IAEA TECDOC SERIES

IAEA-TECDOC-2043

IAEA-TECDOC-2043

Evaluation of Design Robustness of Nuclear Installations Against External Hazards

IAEA
International Atomic Energy Agency

IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available at the IAEA Internet site

www.iaea.org/resources/safety-standards

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

EVALUATION OF DESIGN ROBUSTNESS OF NUCLEAR INSTALLATIONS AGAINST EXTERNAL HAZARDS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CABO VERDE
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GAMBIA
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUINEA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT KITTS AND NEVIS
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TONGA
TRINIDAD AND TOBAGO
TUNISIA
TÜRKİYE
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.

IAEA-TECDOC-2043

EVALUATION OF DESIGN ROBUSTNESS OF NUCLEAR INSTALLATIONS AGAINST EXTERNAL HAZARDS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2024

COPYRIGHT NOTICE

For further information on this publication, please contact:

External Events Safety Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

Printed by the IAEA in Austria
February 2024

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Evaluation of design robustness of nuclear installations against external hazards / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2024. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 2043 | Includes bibliographical references.
Identifiers: IAEAL 24-01659 | ISBN 978-92-0-107124-8 (paperback : alk. paper) | ISBN 978-92-0-107224-5 (pdf)
Subjects: LCSH: Nuclear facilities — Safety measures. | Nuclear facilities — Design and construction. | Hazard mitigation.

FOREWORD

Among the lessons learned from the accident at the Fukushima Daiichi nuclear power plant were the importance of (a) nuclear installation design margins against external natural hazards exceeding those selected for the design basis, (b) the adequacy of design margins to avoid cliff edge effects and (c) independence of different levels of defence in depth. IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design, established specific safety requirements for a robust nuclear power plant design based on those lessons. The present publication provides information to support compliance with the requirements established in SSR-2/1 (Rev. 1) and IAEA Safety Standards Series Nos SSR-3, Safety of Research Reactors, and SSR-4, Safety of Nuclear Fuel Cycle Facilities.

Design robustness against external hazards can be expressed in terms of adequacy of design margins against external events exceeding the design basis. The margin assessment is performed at the nuclear installation level to determine its capability to perform the intended fundamental safety functions. As the margin assessment needs to be performed within the defence in depth framework, the margin adequacy requirement may be different at each level of defence. Failure events that involve cliff edge effects require special consideration in assessing their seismic margin.

This publication provides information on evaluating the adequacy of design safety margins against external events on the basis of the performance goals applicable to a nuclear installation. Performance goals are classified into scenario based and annual frequency based objectives. An approach is first developed for characterizing the design margin of a nuclear power plant against seismic hazard and determining the adequate margin above the design basis seismic hazard. This approach is then generalized to other external hazards. An approach is provided to identify cliff edge failure modes, which are classified into classic and non-classic cliff edge failures. The development of criteria to assess the adequacy of safety margins for seismically induced cliff edge effects is presented. This approach is generalized to other hazards. Information is provided on considerations concerning decisions on design improvements, multi-unit sites and application to nuclear installations other than plants through a graded approach.

The IAEA wishes to thank all the experts who contributed to the drafting and review of this publication, in particular M. Mahmood (Pakistan), F. Beltran (Spain) and M. Talaat (United States of America). The IAEA would like to also acknowledge the contributions of N. Orbovic (Canada). The IAEA officer responsible for this publication was O. Coman of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Guidance and recommendations provided here in relation to identified good practices represent expert opinion but are not made on the basis of a consensus of all Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

In the light of the Fukushima Daiichi Nuclear Power Plant (NPP) accident, which occurred in March 2011, the IAEA established, in the frame of the IAEA Action Plan on Nuclear Safety, revised safety requirements for nuclear installations between 2016 and 2017. IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities [1], states: "Where appropriate, the safety assessment shall demonstrate that the design is adequately conservative so that margins are available to withstand external events more severe than those selected for the design basis." (para. 4.31) and "Where practicable, the safety assessment shall confirm that there are adequate margins to avoid cliff edge effects that would have unacceptable consequences." (para. 4.48A).

Similar statements can be found in paragraphs 5.21 and 5.21A of IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [2]; in paragraphs 6.57 and 6.187 of IAEA Safety Standards Series No. SSR-3, Safety of Research Reactors [3]; and in paragraphs 6.54 and 6.67 of IAEA Safety Standards Series No. SSR-4, Safety of Nuclear Fuel Cycle Facilities [4].

Even though the intent of these revised requirements is clear, practical application stumbles on the need to define quantitatively what an 'adequate margin' is, both to withstand external events more severe than the design basis events and to avoid cliff edge effects. In current IAEA publications, very little quantitative guidance is given to assess the adequacy of these margins.

In Member States working with a risk informed regulatory framework, a rational definition might be derived from the 'performance goals'[1] established by the regulatory body. Namely, since the 'margin' eventually results in a performance of the nuclear installation against a particular hazard, the attribute of 'adequate margin' for a specific hazard would mean that it leads to meeting the applicable performance goal. This is an approach that deserves some consideration. In a more deterministic framework, where no acceptable performance goals have been defined, a quantitative definition of adequate margins may need to make extensive use of judgement.

