that "the fundamental safety functions for a NPP "shall be ensured for all plant states: (i) control of reactivity; (ii) removal of heat from the reactor and from the fuel storage area; and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as the limitation of accidental radioactive releases". Thus, hazard coping strategies and mitigation measures should ensure that the fundamental safety functions are maintained for all plant states.

4.3. The operating organization should achieve the objectives of defence in depth through a combination of: design, installation, and operation of hazard protection and mitigation systems and hazard coping strategies, supported by the operational hazard management programme described in Section 3. The objectives of defence in depth should be maintained throughout the lifetime of the plant.

4.4. The operating organization should consider a simple approach for defence in depth presented in INSAG Series No.10, Defence in Depth in Nuclear Safety [14] that should be beneficial for the protection of the plant from hazards. Protection against hazards is generally provided by a combination of engineered and procedural methods. Protection should be diverse, redundant, separated and segregated where possible. (See Appendix A and B for examples) This is particularly important in the case of external hazards which can have widespread effects across the plant.

5. ENSURING SAFETY AGAINST INTERNAL HAZARDS IN THE OPERATION OF NPPS

5.1. Internal hazards for a particular site are taken into account during the design phase of the plant. With a few exceptions, internal hazards are mainly mitigated by designing and constructing engineered features. As such, an initial hazard analysis forms part of the basic design phase. However, this initial hazard analysis should be supplemented to account for any site or plant specific aspects, such as local drainage, grid connections, etc., and should include the realisation of operating procedures to mitigate and cope with internal hazards specific for the site.

5.2. The hazard analysis should consider the impact of credible internal hazards on SSCs important to safety. This hazard analysis will form the underpinning of the operational hazard management programme (see section 3). Further recommendations on protection against internal hazards in the design of NPPs are given in DS494 [1] .

5.3. The operational hazard management programme should recognise that enhanced administrative and procedural controls over material and operations should be put into place (see section 9) in periods of increased risk (for example, outages or modification implementation), in order to ensure that the hazard mitigation measures are not reduced.

5.4. The operational hazard management programme will help in defining roles in controlling actions following hazards. The plant operators should have a role in initiating some installed protection systems, in reducing the extent of some hazards by plant re-alignment, or by initiating local actions as part of hazard coping strategies to address plant challenges from the hazard (such as local firefighting or the deployment of local flooding protection).

5.5. Where additional hazard mitigating equipment or personnel may need to be deployed, the operational hazard management programme should allow for and describe communications with external organizations and should include aspects of training and practice drills (see section 11).

5.6. Hazard mitigation measures and coping strategies for internal hazards should include the following elements:

- Identification of a response criteria for which the applicable internal hazard needs to be terminated or mitigated to prevent unacceptable consequences;
- Identification of appropriate warning or monitoring systems and equipment for the applicable hazard;

- Characterization of the nuclear safety threats and functional threats caused by the hazard, e.g. specific equipment that may need protection from the hazard;
- Development and implementation of maintenance and inspection requirements and procedures for equipment required to cope and mitigate the applicable hazard;
- Development and implementation of communication standards and protocols with external organizations
- Personnel training to ensure development of necessary skills for implementing mitigating measures.

RECOMMENDATIONS FOR SPECIFIC INTERNAL EVENTS

5.7. Appendix A describes in more detail specific recommendations that should be incorporated into the operational hazard management programme for the following commonly considered internal hazards. Design related aspects of internal hazards are discussed in DS494 [1]. For all credible internal hazards, the general recommendations given in sections 5.1 through 5.6 are applicable. The following is a list of common internal hazard consistent with Ref. [1].

- Internal fires
- Internal explosions
- Missiles
- Collapse of structures and falling objects
- Pipe breaks
- Internal floods
- Release of hazardous substances
- Electromagnetic Interference
- Site specific or design specific internal hazard as appropriate

6. ENSURING SAFETY AGAINST EXTERNAL HAZARDS IN THE OPERATION OF NPPS

6.1. For those external hazards considered applicable to a particular site, the focus should be on the proper consideration of the hazard challenge presented and documented in the appropriate hazard analysis. Specifically, the operational hazard management programme should be fulfilled for levels of hazards more severe than those considered for design, derived from the evaluation for the impact of these hazards. DS498 [2] and DS490 [3] provide general guidance on the design aspects of external hazards including hazard analysis.

6.2. With the external hazard impacts characterized in the operational hazard management programme, potential hazard mitigation should be identified for each hazard that will increase the viability of a hazard coping strategy deployment for external hazard conditions.

6.3. Notification protocols between appropriate external organizations and the operating organizations of periods of enhanced risks from third-party activities should be considered crucial and established in advance. These protocols should allow timely preparation to be taken by the plant organization to mitigate potential external hazards resulting from these activities. The protocols should also avoid confusion in implementing post-event actions if the potential of a deliberate event is considered.

6.4. Hazard mitigation measures and coping strategies should take the form of operator and equipment deployment strategies and the procedural implementation of these strategies.

6.5. The operational hazard management programme should enhance the external hazard mitigation measures in specific period. (See para 5.3.)

6.6. Hazard mitigation measures and coping strategies for external hazards should include the following elements:

- Identification of a realistic predictability or warning time for the applicable hazard,
- Identification of appropriate warning or monitoring systems and equipment for the applicable hazard,
- Characterization of the functional risk caused by the hazard, e.g., specific equipment that may need protection from the hazard,
- Development and implementation of an operational strategy for responding to events with warning, e.g., procedures required to support anticipatory actions,
- Development and implementation of a plant strategy for responding to events without warning e.g., response actions that may be required for a particular hazard such as debris removal following a tornado or seismic event,

– Development and implementation of communication standards and protocols with external organizations.

6.7. The operating organization should establish operating procedures that describe pre-event, event, and post-event actions corresponding to each external hazard. In some cases, there may be sufficient time to perform preparatory actions before the hazard impacts the site.

6.8. The operating organization should take actions for mitigating hazard effects propagation throughout the entire site prior to (for a forecasted event) or during an external hazard that impacts a vulnerable/sensitive portion of the site. This includes ensuring site ingress and egress routes that may be impacted from the hazard are available and useable. Operator personal safety should be taken into account, particularly during an event.

6.9. While the initiation of external hazards is generally unpredictable, conditions may occur where the potential for a hazard may increase (e.g., storm warnings, tornado warnings, extreme drought, movement of hazardous materials), and sufficient time is available to initiate mitigation measures. These measures should include actions to secure loose materials or unsecured equipment to minimize the hazard impact (for high winds, tornados, etc.), and the removal of items that could prevent proper site drainage (heavy rainfall, storm surges, etc.). Communication and notification protocols and standards with offsite organizations and agencies should be implemented, and they should ensure that plant operators are aware of the likelihood of a particular hazard.

6.10. Depending upon the predictability of the external hazard and communication with offsite organizations and agencies, plant shutdown or power reduction should be considered as a pre-event action, especially if there is potential for a station blackout or loss of ultimate heat sink.

6.11. Depending upon the expected severity of the external hazards, the operating organization should consider evacuating all non-essential plant personnel.

6.12. The operating organization should re-establish normal conditions and stand-down any additional staff deployed from normal duties in a controlled manner after the cancellation of a national or local hazard warning.

RECOMMENDATIONS FOR SPECIFIC EXTERNAL HAZARDS

6.13. Appendix B describes in more detail special recommendations that should be incorporated into the operational hazard management programme for the following commonly considered external hazards. For all external hazards, the general recommendations given in sections 6.1 through 6.12 are applicable. The following is a list of common external hazards consistent with DS490 [3] and DS498 [2]:

- Seismic Hazards
- Volcanic Hazards
- External Floods including Tsunami and Storm Surge
- External Floods from Rivers or Extreme Precipitation
- Extreme Winds including Tornados, Tropical Cyclones, Hurricanes, and Typhoons
- Other Meteorological Hazards (including Extreme Temperatures)
- Biological Phenomenon
- Collisions of Floating Bodies with Water Intakes and Ultimate Heat Sink Components
- External Fires and Explosions
- Accidental Aircraft Crash
- Electromagnetic Interference (including Solar Storm).

7. COMBINATION OF HAZARDS

7.1. The effects of combined hazards (i.e. two or more hazards whose effects occur simultaneously or within a specified or short timeframe) and mitigation strategies against them should be considered in the operational hazard management programme. The hazard 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 set of hazard combinations from first principles that are applicable to all plants. Instead, a screening process is required to determine those hazards that should be taken into account for a particular site.

7.2. The operational hazard management programme should include information on how credible combinations of hazards could alter the overall situation of the plant and include information on how this is handled. Combinations of hazards can alter hazard mitigating measures and coping strategies, operating procedures, special hazard mitigating equipment, required internal and external organizations, communication protocols, etc.

7.3. The hazard combination approach for hazard mitigation measures and coping strategies should be performance-based which defines a desired outcome and clear, measurable criteria to determine whether that outcome has been reached. This approach does not prescribe specific steps that should be taken as the potential combination of hazards is potentially limitless.

7.4. Hazard combinations should be consistent with the design of the plant and the local conditions at site. See Appendix C, DS494 [1], DS498 [2] and DS490[3] for guidance on determining hazard combinations.

7.5. The operating organizations should review their operating procedures for each individual hazard event taking into account the potential effects of the combinations of hazards considered applicable at the site. This is because operating procedures for separate hazards could contain conflicting instructions that would lead to confusion if the hazards were to occur in combination. For example, hazard mitigating equipment for a certain hazard may be stored in an area that is affected by another hazard so that the equipment cannot be used for its original purpose. Also, combination of hazards mean that additional or specific equipment may be needed.

7.6. If a combined hazard event occurs that has not been anticipated as part of the safety case, then the precautionary conservative decision-making principles should apply. For reactors operating at the time of the combined hazard, shutdown or power reduction should be considered on the basis of the operating organization performing the operational decision-making process. The plant operating personnel should then follow the site accident management plan in accordance with IAEA Safety Standards Series No. SSR-2/2(Rev.1), Safety of Nuclear Power

Plants: Commissioning and Operation [6], and Safety Report Series No.32, Implementation of Accident Management Programmes in Nuclear Power Plants [15].

7.7. The operating organization should be aware of the potential for the mitigation of one hazard causing the initiation of another hazard. For example, the use of water to extinguish an internal fire may cause internal flooding due to the potential accumulation of the fire extinguishing water. Examples are shown in Appendix C, which covers combinations of hazards.

7.8. Communication protocols with internal or external organizations may need to take combination of hazards into account. These communication protocols should be developed considering the effects of hazard combinations based on specific plant conditions. For example, different external organizations may be required for certain hazards. If there are multiple hazards, there may be more organizations involved in the response with different roles and responsibilities. These differing roles and responsibilities could be overlapping or even be conflicting with each other.

8. PERIODIC UPDATING OF OPERATIONAL HAZARD MANAGEMENT PROGRAMME

8.1. Section 4 ("Application of Defence in Depth") discussed the importance of a good understanding of hazards and their potential effects on the plant and maintaining the fundamental safety functions. This understanding should be obtained by the completion and routine updating of a comprehensive operational hazard management programme throughout the lifetime of the plant. This is consistent with the guidance given in IAEA Safety Standards Series No. NS-G-2.4 [16].

8.2. The operational hazard management programme should be taken into account in the initial plant design. It should be updated if additional hazards have been identified after the plant was constructed, during the operating stage, or as part of a re-licensing application, or for a periodic safety review (IAEA Safety Standards Series No. SSG-25, Periodic Safety Review for Nuclear Power Plants [17]).

8.3. The comprehensive operational hazard management programme should be considered an important part of the overall safety case for the plant and utilized as an input to operational decision making.

8.4. Although DS494 [1], DS498 [2] and DS498 [3] are intended as safety guides for new NPPs, these SSGs should be used for existing plants as a benchmark for comparison when designing plant modifications, and for gap analysis when carrying out a PSR in accordance with requirement 12 in IAEA Safety Standards Series No. SSR-2/2 (rev.1) [6].

8.5. The operational hazard management programme should be reviewed and updated if new information shows the existing design bases (or if applicable for existing reactor, design extension conditions) may be inadequate (See para 1.9.). An update should also be performed when the severity or vulnerability to a hazard has not been previously recognised.

8.6. The operating organization should consider industry operating experience, and new or updated information concerning the site-specific event assumptions since current information may indicate that design basis assumptions, hazard mitigation measures or coping strategies are not adequate. This includes the recognition that, cliff edge effects or challenges to multiple layers of defence in depth may not be identified or addressed. SSG-50 provides recommendations for implementing an operating experience programme to improve plant equipment, procedures and training by learning from hazard events that have already occurred at the installation or elsewhere. [4].

8.7. The operating organization should recognise and address conditions of low margin to external hazard mitigation, taking into account cliff edge effects.

8.8. The operating organization should consider and address, in the periodic updating of the operational hazard management programme, SSCs important for hazard mitigation including portable emergency equipment and passive design features..

8.9. Procedures and training for hazard coping and mitigation strategies and measures should be validated and consistent with updated or new design assumptions and/or analysis.

8.10. Hazard coping strategies should be considered and updated for changes to the physical and social infrastructure around the plant. Examples include contact information with external organizations, changes in local population sizes and proximity to the site, electrical grid interfaces, changes of transportation routes, changes of local industries, and hydrological and geological changes.

8.11. The potential for multiple unit effects from hazards should be addressed since these may change over time. (e.g. extreme wind could cause the loss of off-site power if the switchyard is shared between the units or neighbouring units may have changed their state and now present different hazards, etc.)

8.12. Changes to the NPP during its lifetime (both equipment and organization) should be reflected in the operational hazard management programme. This should be reviewed and updated following any plant modification, periodically, and at times as specified by the regulatory body.

8.13. If proposed solutions to potential hazard impacts are not implemented, the justification for not implementing the solutions should be reviewed and documented. Additionally, the technical justification should describe compensatory features provided to maintain an acceptable level of safety, where applicable.

9. CONTROL OF MATERIALS AND HOUSEKEEPING

9.1. The operational organization should understand that the management and control of materials and the control of plant housekeeping on a routine basis can have a great impact on the progression of hazards and their consequences.

9.2. Plant walkdowns should be performed on a regular schedule, at times when external hazards have been forecast, and after external hazards are experienced. General examples are listed below. Some of these actions are of particular importance at times when an external hazard (such as extreme winds or flooding) is forecast, but proper housekeeping should be in effect at all times:

- Ensuring that culverts are kept clean immediately prior to a predicted major external flooding can have a significant impact on the ability of the site drainage systems to dewater the site.
- Ensuring loose materials (especially metallic objects) are cleared away or tied down can affect the potential airborne missiles in the eventual hazard.

Further examples of actions that need to be taken, and checked during these walkdowns, have been given in Appendices A and B.

9.3. The operational hazard management programme for the plant should identify the measures needed for the management of materials and enhanced housekeeping in accordance with requirement 28 in IAEA Safety Standards Series No. SSR-2/2 (rev.1) [6]. These include controls on procurement and choice of materials, controls over transient accumulations, and controls over the way maintenance and construction are performed.

9.4. The basic principles of material control and plant housekeeping should be supported by adopting appropriate measures to improve human behaviours such as staff hazard awareness training, toolbox talks, pre-job briefs, and by compliance checks, including workplace walkdowns and inspections.

9.5. The operational hazard management programme should include controls over the current state of the various work areas which should be enhanced at times of increased risk, for example if a hazardous event is predicted.

9.6. Housekeeping of routine plant work areas or construction areas should include specific activities to increase hazard resilience by protecting essential equipment, or moving them to safer areas of the plant, etc.

9.7. Housekeeping controls should be enhanced at different times throughout the lifetime of the NPP, for example just prior to coming out from an outage.

10. INSPECTION, MAINTENANCE, AND TESTING OF HAZARD PROTECTION AND MITIGATION MEASURES

10.1. A comprehensive programme should be established and implemented to perform inspections, maintenance, and testing of hazard protection and mitigation measures identified in the hazard analysis in accordance with requirement 31 in IAEA Safety Standards Series No. SSR-2/2 (rev.1) [6] and IAEA Safety Standards Series No. NS-G-2.6, Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants [18].

10.2. The prevention and the mitigation of most internal and external hazards are performed by conservative design. Therefore, the maintenance of hazard mitigation design features should be included in operational condition surveillance programmes.

10.3. The operating organization should develop and maintain a list of hazard protection measures that are relevant for the site and that require inspection, maintenance and testing. The inspection, maintenance and testing programme for the site should include general hazard protection measures and protection measures that are required for specific hazards.

10.4. General hazard protection measures that should be inspected, maintained, and tested include the following:

- hazard detection and alarm systems;
- communication systems for use in hazard events;
- emergency lighting systems;
- emergency vehicles;
- access and escape routes for hazard response personnel;
- respirators and protective clothing for radiological applications.

10.5. Special considerations for off-site equipment dedicated to hazard mitigation should include:

- Equipment provided by external organizations or stored in an offsite location need to be included in an inspection, maintenance, and testing programme.
- Maintenance and inspection procedures need to include the additional onsite and off-site engineered equipment which may be utilized in hazard mitigation and coping strategies.
- For predictable or partially predictable hazards, the operating organization should consider pre-event inspection and/or testing on hazard mitigation equipment to ensure the availability of the equipment when the hazard event occurs.

11. TRAINING OF PERSONNEL

11.1. Before starting work, all personnel including staff of operating organization and contractor personnel temporarily assigned to the plant should receive training in hazards that may affect the plant. Training of personnel should be performed in accordance with requirement 7 in IAEA Safety Standards Series No. SSR-2/2 (rev.1) [6] and the guidance in IAEA Safety Standards Series No. SSG-XX, Qualification and Training of Personnel for Nuclear Power Plants [19].

11.2. Specialized hazard training should be established for designated personnel involved in operations, maintenance and hazard mitigation activities at the plant, including contractor personnel temporarily assigned to the plant, where applicable. The level of training provided should be tailored to the role undertaken by the individual or group, so there may need to be differing training courses provided to different groups.

11.3. The training programme should provide training to ensure that the staff have adequate technical skills commensurate with their roles in the operational hazard management programme and familiarity with the detailed procedures to be followed. Training should be sufficient to ensure that individuals understand the significance of their duties and the consequences of errors arising from misconceptions or lack of diligence.

11.4. This hazard training should include information regarding their responsibilities prior to, during, and following hazards events:

a. Hazards safety principles at the plant, and roles and responsibilities;
b. General awareness of specific hazards. This aspect is further developed in paragraph 11.5.
   - Recognition of audible and visual alarm signals including fire alarms, tsunami warnings, and other alarms as applicable to the site;
   - The means of exit and emergency evacuation routes in the event of an internal or external hazard;
   - The need to delay or discontinue certain plant activities in case specific external hazards are predicted such as extreme ambient temperatures, flooding, or extreme wind; including the means of reporting hazards and actions to be taken to make work safe;
   - The different types of portable or resilience equipment provided and their use in mitigating hazard effects in the initial stage. This may include fire-fighting equipment, aqua dams and dam boards, and special communication equipment such as satellite phones.