Another challenge posed by the revised IAEA safety requirements is the identification of cliff edge effects, which is obviously needed to assess the adequacy of the margin against them. To identify when a cliff edge effect is going to happen is easy for some external hazards, such as floods, since there is a narrow band of the hazard severity parameters (e.g. water level) beyond which the condition of the nuclear installation quickly deteriorates. For other external hazards, the identification of a cliff edge effect may be not as straightforward and, thus, some practical, quantitative guidance is needed.

In practice, assessing the available margins resulting from the design is not a trivial task. The traditional design process includes a series of conservative limits and assumptions, targeted to demonstrate capacity for the design basis external events. In principle, the process is not intended to assess how much margin above the design event is achieved for each external hazard. To assess how much margin has been achieved by the design process, a safety assessment of the design will need to be conducted, considering all relevant hazards. The requirements for safety assessment of the design are established in GSR Part 4 (Rev. 1) [1].

The adequacy assessment of 'margins' against external hazards needs to be done in the framework of the defence in depth (DiD) principle: the 'adequate margins' may be different at each DiD level. For each DiD level, the challenges generated by the external hazards against the safety functions at that level need to be identified. The challenging mechanisms are specific for each external hazard.

[1] Terminology used in the present publication is defined in Section 1.5.

1.2. OBJECTIVE

In the general context described in Section 1.1, the present publication complements the existing relevant IAEA publications by developing technical bases for defining what design safety margins against external hazards are adequate. Additionally, practical guidance and information are provided to identify the external hazard severity corresponding to the onset of cliff edge effects and to assess the adequacy of the margins against them.

The final goal is to recommend procedures to assess if protection against external hazards achieved by the design responds to the new IAEA design safety requirements established after the Fukushima Daiichi NPP accident in GSR Part 4 (Rev. 1) [1], SSR-2/1 (Rev. 1) [2], SSR-3 [3], and SSR-4 [4].

1.3. SCOPE

The scope of the publication is the assessment of the adequacy of safety margins in the design against external hazards. The determination of those margins is covered by other IAEA publications (see for instance Refs [5–8]).

A number of external hazards are addressed to illustrate and to check the proposed framework. A comprehensive coverage of all potentially applicable external hazards is out of the scope of this publication.

The external hazards addressed in the present publication are those which are typically considered in the design, supplemented by some infrequent events of high consequences that can occur beyond the design basis. The scope includes the following external hazards: earthquakes, aircraft crashes, coastal and river flooding, high winds, explosions, and extreme air and water temperatures. Both deterministic and probabilistic methods are considered.

The present publication is intended mainly for nuclear power plants (NPPs). The application of this publication to nuclear installations other than NPPs can be made through a graded approach, whose main guidelines are provided in the publication.

The present publication is intended to be used by regulatory bodies, designers, operating organizations, vendors, research institutes, and technical support organizations working in the area of nuclear safety.

1.4. STRUCTURE

The publication is structured into eleven sections, one appendix and three annexes.

Section 2 provides the general framework in which this publication is developed and the overall approach it puts forward for assessing robustness. It introduces the concepts used throughout the publication. Particularly, this section introduces the idea that having appropriate design margins, as considered in the present publication, is an expression of ‘design robustness’ against external hazards.

Section 3 gathers experience data from nuclear installations that underwent severe external events. The purpose is to show how much ‘robust’ those installations were to cope with these extreme events and how robustness could have been improved.

Section 4 provides an overall perspective about the current design approaches of NPPs against external hazards. The emphasis is set on the design against earthquakes, aircraft crash and flood. An overview of current requirements for design margins is given, and common sources of conservatism are briefly discussed, as they are sources of margins. A summary of the evolution of the design approaches in the last 40 years is also given.

Section 5 is devoted to the available methods to assess design robustness of nuclear installations against seismic hazard. This section explains how to characterize installation seismic performance and reviews common measures of the seismic design margin. A proposal is made for the assessment of seismic margin adequacy. Considerations are also made regarding the DiD principle and the treatment of uncertainties.

Section 6 generalizes the ideas included in Section 5 to external hazards other than seismic. A general methodology for the assessment of design margin adequacy is proposed. Then, a review of the most common external hazards considered in the design is made, including meteorological hazards, external flooding and accidental aircraft crash.

Section 7 proposes an approach to determine margin adequacy against cliff edge effects. Discussion is separated between the one corresponding to seismic hazard and the one corresponding to other hazards.

Section 8 corresponds to the possible uses of the results of the assessment of the design robustness. Namely, it presents how the results could be used in the improvement of the physical plant design.

Section 9 gives a short consideration to the application of the concepts and methods presented in previous sections to multi-unit and multifacility sites.

Section 10 discusses the assessment of design robustness for nuclear installations other than NPPs, based on the selection of the appropriate performance objectives and the application of a graded approach.

Finally, Section 11 includes a set of concluding remarks.

Appendix A, which is closely linked to Section 3, provides an extended description of the severe external events that have been considered to draw lessons from actual events experienced by nuclear installations worldwide.

Annexes I and II expand the formulations given in Section 5. Annex I is devoted to annual frequency based seismic performance prediction based on the seismic margin of the installation. Conversely, Annex II describes the calculation of the seismic margin required to achieve a target annual performance frequency of the installation.

Complementary to Section 7, Annex III provides examples of assessment of margin against cliff edge effects, corresponding to seismic safety evaluation.

2. GENERAL FRAMEWORK

This section provides the general framework for evaluation of the adequacy of the design robustness of nuclear installations against external hazards supported by the relevant IAEA safety standards.

2.1. THE CONCEPT OF DESIGN ROBUSTNESS AND DESIGN MARGIN

The design robustness against external hazards, as considered in the present publication, is an expression of the available design margins against design basis external events. Hence, having a robust design is a result of having adequate design margins against design basis external events, with the distinction that those margins can be different for control of design basis accidents (DiD Level 3), and for mitigation of consequences of severe accidents (DiD Level 4)[2].

This concept is consistent with IAEA-TECDOC-1791, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants [9]. For a particular external hazard, design margin is the difference between the severity of the design basis external event and the severity of event that could start compromising the performance of the intended safety function, either in control of the design basis of accidents (DiD Level 3) or mitigation of consequences of severe accident (DiD Level 4). Hence, the existence of design margins against external hazards is an important attribute of the DiD principle.

The concept of 'design margin' is closely linked to the definition of 'acceptable performance' for events exceeding site specific design events. Acceptable performance can be expressed in both qualitative and quantitative terms. For scenario based hazards, where design margin metrics cannot easily be established, acceptable performance limits for given scenarios can be directly used, instead of design margins, to define the required level of design robustness.

Generally, the design robustness is to be assessed at the nuclear installation level, not at the component level, since the performance of interest is related to the overall installation capability to maintain the fundamental safety functions. However, there are cases in which the performance of the plant as a whole, for a particular external hazard, depends on the performance of a single component (e.g. the containment structure during an aircraft crash). In any case, going from the component level to the installation level normally requires the use of safety assessment techniques.

A safety assessment of the design can be conducted as design is progressing to check if the performance objectives are being met for beyond design basis external events. The results of the safety assessment can be fed back into the design process, leading to design improvements. Figure 1 illustrates the design process and the interface with the safety assessment process.

With respect to external hazards, design margins are characterized in terms of beyond design basis capability and cliff edge capability. In turn, these two capabilities have a strong connection with the redundancy and the diversity introduced by the design process.

2.2. DESIGN AND SAFETY ASSESSMENT PROCESSES

Section 2.1 above presents the concept of design robustness in connection with the presence of adequate design margins for the control of the design basis accidents (Level 3 DiD) and for the mitigation of consequences for severe accidents (Level 4 DiD) caused by external hazards.

[2] For a useful tabulation of the five levels of DiD, see Table 4 in TECDOC-1791 [9]. DiD Level 3 refers to the control of the design basis accidents. DiD Level 4 refers to the control of design extension conditions, either to prevent core melt or to mitigate the consequences of severe accidents.