11.5. The specific hazard awareness training programme should cover the following:

For all hazards:

(a) The importance of maintaining the integrity and operability of plant protection features (both passive and active) by performing regularly scheduled inspections, routine and unplanned maintenance of equipment, and periodic functional tests of equipment and systems;
(b) The design and operating details of the specific hazard protection features installed in the plant to permit effective maintenance of equipment for operability;
(c) The significance of planned design changes and plant modifications with respect to hazards, including both direct and indirect impacts on nuclear safety and any effects on the integrity or operability of the hazard protection features (both passive and active) as a result of the planned modifications;
(d) The need to ensure that the individual who is responsible for the review of planned design changes and plant modifications is sufficiently knowledgeable to recognize issues that may have implications for hazard protection features; this necessitates detailed knowledge of the design and testing requirements of hardware for hazard protection and knowledge of specific design objectives for hazard protection features in each area of the plant, as specified in the hazard safety case or similar documentation;
(e) Familiarization with the physical location of SSCs important to safety, preferably through a plant walkdown;
(f) Familiarization with the physical location of plant hazard protection features.

For fire (including the above):

(a) the need to control combustibles and ensure that area limitations on fire loadings are met,

(b) Awareness of potential ignition sources, and controls over them – for example with hot work procedures,

(c) Passive fire protection: the importance of fire doors, barriers and penetrations and for working practices that respect these.

For flood external to the buildings (including the above):

(a) the role of watertight doors and the need for them to be kept closed by default to protect against external flooding.

11.6. Because certain activities may lead to additional risk involving internal or external hazards, training for personnel who initiate or authorize these activities should be provided. Some examples of these types of additional risk are provided in paras 11.8 and 11.8 below.

11.7. Personnel who initiate or authorize work activities involving hot work and staff who may be assigned the duties of a fire watch should be trained to ensure that they are made aware of the following:

(a) The hazards associated with activities such as cutting and welding which could produce a potential ignition source;
(b) The stipulations of the work permit system, specific situations in which a fire watch is necessary, and the significance of introducing potential ignition sources into fire areas containing components identified as important to safety;
(c) instructions on work implementation and general fire safety training so that they can readily recognize various fire hazards in the plant and can understand the implications of introducing combustible materials or ignition sources into safety related areas;

11.8. Personnel who initiate or authorize work activities involving radioactive materials transport should be trained to ensure they are made aware of the following:

(a) The ambient conditions that form part of the safe operating envelope for individual fuel or waste packages and the requirement to ensure that these values are not exceeded during movement operations.
(b) The method by which the site receives and communicates information on forecasting for events such as extreme wind, flooding, and other hazards that could affect the plant operator’s ability to carry out the fuel or waste movement safely.
(c) Actions to take if a seismic event occurs during a fuel or waste movement operation to ensure the integrity of the transport package has not been compromised and that the receiving facility has not been damaged and is still able to accept the fuel or waste transfer.

REFERENCES

[1]. INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-64, IAEA, Vienna (Under publication, DS494).

[2]. INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Installations, IAEA Safety Standards Series No. SSG-XX, IAEA, Vienna (Under revision, DS498)

[3]. INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design of Nuclear Installations, IAEA Safety Standards Series No. SSG-XX, IAEA, Vienna (Under revision, DS490).

[4]. INTERNATIONAL ATOMIC ENERGY AGENCY, Operating Experience Feedback for Nuclear Installations, IAEA Safety Standards Series No. SSG-50, IAEA, Vienna (2018).

[5]. INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Safety for Existing Nuclear Installations, Safety Standards Series No. NS-G-2.13 (2009).

[6]. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2 (Rev.1), IAEA, Vienna (2011).

[7]. INTERNATIONAL ATOMIC ENERGY AGENCY, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

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

[9]. INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

[10]. INTERNATIO NAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

[11]. FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVILAVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERIGAN HEALTH

ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[12]. INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).

[13]. EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERIGAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

[14]. INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG Series No.10, IAEA, Vienna (1996).

[15]. INTERNATIONAL ATOMIC ENERGY AGENCY, Implementation of Accident Management Programmes in Nuclear Power Plants, Safety Report Series No.32, IAEA, Vienna (2004).

[16]. INTERNATIONAL ATOMIC ENERGY AGENCY, The Operating Organization for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.4, IAEA, Vienna (2002).

[17]. INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-25, IAEA, Vienna (2013).

[18]. INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-XX, IAEA, Vienna (Under revision, DS497E).

[19]. INTERNATIONAL ATOMIC ENERGY AGENCY, Requirement, Qualification and Training of Personnel for Nuclear Power Plants, IAEA Safety Standards Series SSG-XX, IAEA, Vienna (Under revision, DS497F).

[20]. INTERNATIONAL ATOMIC ENERGY AGENCY, Earthquake Preparedness and Response for Nuclear Power Plants, Safety Series Report No. 66, IAEA, Vienna (2011).

APPPENDIX A - EXAMPLE OF THE OPERATIONAL HAZARD MANAGEMENT PROGRAMME FOR INTERNAL HAZARDS

This Appendix provides recommended elements of an operational hazard management programme to mitigate and cope with specific internal hazards. General recommendations for mitigating and coping with internal hazards are provided in Section 5.

A.1 INTERNAL FIRES

A.1.1. The operational organization should establish an on-site group with the specific responsibility for ensuring the continued effectiveness of the fire safety arrangements. Responsibility for co-ordinating fire safety activities should be assigned to an individual staff position, generally referred to as the fire safety co-ordinator.

A.1.2. The fire safety co-ordinator should retain the responsibility for ensuring that all fire safety activities and functions necessary for safety are effectively co-ordinated to achieve the objectives of the fire prevention and protection programme.

A.1.3. To ensure adequate fire safety, an appropriate level of defence in depth for internal fire hazards should be maintained throughout the lifetime of the plant, through the fulfilment of the following three principal objectives:

(1) Preventing fires from starting;

(2) Detecting and extinguishing quickly those fires which do start, thus limiting the damage; and

(3) Preventing the spread of those fires which have not been extinguished, thus minimizing their effects on essential plant functions.

A.1.4. By satisfying the above objectives, the following should be ensured:

—the probability of a fire occurring is reduced to as low as reasonably practicable;

— SSCs important to safety and hazard protection and mitigation features are adequately protected to ensure that the consequences of a single fire will not prevent those systems from performing their required function, account being taken of the effects of a single failure.

A.1.5. Procedures should be established for the purpose of ensuring that amounts of combustible materials (the fire load) and the numbers of ignition sources be minimized in areas containing items important to safety and in adjacent areas that may present a risk of exposure to fire for items important to safety.

A.1.6. A comprehensive fire hazard analysis should be performed for the plant in order to do the following:

—demonstrate the adequacy of existing fire protection measures (both passive and active) to protect areas identified as important to safety for all operational states;

—identify any specific areas where levels of fire protection are inadequate and where corrective measures are necessary;

—provide a technical justification from the recommended practices (IAEA Safety Series No. SSG-64, Protection against Internal Hazards in the Design of Nuclear Power Plants [1]) for which no corrective measures are taken.

The fire hazard analysis should be updated regularly over the lifetime of the plant.

A.1.7. Any modification that may affect, directly or indirectly, the installed fire safety measures, including the manual fire-fighting capability, should be subject to a procedure for controlling modifications. Such a procedure for modifications should provide assurance that there will be no detrimental effects on the installed fire safety measures or on the ability to provide an effective manual fire-fighting capability in those areas for which fire safety measures are identified as necessary to maintain safety.

A.1.8. The technical justification from recommended practice (IAEA Safety Series No. SSG-64 [1]) that is identified when the fire hazard analysis is updated should include a discussion of the plant modifications that would be necessary to follow accepted practice and the reasons why it is not reasonably practicable to implement such modifications. The technical justification should also describe compensatory features provided to maintain an acceptable level of safety, where applicable.

A.1.9. A review of implications for fire safety should be carried out for the following modifications to the plant:

— modifications to the fire protection features;
— modifications to the protected items important to safety or systems that could adversely affect the performance of the fire protection features;
— any other modification that could adversely affect the performance of the fire protection features, including modifications affecting area fire loading.

A.1.10. A formal review system to evaluate the impacts of modifications on fire safety should be incorporated into the overall modification procedure. Alternatively, a separate procedure should be established and implemented specifically for reviews for fire protection. Modifications should not be commenced until the review has been completed.

A.1.11. The staff assigned the responsibility for carrying out such reviews for issues of fire safety should be suitably qualified to evaluate the potential effect of any modification on fire safety and have sufficient authority to prevent or suspend modification work, if necessary, until any issues identified have been satisfactorily resolved.

A.1.12. Plant modifications should only be carried out on the authority of a work permit issued by a person who is competent in and knowledgeable of the implications for fire safety.

A.1.13. If a modification necessitates the removal from service of any of the fire protection features, careful consideration should be given to the consequent reduced level of protection of item(s) important to safety or hazard protection and mitigation features, and appropriate temporary arrangements should be made to maintain adequate protection against fires. On completion of the modification, the plant as modified should be inspected to confirm its compliance with the modified design. In the case of an active system, the plant as modified should be commissioned and placed into or returned to normal service, as applicable.

A.1.14. The fire hazard analysis should be reviewed and updated to reflect the modification, as appropriate.