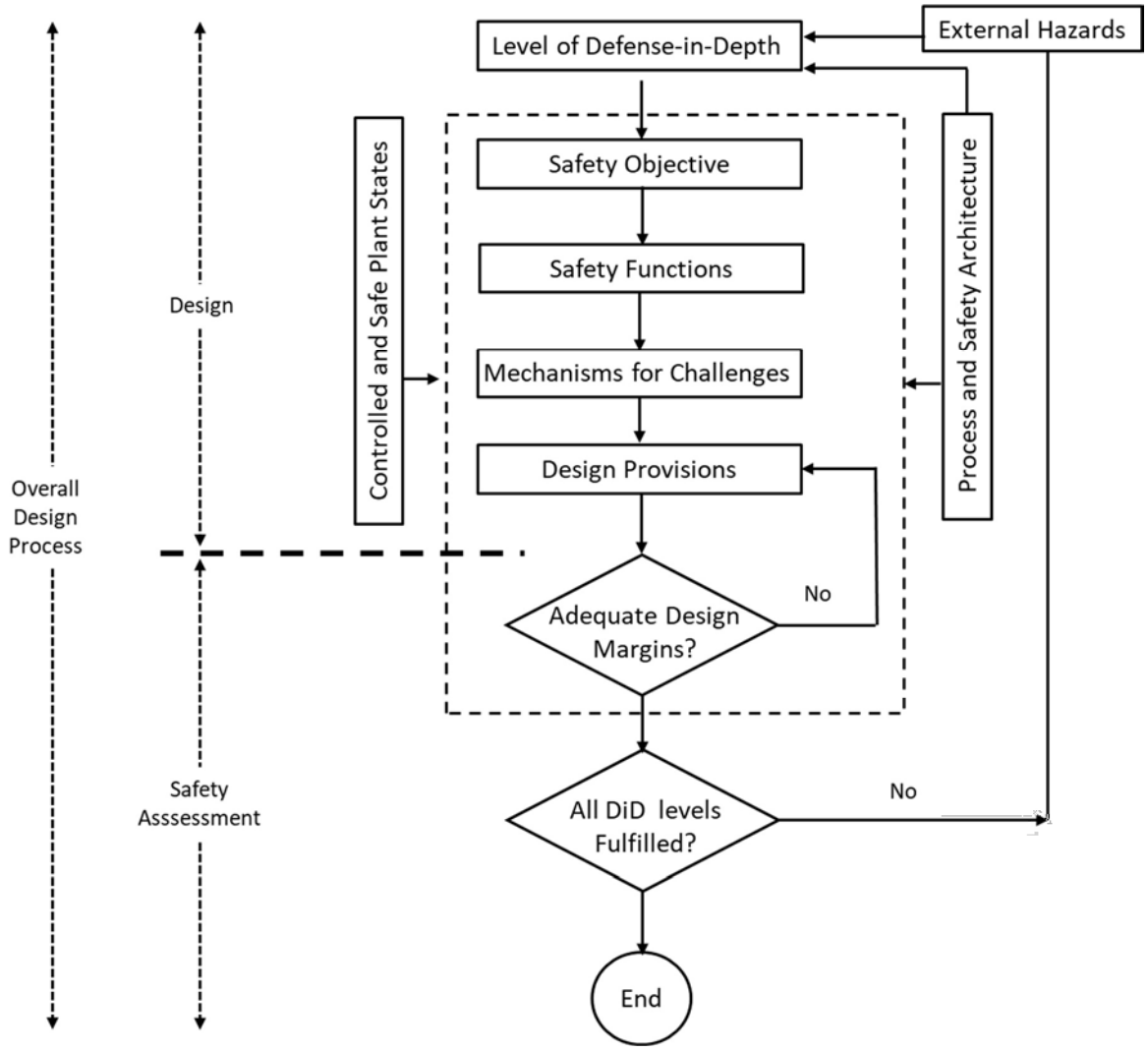

FIG. 1. Schematic of the design process and interface with the safety assessment process.

The design margins are built throughout the design process, as a consequence of the use of conservative design parameters and procedures. A certain level of conservatism is always needed due to the existence of uncertainties. The traditional design process (i.e. not including the safety assessment of the design) cannot quantify the resulting margins. As already mentioned, the resulting margins against external hazards and the adequate performance of the design are normally evaluated using safety assessment methods and provide feedback for design improvements.

An integrated process would bring together design and safety assessment of the design. The latter considers the full range of hazard severity, including beyond design basis challenges. The IAEA publications recognize both, design and safety assessment, as being part of an overall design process (Fig. 1).

In many cases, design basis events are addressed within the traditional design process, whereas beyond design basis external events are addressed by the safety assessment of the design. The exception is when the performance required for a beyond design basis external event cannot be achieved without considering this event at a very early stage within the design process. In those cases, the designer needs to consider from the very beginning the beyond design basis external event when developing the design and the separation between design and safety assessment shown in Fig. 1 could be less distinct.

2.3. OVERVIEW OF THE APPROACH FOLLOWED IN THE PRESENT PUBLICATION

As stated in Section 1, the main objective of the present publication is to provide an answer to the question about what design safety margins against external hazards are adequate for meeting the revised design safety requirements established in SSR-2/1 (Rev.1) [2]. In order to address this objective, the general workflow of the publication is shown schematically in Fig. 2.

Design safety margins are the result of nuclear design practices and general design principles. In an existing nuclear installation, the actual safety margins depend as well on construction and effectiveness of operational management which includes, in particular, maintenance procedures and equipment qualification. In this publication, as a first step, a review of beyond design basis external events that have happened in nuclear plants is made and a set of lessons learned is compiled. This is done in Section 3, where actual earthquake, flood and extreme temperature events are described and analysed. In many cases, basic nuclear safety design principles, such as redundancy and diversity, played a key role in coping with circumstances exceeding the design basis.

Following the compilation of lessons learned, the next step in this publication is to review current design practices against external events, according to the guidelines in the IAEA safety standards. Design uses codes and standards to define SSCs able to resist design basis events, with a conservative treatment of demand and capacity. Section 4 summarizes design practices against earthquake, aircraft crash, flood and general external hazards, trying to identify the main sources of conservatism. The goal is to understand how the design process introduces the margins which are found in the actual experience of facilities that have been subjected to beyond design basis external events. The current requirements for margin over the design basis events are also provided, if any.

Beyond design basis external events are introduced in safety assessments to challenge the design and to reveal a realistic capacity, for which there is high confidence that failure will have an acceptably low probability. In compliance with the current IAEA safety requirements, the consequences of external events with severity exceeding that of the design basis events need to be estimated. The available techniques are relatively well developed for the seismic hazard, where there is a general agreement within the technical community about how to perform the studies and quantify the design margins. This is presented in Section 5, where a proposal for assessing adequacy of the computed seismic margins is made, based on the performance goals applicable to the installation.

A generalization of the concepts presented in Section 5 for the seismic hazard is given in Section 6 for other hazards. To answer the question about what design safety margins against external hazards are adequate, this publication proposes an answer based on predefined performance objectives.

As a first step, external hazards are classified into groups, depending on the possibility of correlating severity levels with annual frequencies of exceedance (AFEs). When this correlation can be established, then an annual frequency based performance metric (e.g. an annual frequency of failure) can be obtained for the hazard and compared with the performance goals set by the regulatory body. Following this strategy, the design margin against a given external hazard is adequate if it leads to compliance with the performance goal established for the external hazard by the regulatory body. For instance, in an NPP, the goal set by the regulatory body for core damage frequency (CDF) can be used to determine the adequacy of design margin for SSCs contributing to DiD Level 3, and the goal for LERF can be used to assess the adequacy of design margin for SSCs ultimately necessary to prevent an early radioactive release or a large radioactive release.

For scenario based external hazards whose design and beyond design basis scenarios are established irrespective of its frequency of occurrence, an annual frequency based performance metric cannot be obtained and, consequently, adequacy of design robustness cannot be assessed based on annual frequency based performance metrics. In those cases, the robustness of the facility will be adequate if it is able to cope with the specified scenarios, complying with the conditions set by the regulatory body for these extreme events. Thus, in these cases, the ‘adequate design margin’ is implicitly defined by the

regulatory body when the beyond design basis scenario, and the performance objectives of the installation for this scenario, are specified.

Design safety margins are also needed to be adequate to avoid cliff edge effects. To check compliance with this requirement, the external hazard severity level at which a potential cliff edge failure can initiate needs to be sufficiently larger than the severity of the design basis hazard severity level, to practically avoid adversely affecting the installation safety performance. Section 7 introduces a proposed approach to assess the adequacy of safety margins for seismically induced cliff edge effects and outlines a process to generalize this approach for other hazards.

Finally, when the robustness against a particular external hazard is found to be inadequate following proposed methods will need to be decided if and how the robustness has to be improved. In the process of decision making a number of plant specific issues will need to be taken into account. Section 8 deals with this topic, both for new and existing nuclear installations. Sections 9 and 10 present additional considerations for the applicability of the present publication to multi-unit sites, nuclear installations other than NPPs, and Section 11 provides final remarks.

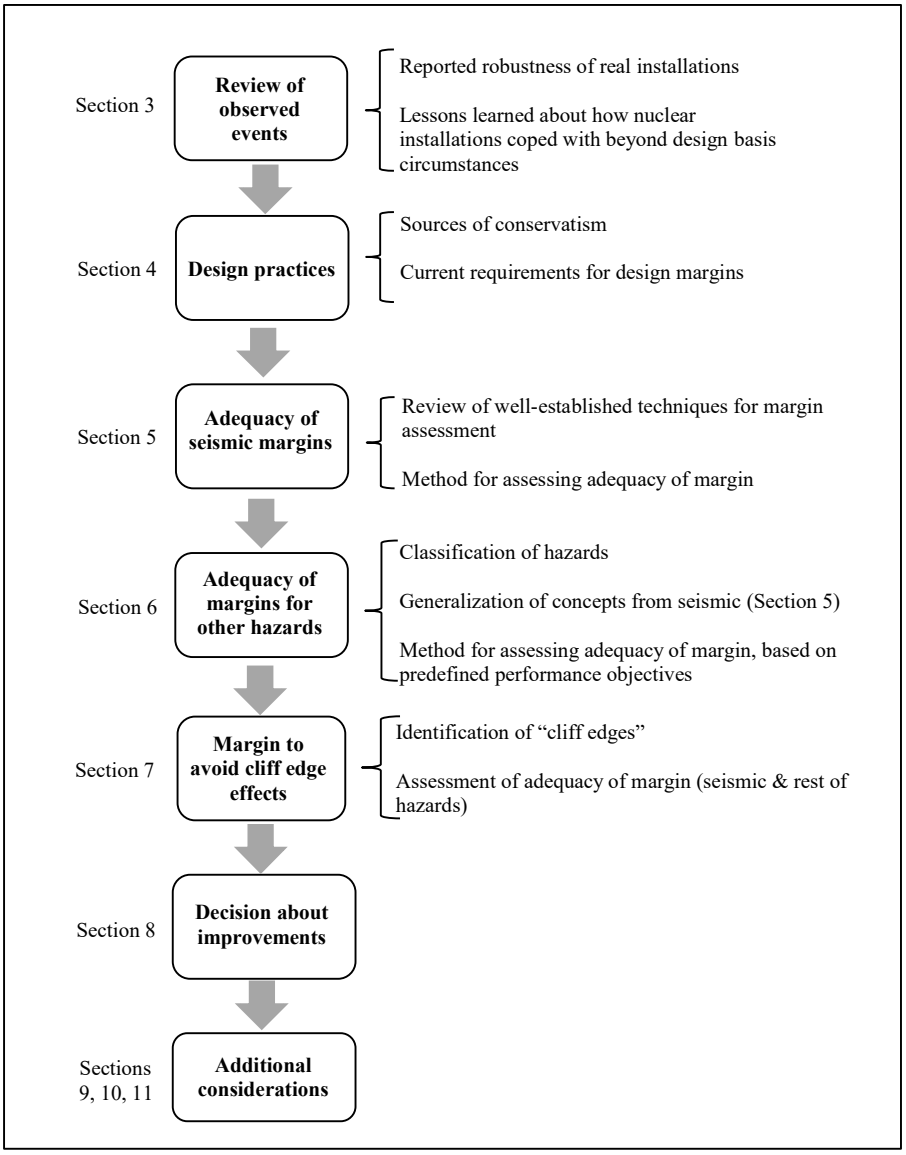

FIG. 2. Schematic view of the general workflow followed in the publication.

3. LESSONS LEARNED FROM EXISTING NUCLEAR INSTALLATIONS THAT HAVE EXPERIENCED SEVERE EXTERNAL EVENTS

3.1. EARTHQUAKE EXPERIENCE FEEDBACK

This section provides details on lessons learned from existing nuclear installations that have experienced severe earthquake in the past.

3.1.1. Significant events

Table 1 includes a summary of significant earthquake experience for nine NPPs, for which published information is available. A more detailed description of the events and of the effects at each plant is given in Appendix A.

3.1.2. Summary and lessons learned

Table 1 and Appendix A briefly describe potentially damaging earthquakes experienced by NPPs in Japan and in the United States of America.

In all reported experience for which the IAEA is aware of, the earthquakes did not produce relevant damage to structures, systems and components (SSCs), even for earthquake severities similar or larger than the severity of the design level earthquake[3]. This is indicative that seismic design practices led to a certain level of robustness for events beyond the design level events, namely, that seismic design practices provided some 'margin' above the design requirements, as required by SSR-2/1 (Rev.1) [2].