A.1.15. Written procedures should be established and enforced to minimize the amount of transient (i.e. non-permanent) combustible materials, particularly packaging materials, in areas identified as important to safety. Such materials should be removed as soon as the activity is completed (or at regular intervals) or will be temporarily stored in approved containers or storage areas.

A.1.1.6. The total fire load due to combustible materials in each area identified as important to safety should be maintained as low as reasonably practicable, with account taken of the fire resistance rating of the compartment boundaries. Records should be maintained that document the estimated or calculated existing fire load as well as the maximum permissible fire load in each area.

A.1.17. The use of combustible materials in the furnishings of the power plant should be minimized. Combustible materials should not be used for decorative or other non-essential effect in areas identified as important to safety.

A.1.18. Administrative controls should be established and implemented to ensure that areas important to safety are inspected periodically in order to evaluate the general fire loading and plant housekeeping conditions, and to ensure that means of exit and access routes for manual fire-fighting are not blocked. Administrative controls should also be established and implemented to ensure that the actual fire load is kept within permissible limits.

A.1.19. Administrative procedures should be established and implemented to provide effective control of temporary fire loads in areas identified as important to safety during maintenance and modification activities. These procedures should cover combustible solids, liquids and gases, their containment and their storage locations in relation to other hazardous material such as oxidizing agents. These administrative procedures should also include a procedure for issuing work permits that requires in-plant review and approval of proposed work activities prior to the start of work to determine the potential effect on fire safety. The on-site staff member responsible for reviewing work activities for potential temporary fire loads should determine whether the proposed work activity is permissible and should specify any additional fire protection measures that are needed (such as the provision of portable fire extinguishers or the use of a fire watch officer, as appropriate).

A.1.20. Administrative procedures should be established and implemented to control the storage, handling, transport and use of flammable and combustible solids and liquids in areas identified as important to safety. The procedures should be established in accordance with national practice and should provide controls for solids and liquids. For solids:

(a) The use of combustible materials (such as wooden scaffolding) should be restricted. Where wooden materials are permitted, they should be chemically treated or coated so as to be fire retardant.

(b) The storage of combustible materials such as charcoal filters and dry unused ion exchange resins should be restricted; large stocks of such materials should be placed in a designated storage area with appropriate fire rated compartmentation and fire measures provided.

(c) The storage of combustible materials such as papers and protective clothing should be restricted; large stocks of such materials should be placed in designated storage areas with appropriate fire rated compartmentation and fire protection measures provided.

(d) The storage of all other combustible materials should be prohibited.

For liquids:

(i) The amounts of flammable or combustible liquids introduced into fire areas during maintenance or modification activities should be limited to the amount needed for daily use. Suitable fire protection measures such as the provision of hand-held fire extinguishers should be taken, as appropriate.

(ii) Approved containers or dispensers should be used whenever possible for the transport and use of flammable or combustible liquids. Openings in containers should be fitted with spring loaded closures. Transport of flammable or combustible liquids in open containers should be avoided.

(iii) If it is necessary to store small amounts of flammable or combustible liquids within a working area, cabinets of an approved design for flammable liquids should be used.

(iv) All containers of flammable or combustible liquids should be clearly and prominently labelled to indicate their contents.

(v) Stores of large quantities of flammable or combustible liquids should be located and protected such that they should not compromise safety. Such bulk storage areas should be separated from other plant areas by fire rated compartmentation or by spatial separation with suitable fire protection measures taken as appropriate.

(vi) Warning signs should be placed at storage areas for flammable or combustible liquids.

A.1.21. Administrative procedures should be established and implemented to control potential ignition sources throughout the plant. The procedures should include controls to:

— restrict personnel smoking to designated safe areas and to prohibit personnel from smoking in all other areas;
— prohibit the use of open flames for testing heat or smoke sensing devices (such as fire detectors) or for leak testing purposes;
— prohibit the use of portable heaters, cooking appliances and other such devices in areas identified as important to safety;
— limit the use of temporary wiring.

A.1.22. Procedures should be established to ensure that, before any hot work is attempted, the immediate work area and adjacent areas are inspected for the presence of combustible materials and that the operability of necessary fire protection measures is confirmed. If the configuration and design of the work area may permit the spread of sparks or slag beyond the initial work area, spaces both above and below the work area should be checked, and any combustible materials should be either removed to a safe area or suitably protected.

A.1.23. During hot work, regular inspections should be made to ensure that the conditions of the permit are observed, that there are no exposed combustible materials present, and that the fire watch is on duty (if a fire watch has been stipulated in the permit).

A.1.24. In cases where the hot work permit identifies the need for a fire watch, the following procedures should be followed:

(a) The fire watch should be on duty in the immediate vicinity before any hot work is attempted, the work should be stopped if the fire watch leaves the work area, and the fire watch should remain in the work area for an appropriate period after open flame work is completed.

(b) While the work is in progress the fire watch should perform no other duties.

(c) Suitable dedicated fire-fighting equipment should be readily available and means should be provided by which additional assistance can be readily obtained, if necessary. Adequate access routes for fire fighters should be maintained.

A.1.25. Any equipment or vehicle in use in areas in which a flammable gas could be released should be appropriately qualified for use in explosive atmospheres.

A.1.26. The use of compressed gas cylinders for cutting or welding operations or other hot work should be controlled by a system of work permits.

A.1.27. Warning signs should be erected at the entrances to areas containing combustible materials to warn personnel of restrictions or access requirements and of the necessity to permanently control ignition sources.

A.1.28. The inspection, maintenance and testing programme should cover the following fire protection measures:

- passive fire rated compartment barriers and structural components of buildings, including the seals of barrier penetrations;
- fire barrier closures such as fire doors and fire dampers;
- locally applied separating elements such as fire-retardant coatings and cable wraps;
- flammable gas detectors;
- water based fire extinguishing systems;
- a water supply system including a water source, a supply and distribution pipe, sectional and isolation valves, and fire pump assemblies;
- gaseous and dry powder fire extinguishing systems;
- portable fire extinguishers;
- smoke and heat removal systems and air pressurization systems;
- manual fire-fighting equipment.

A.1.29. A fire-fighting strategy should be developed for each area of the plant identified as important to safety (including those areas, which present a fire exposure risk to areas important to safety). These strategies should provide information to supplement the information provided in the general plant emergency plan. The strategies should provide all appropriate information needed by fire fighters to use safe and effective fire-fighting techniques in each fire area. The strategies should be kept current and should be used in routine classroom training and in actual fire drills at the plant. The fire-fighting strategy developed for each fire area of the plant should cover the following:

- access and exit routes for fire fighters;
- locations of structures, systems or components identified as important to safety; — fire loadings;

- particular fire hazards, including the possible reduced capability for fire-fighting due to external events;
- special radiological, toxic, high voltage and high -pressure hazards, including the potential for explosions;
- the fire protection features provided (both passive and active);
- restrictions on the use of specific fire extinguishing agents because of concerns about nuclear criticality or other particular concerns, and the alternative extinguishing media to be used;
- locations of heat and/or smoke sensitive components or equipment important to safety;
- location of fixed and portable extinguishing equipment;
- water supplies for manual fire-fighting;
- communication systems (not affecting items important to safety) for use by fire-fighting personnel.

A.1.30. Plant documentation should provide a clear description of the manual fire-fighting capability provided for those areas of the plant identified as important to safety. The manual fire-fighting capability may be provided by a suitably trained and equipped on-site fire brigade, by a qualified off-site service or by a co-ordinated combination of the two, as appropriate for the plant and in accordance with national practice.

A.1.31. If reliance is placed on off-site response, designated plant personnel in each shift should be assigned the responsibility to co-ordinate and liaise with the off-site fire-fighting service and to establish a clear line of authority at the fire scene. Appropriate plant personnel should be designated even in situations in which the off-site response is supplementary to a primary response by a qualified on-site fire brigade.

A.1.32. Where full or partial reliance for manual fire-fighting capability is placed on off-site resources, there should be proper co-ordination between the plant personnel and the off-site response group in order to ensure that the latter is familiar with the hazards of the plant. The responsibilities and lines of authority for manual fire-fighting personnel should be documented in a fire-fighting plan.

A.1.33. If an on-site fire brigade is established to provide a manual fire-fighting capability, the fire brigade’s organization, minimum staffing level, equipment (including self-contained breathing apparatus) and training should be documented and their adequacy should be confirmed by a competent person.

A.1.34. Members of the on-site fire brigade should be physically capable of performing fire-fighting duties and should attend a formal programme of fire-fighting training prior to assignment to the plant fire brigade. Regular training (routine classroom training, fire-fighting practice and fire drills) should be provided for all on-site fire brigade members.

Special training should be provided for fire brigade leaders to ensure that they are competent to assess the potential safety consequences of a fire and advice control room personnel.

A.1.35. If manual fire-fighting represents the primary means of fire protection, it should be ensured, as far as possible, that the necessary actions in the event of fire can be carried out safely in terms of radiological protection.

A.1.36. Fire protection features are not generally classified as hazard protection and mitigation features and thus they may not be subject to the rigorous qualification requirements and the associated quality assurance programme applied to hazard protection and mitigation features. However, fire has the potential to give rise to common cause failure and thus to pose a threat to safety, and therefore the installed active and passive fire protection measures should be considered as important to safety. An appropriate level of quality assurance should therefore be applied to fire protection features.

A.2 INTERNAL EXPLOSIONS

A.2.1. The operating organization should consider various explosion sources when preventing, detecting, and mitigating internal explosions. Potential sources of internal explosions may be related to the use or the generation of explosive gases. There is also a potential for dust or oil mist explosions although these are judged less likely. Additionally, events leading to an energy release similar to an explosion may also come from High Energy Arc Flashes in high voltage equipment. Explosion events may also occur in conjunction with other hazards, such as fire. Section 7 and Appendix C gives additional guidance on combined and consequential hazards.

A.2.2. Internal Fires and Internal Explosions are similar hazards and, in developing an operational hazard management programme the recommendations from Appendix A.1 should be reviewed. As with fires, there should be enhanced controls over materials and operations during times of increased explosion risks.

A.2.3. Active and passive protection systems (such as blast doors, blowout panels, room and area ventilation systems, etc.) should be subject to the inspection, maintenance and testing regimes identified in the operational hazard management programme.

A.2.4. Operating procedures should play a role in preventing explosion events such as area ventilation procedures or area or system isolation procedures, and in any post-explosion event.

A.2.5 Administrative procedures should be established and implemented to control the delivery, storage, handling, transport and use of flammable and explosive materials, including the types, quantities, and locations of gases throughout the plant. The procedures should be established in accordance with national practice and should be implemented to ensure that:

(a) Containers of compressed gases that sustain fires, such as oxygen, are properly secured and are stored separately from flammable gases and away from combustible materials and ignition sources;

(b) Where a supply of flammable gas is needed inside a building for permanent use, it is supplied from cylinders or a bulk storage area safely located outside the building in a dedicated storage area such that a fire affecting the storage area would not compromise safety.

A.2.6. Control of ignition sources is the main prevention measure for internal explosions. Therefore, administrative procedures should be established and implemented to control maintenance and modification activities that necessitate the use of a potential ignition source or that may themselves create an ignition source. The performance of such work will be controlled by means of formal written procedures, i.e. by means of either the work permit system discussed earlier or a special system for hot work permits. The provisions discussed in A.1.22-24 are applicable.

A.2.7. In areas containing items important to safety, work which involves the use of a potential ignition/explosion source or which may create ignition sources should be permitted only after consideration of the possible consequences for safety. For example, such work may be prohibited from occurring simultaneously on functionally redundant components important to safety or in the areas containing such components.

A.2.8. The operating organization should control and/or limit personnel access in areas where explosion hazards could occur such as main and auxiliary transformer areas.

A.3 MISSILES

A.3.1. Potential missile sources exist at all NPPs. The operating organization efforts should concentrate on ensuring the integrity of potential missile sources and of engineered barriers is maintained so that missile generation and hazard propagation are unlikely and limited in extent, should the hazard occur and is mitigated before it affects essential plant or system functions.

A.3.2 Operating procedures should be developed and implemented to identify potential missile hazards before they occur and include the following:

- Regular plant area walkdowns to detect potential missile hazards;
- Observation of personnel interacting with potential missile sources;

- Rotating machinery inspections;
- Regular turbine blade inspections for turbine blade fatigue;
- Inspection of storage areas of high-pressure gas bottles and the integrity of the gas bottles themselves.

A.3.3. The operating organization should control and/or limit personnel access in areas where missile hazards could occur.

A.3.4. The operating organization should establish operating procedures that describe actions following early identification of potential missile events at the site. These indications of a potential missile event may include output from vibration monitors or reports of unusual sounds. Indication that an event has occurred may come from direct observation of missile effects by plant personnel, or video monitoring of plant areas.

A.3.5. Operating procedures after missile events should include short-term and long-term actions such as plant walkdowns to determine the missile impact on the functionality of SCCs important to safety.

A.3.6 . Much of the protection provided against the effects of missile hazards is from basic layout decisions in design, and by passive hazard protection such as engineered barriers. The passive features should be subject to the inspection, maintenance, and testing regimes identified in the operational hazard management programme (see section 3), and to plant surveillance programmes (see section 10).

A.4 COLLAPSE OF STRUCTURES AND FALLING OBJECTS

A.4.1. Analysis of these hazards should be performed in accordance with DS494 [1]. Although this is written as a safety guide for the design of new NPPs, it specifically says it should be expected for existing plants that the safety assessments of such designs a comparison will be made with the current standards to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements. Typically, the prevention of structural collapses and falling objects from crane lifts is largely through conservative design. Nevertheless, falling objects from cranes and other lifting equipment should be considered a potential hazard. Non-crane related load drops from heights may be related to mishandling of other heavy objects at height.

A.4.2. Hazard protection and mitigation measures should include load cells on hoists, fall zone controls, and crane and lifting equipment travel limit switches.

A.4.3. The operating organization should establish procedures for planning hoisting and lifting activities. Planning of these activities should include risk assessments, pre-planned lifting routes, defining of restrictions, and interlocking of lifting routes, as applicable. In some cases where there may be unclear lifting instructions, trial lifts should be considered.

A.4.4. Communication protocols should be established between plant operators in the main control room and personnel controlling and performing the lifts where required.

A.4.5. The operating organization should establish operating procedure actions to implement the hazard mitigating measures and coping strategies when there is a high risk of damage or multiple hazard impacts (i.e. fire, flooding, etc.) following a dropped load.

A.4.6. The operating organization should establish operating procedures for performing regular walkdown and inspection of areas and structures where collapses and falling objects may occur, especially for those areas which are located outside plant buildings.

A.5 PIPE BREAKS

A.5.1. Pipe breaks (or pressure part failure) is associated with a variety of resulting hazard phenomena, including pipe whip impacts, room pressurisation, jet effects, and flooding. The extent of each of these phenomena depends on the fluid involved, and its temperature and pressure. The operating organization should ensure the control of plant configuration for the plant piping including engineered structures designed to minimize the impact of pipe breaks is maintained at all times in accordance with requirement 10 in IAEA Safety Standards Series No. SSR-2/2 (rev.1) [6]. The ageing management programme should incorporate the appropriate aspects of pipe integrity and be included in the operational hazard management programme.

A.5.2. The operating organizations should periodically walk down plant areas to confirm that the plant conditions correspond to those stated in the design, including; identification of items that hinder or make ineffective leak detection devices, proper closure of compartment doors, and proper installation of protective covers. These periodic walkdowns should also include the identification of general pipe and piping component degradations, and steam and water leaks. Also included in these NPP operator walkdowns should be engineered barrier integrity, pipe whip restraints, pipe hangars, blast doors, and blowout panels.

A.5.3. Apart from the operating procedures associated with preventive actions, there should be procedures related to the implementation of actions in the event of pipe whip impacts, room pressurisation, or jet effects, and that should include implementation of hazard coping strategies.

A.6 INTERNAL FLOODS

A.6.1. Internal floods at an NPP may be caused by pipe breaks, tank breaches, open valves, or operation of firefighting water. These may also be the indirect effects of challenges from external hazards such as earthquakes or external floods. The operating organization should ensure the integrity of engineered structures and barriers that are designed to minimize the impact of internal flooding is maintained at all times.

A.6.2. Enhanced operational controls during maintenance or construction activities should be put into place during times of increased flooding risks (e.g. temporary water hoses during outage period).

A.6.3. Operational controls should include inspections of water-based systems for integrity before returning them to service and that any temporary modifications to drains, including temporary covers, have been restored to the pre-work conditions.

A.6.4. Protection and mitigation measures against internal flooding hazards should include level detection systems, engineered drainage routes, water proofing measures to prevent flooding, and protection covers or embankments around critical structures and components to prevent water spreading to other areas of the plant in an uncontrolled manner. Mitigation of internal flooding should be achieved in part by design choices with respect to the layout of the plant, therefore, some flood scenarios are naturally self-limiting (for example where the flood is limited to the contents of a single tank), whereas others may actions by plant personnel are assumed.

A.6.5. General housekeeping rules control debris in drain systems, but inspections and plant walk downs should check the general condition of drainage systems.

A.6.6. The operating organization should establish operating procedures for the detection and mitigation of internal floods. Procedures should include instructions for the isolation of leaking systems and flooded rooms, and the potential use of deployable pumping equipment to drain flood water.

A.7 RELEASE OF HAZARDOUS SUBSTANCES

A.7.1. Releases of on-site hazardous substances are generally viewed as unlikely, limited in extent should they occur, and can be avoided before they affect essential plant functions. However, the operating organization should consider the effects of hazardous substances on plant operators carrying out important actions, and in particular the habitability of the main control room.

A.7.2. The operating organization should establish operating procedures that describe actions following indications of a hazardous substance release at the site. Entry into these procedures is typically based upon indications from a gas detection system, or from direct reports from plant personnel. The operating procedures should have the objective of limiting exposure to personnel through the event and timely recovery after the release has dispersed.

A.7.3. From an on-site release, operating procedures should include isolation of damaged systems or storage tanks, isolation of rooms with non-habitable atmospheres, preservation of habitable atmospheres in the main control rooms, and may include a partial evacuation process for site staff. There should be considerations of the need for on-site safety equipment (e.g. breathing apparatus, protection suit) to allow operators to move to places of safety.

A.7.4. Protection and mitigation measures against the effects of internal release of hazardous substances is largely by passive means, (e.g. redundancy of rooms or systems, administrative requirements, etc.). Operating procedures should include provisions to shut inlet dampers to the main control room ventilation system if required, and may also include other controls over ventilation flows.

A.8 ELECTROMAGNETIC INTERFERENCE

A.8.1. All potential sources of Electromagnetic interference (EMI) in the plant should be identified. Significant sources of EMI can be eliminated by proper design, construction, and maintenance of instrumentation and control systems. Other potential sources may include maintenance or construction equipment and activities such as portable arc welding equipment, portable radio communications or telephony brought into the nuclear plant, and ground penetrating radar used for ground surveys.