The margin cannot be quantified from the available experience, since in no case did the earthquake lead to accident conditions, that is, no fundamental safety function was lost. Methods as those defined in Section 5 are then required to assess the margin in a particular NPP.

The overall conclusion above might lead to some degree of complacency about the robustness provided by seismic design practices. However, the following aspects need to be taken into account:

- In the reviewed experience, near field earthquakes[4] with magnitudes between 5.0 and 6.5, with relatively short durations, have a large representation (Perry, Kashiwazaki-Kariwa, Hamaoka and North Anna). It is known that, for the same peak accelerations and response spectra, this kind of earthquake is less damaging than far field earthquakes [10][5].
- Experience from events in Japan has to be considered with caution. In contrast with the practice in other Member States, where only dynamic load cases are considered, Japanese design practice for nuclear safety structures considers three load cases, one static and two dynamic, and chooses the most conservative result. The static load case corresponds to the application of a static equivalent acceleration which, for the cases that have been reported here, has a value of 0.47 *g* in the horizontal direction. This is a severe load, which may be providing additional robustness with respect to other design practices [11] (see discussion in Section A.1.3). Hence, the use of static and dynamic load cases in the Japanese design introduces difficulties in the assessment of whether or not there has been exceedance of the design basis when a strong earthquake occurs.

[3] Comparison of severity has been made mainly based on peak accelerations and response spectra, which are the main indicators used in seismic design. Other damage indicating parameters could have been used, as discussed in IAEA-TECDOC-1956, Seismic Instrumentation System and Its Use in Post-earthquake Decision Making at Nuclear Power Plants [12].
[4] Epicentral distance within which 'near field' effects occur actually depends on the magnitude of the earthquake. It typically varies between 16 and 37 km. The smaller the magnitude, the smaller is the distance.
[5] This issue is discussed in Section 2.1 of IAEA-TECDOC-1655, Non-linear Response to a Type of Seismic Input Motion [10]. The point is that response spectra and peak ground accelerations are not good indicators for seismic damage [12]. Duration and number of cycles are also key factors. Near field earthquakes have durations shorter than far field earthquakes with similar response spectra.

Consequently, when assessing the seismic margins of a nuclear installation, a detailed examination of the actual design procedures needs to be performed to understand the sources of conservatism, on a case-by-case basis (see IAEA Safety Standards Series No. SSG-89, Evaluation of Seismic Safety for Nuclear Installations [13]). It would not be appropriate to automatically assume that there is a high degree of conservatism in the design process all over the nuclear installation.

TABLE 1. SUMMARY OF SIGNIFICANT EARTHQUAKES AFFECTING NINE EXISTING NPPS

Facility	Earthquake	Severity of the Event	Damage
Humboldt Bay NPP, Unit 3 (65 MWe BWR) South of Eureka, California, USA. Original plant design basis earthquake had 0.25 *g* PGA, which was upgraded in 1975 to 0.5 *g* PGA.	8 November 1980 Magnitude 7.0 Off the coast, at about 120 km from the site.	Free field peak ground acceleration at the site was between 0.20 and 0.25 *g* (horizontal).	No damage
Perry NPP (1300 MWe BWR-6) Lake Eire, NE of Cleveland, USA. Plant design basis earthquake with 0.15 *g* PGA.	31 January 1986 Magnitude 5.0 At about 17 km south off the site.	Relatively high accelerations (0.18-0.19 *g*) of short duration in the site. CAV < 0.16 *g* sec	No damage
Kashiwazaki-Kariwa NPP (5 BWR x 1100 MWe + 2 ABWR x 1356 MWe) West coast of Honshu Island, Japan. Design basis dynamic S2 earthquake with 0.45 *g* PGA at a virtual bedrock outcrop. Equivalent static acceleration value of 470 Gal specified as well for design.	16 July 2007 Magnitude 6.6 Off the coast, at about 16 km from the site.	Largest PGA at free field surface was 1.25 *g*. The static design analysis for the equivalent static acceleration value specified for the plant (470 Gal) leads to story shear forces similar to those derived from accelerations recorded at the different elevations, at least in Unit 7. The loads induced by the earthquake on SSCs may not have exceeded the equivalent static loading conditions to the same degree as the dynamic S2 design basis earthquake was exceeded.	No relevant damage to safety related SSCs in any of the seven units. Widespread damage all over the site, affecting non-safety related items. Damage included generalized soil failures, which severely affected access roads, buried piping of the fire protection system, supports of exhaust ducts, and the anchorage of some equipment items.
Hamaoka NPP (2 BWR-5 x 1100 MWe + 1 ABWR x 1380 MWe) East coast of Honshu Island, Japan. Design basis dynamic S2 earthquake with about 0.60 *g* PGA, at the basemat slabs.	11 August 2009 Japan Meteorological Agency magnitude 6.5 At about 37 km from the site	Short duration shock (3 seconds) Maximum accelerations at the reactor building basemats ranged from 0.11 *g* to 0.45 *g*. Vertical accelerations ranged from 0.03 *g* to 0.084 *g*.	No relevant damage in Units 3 and 4. Damage was found in the shaft of the main turbine of Unit 5, which experienced displacements that render the turbine inoperable.
Fukushima Daiichi NPP (1 BWR-3 x 460 MWe + 4 BWR-4 x 784 MWe + 1 x BWR-5 x 1100 MWe) East coast of Honshu Island, Japan. Design basis dynamic S2 earthquake with 0.25 to 0.50 *g* PGA, at the basemat slabs. Equivalent static acceleration value of 470 Gal specified as well for design.	11 March 2011 Magnitude 9.0 Off the coast, at a minimum distance of about 180 km off the site.	Long motion (120 seconds), which produced maximum horizontal accelerations between 281 and 550 Gal at the basemats of the reactor buildings. Vertical accelerations ranged between 200 and 302 Gal.	The earthquake damaged the on-site switchyard, leading to a loss of off-site power scenario and the startup of emergency diesel generators (EDGs) in all six units. Using emergency power, RHR systems were started and post-earthquake inspections were initiated. No signs of significant damage in safety related SSCs due to the earthquake motion were identified before arrival of the tsunami (about 45 minutes after the earthquake).

TABLE 1. SUMMARY OF SIGNIFICANT EARTHQUAKES AFFECTING NINE EXISTING NUCLEAR POWER PLANTS (cont.)

Facility	Earthquake	Severity of the Event	Damage
Fukushima Daini NPP (1 BWR-5 x 1100 MWe + 3 x ABWR-5 x 1100 MWe). East coast of Honshu Island, Japan. Design basis dynamic S2 earthquake with 0.19 *g* to 0.37 PGA, at the basemat slabs. Equivalent static acceleration value of 470 Gal specified as well for design.	11 March 2011 Magnitude 9.0 Off the coast, at a minimum distance of about 180 km off the site.	Long motion (120 seconds), which produced maximum horizontal accelerations between 210 and 277 Gal at the basemats of the reactor buildings. Vertical accelerations ranged between 208 and 305 Gal.	No damage to safety related SSCs due to the seismic motion was reported.
Onagawa NPP (1 BWR-4 x 524 MWe + 2 BWR-5 x 825 MWe) East coast of Honshu Island, Japan. Design basis dynamic S2 earthquake with 278 to 375 Gal PGA, at the basemat slabs. Equivalent static acceleration value of 470 Gal specified as well for design.	11 March 2011 Magnitude 9.0 Off the coast, at a minimum distance of about 125 km off the site.	Very long motion (160 seconds), which produced maximum horizontal accelerations between 458 and 607 Gal at the basemats of the reactor buildings. Vertical accelerations ranged between 321 and 399 Gal. (This plant experienced the strongest shaking that any NPP has ever experienced from an earthquake.)	No relevant damage to safety related SSCs was found during the inspections due to the earthquake motion. The three units achieved cold shutdown conditions, with all systems working as designed. Minor cracking of concrete structures was identified during inspection walkdowns. Small displacements were detected in the main steam turbine rotor at Units 2 and 3, which caused damage to the blades. In the turbine building of Unit 1, insulators in a medium voltage switchgear cabinet fractured and allowed contact of the bus bar with the cabinet enclosure. This led to a small fire in the cabinet.
Tokai Daini NPP (BWR-5 1100 MWe) East coast of Honshu Island, Japan. Design basis dynamic S2 earthquake with 520 Gal PGA, at the basemat slab. Equivalent static acceleration value of 470 Gal specified as well for design.	11 March 2011 Magnitude 9.0 Off the coast, at a minimum distance of about 250 km off the site.	Maximum recorded horizontal acceleration was 225 Gal at the basemat of the reactor building. Maximum vertical acceleration recorded at the basemat was 189 Gal.	No relevant damage reported for safety related SSCs. All three off-site power sources were lost and all three EDGs started automatically, providing power to the safety buses.
North Anna NPP (2 PWR x 1000 MWe) Northwest of Richmond, Virginia, USA. Plant design basis earthquake with 0.15 *g* PGA.	23 August 2011 Magnitude 5.8, at about 18 km WSW off the site.	Very short shock (2 seconds), with strong NS directionality. PGA was 0.23 *g*. CAV = 0.172 *g* sec	No relevant damage reported for safety related SSCs.

3.2. EXPERIENCE FEEDBACK FROM FLOOD EVENTS

This section provides details on lessons learned from existing nuclear installations that have experienced flooding events in the past.

3.2.1. Significant events

Table 2 includes a summary of significant flood experiences for seven NPPs. A more detailed description of the flood events and their effects is given in Appendix A.

3.2.2. Summary and lessons learned

From the analysis of the flood events reported in Table 2 and Appendix A, a first observation is that flood hazard has an inherent 'cliff edge' effect which is not present in other hazards. Underestimation of potential flood levels may have catastrophic consequences. Even a small underestimation (e.g. 30 cm) may lead to serious safety consequences. Therefore, a reliable flood hazard assessment is key to achieve robustness. The assessment needs to include all credible combinations of events which could lead to flooding of the site. In addition, aspects such as the construction of new water retaining structures and climate changes need to be taken into consideration.

An immediate consequence is that periodic safety reviews of the flood hazard assessment are essential and a timely introduction of the improvements, if necessary, is crucial. For instance, timely protection of seawater pumps at the Tokai Daini NPP as a result of the revised tsunami hazard assessment, probably prevented a major accident from occurring.

A second observation is that, in coping with the flood events, redundancy, diversity and segregation of safety systems played an important role. These three essential design principles may not be as easily defeated by flood hazard as by other hazards (e.g. earthquake). When flooding does not massively affect the plant, as happened at the Fukushima Daiichi NPP, damage caused by the flood can be very different from one safety train to the other or from one safety system to the other. Damage depends on factors such as elevation, integrity of doors and penetration seals, and drainage capacities, which may vary across the plant. Diversity (e.g. having air cooled systems) has also demonstrated its importance.