A.8.2. Within the operational hazard management programme, identification of potential EMI hazards should account for all potential sources during normal or special maintenance periods or other plant activities.

A.8.3. The EMI identification process should include the potential location of permanent and temporary sources of EMI, where possible, and focus on sources close to sensitive equipment.

A.8.4. The EMI identification process should contain controls for portable or temporary EMI sources. These controls should include the location and timing of maintenance and construction activities, and exclusion zones or other administrative or operational controls to minimize an EMI hazard, including cellular phones.

A.8.5. The persons responsible for the activities where EMI may be generated should have a role in hazard management of EMI. Communications between operators and those carrying out the work may be necessary to terminate the generation source and stop further effects on the plant.

APPPENDIX B - EXAMPLE OF THE OPERATIONAL HAZARD MANAGEMENT PROGRAMME FOR EXTERNAL HAZARDS

This Appendix provides recommended elements of an operational hazard management programme to mitigate and cope with specific external hazards. General recommendations for mitigating and coping with external hazards are provided in Section 6.

B.1 Seismic Hazards

B.1.1. To ensure this external hazard is completely included in the operational hazard management programme, the operating organization should consider and include the guidance given in IAEA Safety Standards Series DS490, Seismic Design and Qualification for Nuclear Power Plants [3] and NS-G-2.13, Evaluation of Seismic Safety for Nuclear Installations [5].

B.1.2. The operating organization should use the insights given in Safety Series Report No. 66, Earthquake Preparedness and Response for Nuclear Power Plants [20] in the development of an earthquake response plan for pre-event and post-event actions. These event actions take the form of procedures that describe short-term and long-term actions and include system and component walkdowns to determine the status and functionality hazard protection and mitigation features. Entry into these actions is based upon indications from the seismic monitoring system, offsite geological centres, or ground motion experienced by plant personnel. Insights for plant shutdown is provided in the Safety Series Report.

B.1.3. As a pre-event action, the operating organization should maintain plant housekeeping at acceptable levels to ensure earthquake damage is not propagated or increased by extraneous debris or loose items. This pre-event action should include securing equipment (through seismic restraints) that may become damaged or cause damage during a seismic event.

B.1.4. If the plant is shutdown after an earthquake event, the operating organization should ensure long-term shutdown operational safety after the safe shutdown. Items to be considered are emergency diesel generator fuel supplies, plant back feed power supply integrity, control room habitability, and the restoration or possible repair of disabled/damaged items important to safety and hazard protection and mitigation features.

B.1.5. As appropriate, communication protocols with offsite geological monitoring centres should be established for redundant seismic notifications.

B.2. Volcanism

B.2.1. To ensure this external hazard is completely included in the operational hazard management programme, the operating organization should consider and include the guidance given in IAEA Safety Standards Series DS498 [3].

B.2.2. The operating organization should establish communication protocols and standards with national or local agencies to have sufficient warning of volcanic activity and the potential transport of volcanic ash and toxic gases.

B.2.2. The operating organization should determine if a plant shutdown is required due to volcanic activity.

B.2.3. Operating procedures should be developed and implemented for the inspection and removal of volcanic ash on or near SSCs. Special considerations should include equipment affected by volcanic ash deposition impacting ventilation and structural loading.

B.2.4. Operating procedures should be developed and implemented to inspect and maintain the functions of automatic screen wash equipment to prevent blockage of water intake facilities and pumps.

B.2.5. Operating procedures should be developed and implemented to monitor the differential pressures of HVAC filters and the main control room. These procedures include cleaning or replacing the filters as required due to the deposition of volcanic ash.

B.2.6 Operating procedures should be developed and implemented to inspect and clean electrical insulators for SSC related power cables, plant power back feed cables, and switchyard connections.

B.2.7. The operating organization should ensure sufficient spare parts for vital plant equipment that may be impacted by volcanic ash deposition. Special consideration should be for sufficient quantities of ventilation filters.

B.2.8. The operating organization should consider the removal of volcanic ash from access ways to ensure the safe passage of plant operators and other plant operating personnel.

B.3. External floods including Tsunami and storm surge

B.3.1 To ensure this external hazard is completely included in the operational hazard management programme, the operating organization should consider and include the guidance given in IAEA Safety Standards Series DS498 [3].

B.3.2. Since external floods by storm surge or tsunami are somehow predictable, the operating organization should establish communication protocols and standards with national and local agencies that predict these types of phenomenon.

B.3.3. If communication protocols with national agencies is not available for tsunami warnings, the operating organization should consider the installation of a local tsunami warning system.

B.3.4. The operating organization should establish and implement procedures that describe pre-, during and post-event actions corresponding to the estimated height, arrival time, and duration of tsunami and storm surge.

B.3.5. Prior to a flooding or storm surge event, monitoring of sea water levels should be started. Status of water-tight doors, bulkhead openings and water intake structures should be checked as appropriate. Deployment of dam board and aqua dams, for example, for specific buildings should be considered. Necessary action should also be taken for any low water level conditions (e.g. stopping operation of the seawater pump). All site drainage systems and engineered water runoff systems should be checked and made functional. Additional waterproofing measures should also be considered for vulnerable and/or sensitive areas.

B.3.6 Prior to the flooding event, the plant site should be inspected for loose equipment or structures that may become structural loading and impact structures or equipment during the event. If possible, these items should be removed from the site, or secured as to minimize hazard propagation during the flood. These activities should include restraining items that may become buoyant during an extreme flooding event and block drainage outlets or access routes.

B.3.7. Prior to the flooding event, all operation and maintenance activities not related to the flooding hazard mitigation should be completed and placed into a safe condition as soon as possible.

- B.3.8. During the flooding event, operating organization should perform the following activities, with consideration of personnel safety: Inspection of water levels in vulnerable and/or sensitive areas should be monitored and results communicated with plant personnel. Also, water levels overtopping any dykes, dams, or seawalls should be identified and communicated to plant personnel.

  Use of heavy loading equipment to remove large debris from required access areas.

- Isolating damaged systems and/or plant areas to minimize flooding propagation and avoid increasing the damage caused by the flooding.

B.4. External floods (riverine flooding or floods due to extreme precipitation)

B.4.1 To ensure this external hazard is completely included in the operational hazard management programme, the operating organization should consider and include the guidance given in IAEA Safety Standards Series DS498 [3].

B.4.2. Since external floods by extreme precipitation or rivers are predictable, the operating organization should establish communication protocols and standards with national and local agencies that predict these types of phenomenon to ensure the flooding hazards are understood.

B.4.3. The operating organization should establish and implement procedures that describe pre-, during and post-event actions corresponding to the expected amount of precipitation or the expected time of maximum river flood height.

B.4.4. Prior to the flooding event, site water levels should be monitored. Status of water-tight doors, bulkhead openings and water intake structures should be checked as appropriate. Deployment of dam board and aqua dams, for example, for specific buildings should be considered. The recommendation in para B.3.5. for drain and waterproofing measures also should be considered..

B.4.5. For the case of extreme precipitation, mitigation strategies should include ensuring the site drainage systems are clear of debris and able to handle the expected water runoff. Where necessary, the operating organization should consider the use of mobile pumps to remove water from vital areas.

B.4.6. The recommendation in para B.3.7. and B.3.8. for activities of personnel should be considered for external floods.

B.4.7. Prior to the flooding event, the operating organization should ensure there are adequate supplies of mobile pumps, dam boards, and other necessary flood mitigation equipment.

B.5. Extreme winds (including Tornadoes, Tropical cyclones, Hurricanes, Typhoons)

B.5.1 To ensure this external hazard is completely included in the operational hazard management programme, the operating organization should consider and include the guidance given in IAEA Safety Standards Series DS498 [3]

B.5.2. The operating organization should establish communication protocols and standards with national and local meteorological organizations to be properly warned of these hazards, including any rare meteorological phenomenon.

B.5.3. The operating organization should regularly check the site meteorological systems to ensure consistency with national/local predictions as well as determining localized weather conditions.

B.5.4. Prior to predicted extreme wind events, the operating organization should perform walkdowns and inspections of the site to identify and remove any loose debris and unsecured items or equipment stored around the plant site, especially metallic items. These activities should include reinforcing or removing any temporary scaffolding, securing any unstable equipment, and preparatory checks of internal power systems.

B.5.5. Prior to the extreme wind events, all operation and maintenance activities not related to this external hazard mitigation should be completed and placed into a safe condition as soon as possible.

B.5.6. Depending upon the severity of the extreme wind hazards, the operating organization should consider evacuating all non-essential plant personnel. This will also reduce the number of transportation vehicles in the parking areas.

B.6. Other meteorological hazards (including lightning strikes, extreme temperatures)

B.6.1 To ensure this external hazard is completely included in the operational hazard management programme, the operating organization should consider and include the guidance given in IAEA Safety Standards Series DS498 [3].

B.6.2. The operating organization should establish communications protocols and standards with national and local meteorological agencies to be forewarned of any extreme meteorological conditions, including the possible duration. This information should be supplemented as necessary by the use of the site's meteorological systems.

B.6.3. In cases of extreme ambient air or water temperatures (both hot or cold), analyses or testing of equipment or systems such as pumps, fans, cooling circuits such as emergency cooling, HVAC cooling circuit etc., should be performed to ensure the equipment is working properly and determine if there is sufficient operating margin. Operating procedures should be developed and implemented to perform the necessary testing.

B.6.4. In cases of extreme ambient air temperatures, procedures should be developed and implemented to enhance area or equipment heating or cooling. Simple measures include opening/closing doors, dampers, adding additional heating/cooling, etc. The operating organization should ensure these measures do not invalidate the plant's safety analysis for the subject areas or equipment.

B.6.5. If there is insufficient margin in required equipment or systems, appropriate actions such as cleaning of heat exchangers or reducing pump flow should be performed. In some extreme cases margin may only be gained by reducing reactor power.

B.6.6. Snow or large amounts of hail can block inlets or outlets of protective features such as safety valves, blowout panels and HVAC intakes. These should be cleared during and after the event. Installation of electric heaters in some vital areas should be considered.

B.6.7. The operating organization should have procedures for storing and moving snow at the site, if applicable. This should include maintaining all required accesses clear, removal of snow from buildings so design loads are not exceeded, and checks for proper diesel fuel composition.

B.6.8. At sites where frazil ice can occur, temperature of the cooling water should be observed carefully before the inlet of the cooling water circuit freezes. Freezing may be prevented by circulating warm water from the outlet circuit to the inlet.

B.6.9. The operating organization should ensure the integrity of the plant's lightning protection system is maintained in an operational state.

B.6.10. When hail is predicted, the operating organization should remove or protect as necessary vital equipment that is located outdoors.

B.7. Biological phenomena

B.7.1. This hazard encompasses three types of biological hazards. The operating organization should consider these as appropriate in the operational hazard management programme. These types of hazards are:

-Marine/Waterborne

- Jellyfish
- Seaweed
- Fish

-Land

- Infestation from mice, rats, rabbits, etc.
- Biological debris such as fallen leaves

-Airborne

- Swarms of insects and birds

B.7.2. For waterborne biologics that could overburden plant intake structures, communication protocols and standards should be established with local environmental, meteorological, and waterways agencies to identify when biological hazards may be present or expected so the plant operators can take timely actions to mitigate the hazard.

B.7.3. For waterborne biological hazards, the operating organization should consider the use of chemical controls where allowed by environmental regulations.

B.7.4. For infestation of animals, operating organization should identify the evidence of ingress or equipment damage while performing plant walkdowns. Where evidence is found, the operating organization should make arrangements to deter animals from entering buildings or provide special equipment protection from animal induced damage.

B.7.5. For leaves and similar debris, the operating organization should perform routine inspections and walkdowns to ensure drainage systems or vital plant equipment remain operational.

B.7.6. For insect swarms, the hazard threat is to water intakes, to heating, ventilation, and air conditioning equipment, or to the emergency diesel generators by restricting airflow, thus limiting the operational capability of the equipment. Thus, the operating organization should perform inspections and cleaning of the affected equipment when this hazard occurs.

B.8. Collisions of floating bodies with water intakes and ultimate heat sink (UHS) components

B.8.1. The operating organization should establish and implement communication and response protocols with local or national maritime authorities, as appropriate, to be forewarned of ships adrift in heavy weather, and of the possibility of collision with ice masses or large floating debris. This should provide the operating organization time to prepare for the mitigation of the hazards.

B.8.2. Prevention of ship collisions, large debris, and large amounts of waterborne debris should be by measures implemented by navigation and coast guard authorities.

B.8.3. If applicable, operating procedures should be developed and implemented to prepare and/or actuate a diverse ultimate heat sink to accommodate the potential loss of normal cooling and ultimate heat sink systems.

B.8.4. Operating procedures should be developed and implemented for the deployment of floating booms or curtains to intercept oil spills, or surface skimmers to keep any oil from a safe distance from water intake structures. This will prevent damage to existing plant equipment and to facilitate safe hazard recovery actions.

B.8.5. Operating procedures should be developed and implemented for actions to identify potential debris accumulation at water intake structures and subsequent cleaning. This will aid in the plant's safe hazard recovery actions.

B.9. Electromagnetic interference (including Solar Storm)

B.9.1. Large solar flares have the potential to affect the electrical grid. However, they should be predicted by national agencies. Therefore, communication protocols and standards should be established with the appropriate national agencies so the operating organizations can take appropriate mitigation measures for possible grid disturbances.

B.9.2. Because solar flares may damage the electrical grid with a potential for a loss of plant internal power systems, sufficient emergency fuel oil should be obtained or maintained in preparation for loss of off-site power.

B.9.3. Additional monitoring of grid connected transformers should be considered as grid damage may adversely impact the transformers.

B.9.4. As this hazard may impact station transformers, the operating organization should perform inspections and maintenance checks for proper transformer operation.

B.9.5. The operating organization should perform routine inspections and maintenance on shielding cable for instrumentation and control systems.

B.10. External fire

B.10.1. Communication protocols and standards should be established with offsite agencies and organizations when movements or activities with explosive or flammable materials will take place. Because the potential of the hazard increases during these times, it is imperative that off-site organizations within the site characterization boundaries notify plant operators and emergency managers when offsite activities with flammable and explosive materials occur (i.e. transport or movement of these materials). This allows the plant operators to prepare for an accident that could involve highly flammable and explosive materials and impact the site's external hazard mitigation strategies.

B.10.2. Communications protocols and standards should be established with offsite agencies to notify the operating organization when environmental and/or population conditions are such that external fires could occur (i.e. extreme droughts, local festivals).

B.10.3. Communications from external organizations should include the notification of plant operators when fires external to, but in close proximity to the site boundary, are being extinguished by local fire officials.

B.10.4. If notified of offsite fire potential (e.g. during extreme droughts), the operating organization should consider notifying the on-site fire brigade and emergency response personnel of the potential hazard. This includes the early deployment of emergency on-site response and fire-fighting equipment to a standby readiness condition.

B.10.5. If there is an external fire with the potential to affect the site, the on-site fire brigade should be placed in readiness. This includes performing necessary equipment and personnel preparations.

B.10.6. Response to this hazard will typically require a response from on-site and off-site emergency personnel. As such, the operating organization should conduct regularly scheduled training and practical exercises with off-site organizations to ensure coordination and response actions are understood by all emergency personnel.

B.10.7. The operating organization should regularly inspect and maintain all installed engineered structures and barriers designed to mitigate this hazard, as appropriate. This includes the inspection and maintenance of protection walls or earth mounds (dykes) and outer walls of buildings.

B.10.8. In order to minimize the impact of external fires from affecting the plant site, the operating organization should regularly inspect and assess the build up of combustible material at or near the site boundary.

B.10.9. Due to the potential for toxic gas and hazardous fumes from this hazard, operating procedures should be established and implemented to ensure proper isolation or realignment of buildings plant area ventilation systems for personnel habitability.

B.11. External explosion including Missiles and Shockwaves

B.11.1. The recommendation in para B.10.1 for communication with offsite agencies and organizations for external fire should be considered for explosion.

B.11.2. If notified of potential offsite explosions or shockwaves, the operating organization should consider notifying the on-site fire brigade and emergency response personnel of the potential hazard. This includes the deployment of emergency on-site response and fire-fighting equipment to a standby readiness condition.

B.12. Accidental aircraft crash

B.12.1. Accidental aircraft crashes are rare. Nevertheless, operating procedures and communications with national or local air traffic control should be established and maintained functional. As appropriate, communication protocols with air traffic control should be established for immediate or redundant event notifications.

B.12.2. Since NPP sites are generally regarded as "no-fly zones," the operating organization should review and understand the requirements of the site and report any violations to national or local air traffic control agencies.

B.12.3. This hazard will most likely involve the use of off-site fire-fighting and emergency response personnel. Thus, the operating organization should establish and implement communication protocols to ensure efficient response by required off-site personnel.

B.12.4. Response to this hazard will typically require a response from on-site and off-site emergency personnel. As such, the operating organization should conduct routine training and practical exercises with off-site organizations to ensure coordination and response actions are understood by all emergency personnel.

B.12.5. The operating organization should perform regularly scheduled inspections and maintenance to preserve the integrity of all engineered structures and barriers designed to mitigate this hazard.

B.12.6. As aircraft accidents are rare, the operating organization should consider deployment of fire-fighting staff and equipment when notified of this hazard. As appropriate, this includes the prompt dispersment of equipment and personnel from any central location to prevent a large loss of emergency response capability.

B.12.7. Since an aircraft accident on site may include the generation of toxic gases and fumes, emergency response staff should consider the recommendations provided in Section B.13. This includes the use of air monitoring equipment.

B.12.8. If sufficient time is available prior to an aircraft crash, the operating organization should make preparations to shutdown the plant.

B.12.9. The operating organization should consider the evacuation of non-essential plant personnel for this hazard.

B.13. Release of hazardous substances (Asphyxiant and toxic gases, corrosive and radioactive fluids)

B.13.1. Communication protocols and standards should be established with offsite agencies and organizations when movements or activities with asphyxiants, toxic gases, corrosive and radioactive fluids will take place. Because the potential of the hazard increases during these times, it is imperative that off-site organizations within the site characterization boundaries notify plant operators and emergency managers when offsite activities with asphyxiants, toxic gases, corrosive and radioactive fluids occur (i.e. transport or movement of these materials). This allows the plant operators to prepare for an accident that could involve these substances and impact the site's external hazard mitigation strategies.

B.13.2. Operating procedures should be developed and implemented to properly isolate the affected buildings, areas, or ventilation realignments to ensure personnel habitability. This includes protecting plant operators in the main control room.

B.13.3. Operating procedures should be developed and implemented to ensure the hazard will not propagate to unaffected buildings and areas by closing openings to unaffected buildings and areas, including windows and doors.

B.13.4. There should be considerations of the need for on-site safety equipment (e.g. breathing apparatus, protection suit) to allow plant operators and emergency staff to move to places of safety.

B.13.5. The operating organization should consider sheltering or evacuating non-essential plant personnel and the potential need for the use of external emergency response organizations to organise safe evacuation from the site.

APPPENDIX C - THE OPERATIONAL HAZARD MANAGEMENT PROGRAMME FOR COMBINATION OF HAZARDS

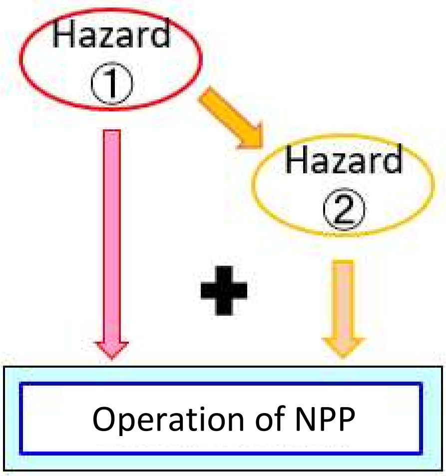
This Appendix provides recommendations for the operational management of combinations of internal and/or external hazards. It also provides a potential classification system that could be used for combinations of hazards and gives examples to illustrate how to consider these types of combinations as part of the operational hazard management programme.

C.1 The operating organization should identify and take into account combinations of hazards that could reasonably be expected to occur at the site. The goal of the operational hazard management programme is to ensure that the operation of the plant can withstand the reasonable combination of hazards and the various effects.

C.2 The operating organization should follow a systematic process to identify and categorize hazard combinations and should then screen those hazards on the basis of the significance of effects on the plant and occurrence frequency.

C.3 The following paras C.4., C.5., C.6., C.7. and C.8. below describes different types of combinations of hazards that may be applicable to the site and should be considered in the operational hazard management programme.

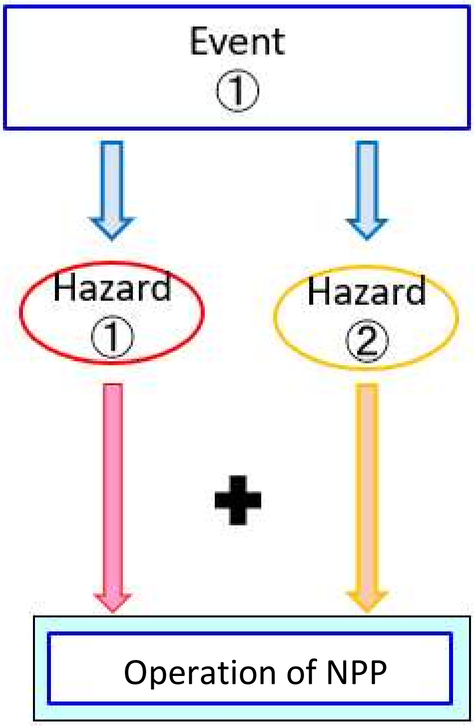
C.4 One or more hazards that affect the plant and occur as the result of a separate event that also affects the plant (causal event).



Example Combination: An earthquake that causes a tsunami.

Example Operational Aspects: In this case, if an earthquake occurs, operating organization should focus their initial response on ensuring the plant is adequately protected against the tsunami (for example, shutting flood gates if applicable). This should take precedence over assessing the earthquake damage itself, which can be done after the risk from tsunami has passed.

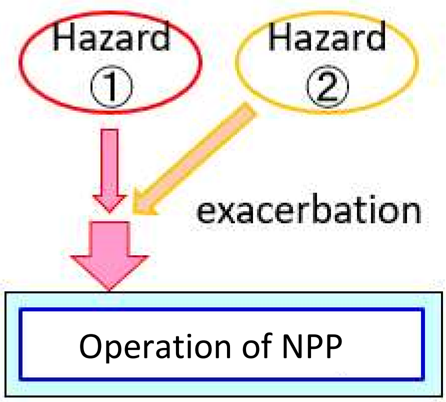
C.5. One or more hazards that affect the plant at the same time-frame due to persistence or similar causal factors (coincidental events).



Example Combination: Meteorological conditions such as storms that intrinsically involve the combination of several phenomena such as rainfall, wind, and storm surge.

Example Operational Aspects: In this case, operating organization should use their judgment to determine whether emergency response equipment such as aqua dams should be deployed – this will be based on whether the risk from storm surge outweighs the risk from extreme rainfall (an aqua dam could prevent rainwater from draining away from the site, exacerbating the effects of the hazard).

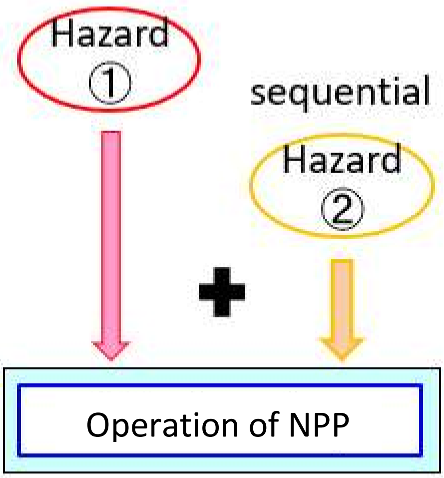
C.6. One or more hazards may exacerbate other hazards.



Example Combination: Freezing conditions or persistent rain that can affect drainage conditions during subsequent rainfall.

Example Operational Aspects: The operating organization should ensure that installed drains have been properly cleared to prevent this type of compound effect.

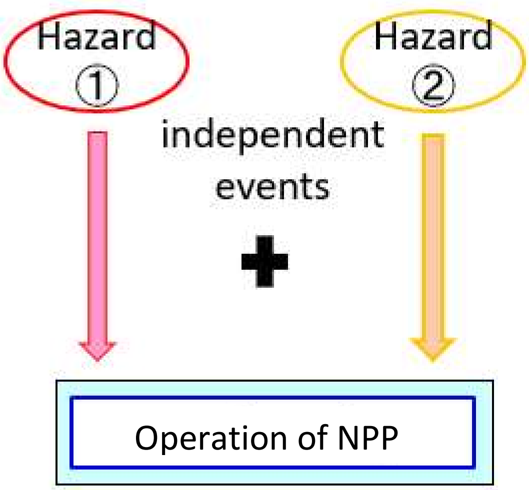
C.7. One or more sequential hazards that affect the plant.



Example Combination: Consider the case where wind hazard causes damage to the building exterior, part of whose safety function is to provide a weather envelope to keep rainwater from entering the building. Any rainfall occurring during the period before the building exterior is repaired and the safety function is restored will gain entry to the building and the potential for internal flooding is heightened.

Example Operational Aspects: The operating organization should assess the damage to the building exterior to determine whether rainfall could enter the building and affect equipment important to safety. The operating organization should consider temporary repairs to the building exterior if rainwater entry could lead to adverse effects on equipment.

C.8. Realistic combinations of randomly occurring independent events can affect the plant simultaneously.



Example Combination: Earthquake and extreme outside air temperature

Example Operational Aspects: In this example, there is no causal link between an earthquake and extreme air temperature outside. Therefore, it would be overly conservative to include extremes of these external hazards occurring together in the operational hazard management plan. However, operating organization should maintain situational awareness when responding to hazards and use their judgment based on the conditions in which they are operating at the time of response.

C.9 For all types of hazard combinations, it is the duration of the consequential effects of each hazard that should be considered, rather than the duration of the hazard itself. For example, a seismic event may last just a few tens of seconds, but the overall effect on the plant could last several days or weeks. Then, if a severe rainfall event were to occurbefore damage from the seismic event had been repaired, the consequences of the rainfall event could be more significant. This aspect of hazard combinations should be considered in the operational hazard management programme.

C.10 Combinations of hazards may be screened out if it can be justified that they do not pose a significant risk to the plant, or the consequences of the hazard combination do not exceed the consequences of one of the elements of the combination (See Appendix I in DS494 [1].

C.11 The operational hazard management programme should consider that some hazard combinations can affect the plant by undermining the diversity of systems – for example, an earthquake that causes loss of off-site power (LOOP) combined with a tsunami that causes loss of emergency power supply, as was the case for the Fukushima Dai-ichi event.

C.12 The operational hazard management programme should consider that some hazard combinations can affect a single system via the production of an additional load. An example of this would be an extreme snow load on the roof of a building that should also resist loading from an extreme wind event.

C.13 If the effect of hazard combinations has the potential to undermine the defence in depth strategy of the plant, the operating organization should take this into account when considering whether or not to screen a particular hazard combination into the operational hazard management programme. An example of this is outside freezing conditions (the hazard) may reduce fire-fighting capability (mitigation measure) of an internal fire (another hazard).

CONTRIBUTORS TO DRAFTING AND REVIEW

Altinyollar, A.	International Atomic Energy Agency
Amri, A.	International Atomic Energy Agency
Dybach, O.	International Atomic Energy Agency
Jiang, F.	International Atomic Energy Agency
Macleod T. M.	Office for Nuclear Regulation, United Kingdom
Maekelae, K.	International Atomic Energy Agency
Morgan, S.	International Atomic Energy Agency
Rantakaulio, A.	Fortum, Finland
Schwartzbeck, R.	Highland TEMS, United States of America
Shahzad, M	International Atomic Energy Agency
Stoeva, N.	International Atomic Energy Agency
Sugahara, J.	International Atomic Energy Agency
Takiguchi, T.	Tokyo Electric Power Company Holdings, Japan
Tanabe, K.	Tokyo Electric Power Company Holdings, Japan
Tarren, P.	International Atomic Energy Agency
Wendt, O.	Vattenfall, Sweden
Williams, G.	Office for Nuclear Regulation, United Kingdom
Zahradka, D.	International Atomic Energy Agency