In line with having diversity, the flood events reported in Table 2 and Appendix A show that, even though a site is kept 'dry', the main ultimate heat sink (UHS) may be lost due to clogging at the intake structures. Having an alternate UHS, even based on non-safety related systems, adds robustness to the plant.

Thus, from an overall perspective, robustness of design originates basically from two sources:

- A quality flood hazard assessment and the 'freeboard' introduced in the design over the maximum flood coming from the hazard assessment;
- Redundancy, diversity and segregation of systems for residual heat removal (RHR). Particularly, having a secondary UHS at higher elevations (e.g. air cooled), independent from primary UHS located at lower elevations (i.e. closer to the level of the sea or the river origin of the flood).

For an existing nuclear installation, robustness can be assessed by checking a series of barriers:

A. Height with respect to the flood source is the first barrier;
B. Water tightness of safety related buildings is the second barrier, especially for access doors and seals of penetrations;
C. Flood barriers within the safety building are the third barrier. Bypass of flood barriers needs to be carefully avoided.

The assessment of the first barrier depends on having a reliable flood hazard analysis. The systematic identification and assessment of the items corresponding to the subsequent two barriers have to be carried out using specialized techniques.

TABLE 2. SUMMARY OF SIGNIFICANT FLOODS AFFECTING SEVEN EXISTING NPPS

Facility	Flood	Severity of the Event	Damage
Le Blayais NPP (4 PWR x 950 MWe) On the banks of the Gironde estuary, Northwest of Bordeaux, France. Plant grade level is at 4.5 m above the French national datum (NGF). The site is surrounded by a dike. The height of the dike was 5.2 m NGF. The design river flood level for the protection of the site was 5.02 m NGF.	During the night of 27–28 December 1999, high waves, caused by a combination of tides and exceptionally high winds, moved up the Gironde estuary.	Plant platform was flooded. During the flooding event, the waves moved the rock blocks protecting the earth structure of the dike and part of it was washed away down the river. The water reached a depth of around 30 cm in the Northwest corner of the site. Investigations carried out on the site after the flood showed that the water had overtopped obstacles from 5.0 to 5.3 m NGF in height.	The water went into the underground gallery of the site mainly through the maintenance openings at the plant grade level. Water flows developed from this gallery into the buildings due to hydrostatic pressure on the penetrations. Units 1 and 2 were affected by the incoming water. In Unit 1, the essential service water (ESW) pumps of train A were lost as a result of the immersion of their motors. Train B remained operable. Redundancy of the ESW system allowed to cope with the emergency situation.
Madras NPP (2 PHWR x 235 MWe) Located at Kalpakkam, on the SE coast of India. The plant grade is about 4.5 m above mean sea level, but the pump house operating floor is located only about 2.5 m above mean sea level.	Tsunami generated by the 26 December 2004, magnitude 9.1, earthquake that occurred off the western coast of Sumatra, Indonesia.	The maximum runup of the tsunami at the site was 4.5 m above mean sea level, flooding the pump house.	Unit 1 was in extended outage. The vital areas of the plant such as the reactor building, turbine building, service building, switchyard and ancillary systems were unaffected by the tsunami. Off-site power remained available. The flooding of the pump house during the tsunami rendered all the seawater pumps located in this area inoperable except for one process seawater pump. The reactor of Unit 2 tripped automatically after the loss of the circulating water pumps. The only pump available was then used to cool the plant heat loads in the initial period following reactor shutdown. Later, this pump also became unserviceable due to clogging of the travelling water screen. After this point, cooling was achieved using the firewater system.
Fukushima Daiichi NPP (1 BWR-3 x 460 MWe + 4 BWR-4 x 784 MWe + 1 x BWR-5 x 1100 MWe) East coast of Honshu Island, Japan. In Units 1–4, plant grade level was set at elev. OP+10.0 m. In Units 5–6, plant grade was set at OP+13 m. The design tsunami height was specified as OP+3.12 m. OP+4.00 m level for the safety related SSCs at the	Tsunami generated by the 11 March 2011, magnitude 9.0, earthquake that occurred off the east coast of Honshu Island, Japan.	The tsunami wave reaching the site about 50 minutes after the earthquake had a runup height of 14–15 m. It overtopped the seawalls and inundated the site.	The tsunami flooded the seawater pumps and motors of all six units at the intake locations on the shoreline, resulting in a loss of UHS event for all units. Water flooded the main buildings, including all the reactor and turbine buildings, the common spent fuel storage building and diesel generator buildings. This resulted in the loss of emergency AC power in all units, except for Unit 6: a station blackout scenario in Units 1 through 5. DC power sources in Units 1, 2 and 4, were flooded. DC power was gradually lost. Operators were no longer able to monitor essential plant

TABLE 2. SUMMARY OF SIGNIFICANT FLOODS AFFECTING SEVEN EXISTING NUCLEAR POWER PLANTS WORLDWIDE (cont.)

Facility	Flood	Severity of the Event	Damage
water intake area (sea-water cooling pumps). The top of seawalls protecting the intakes was set at OP+5.5 m.			parameters. The damage led to core damage in several of the units, and serious difficulties to cool some of the spent fuel pools.
Fukushima Daini NPP (1 BWR-5 x 1100 MWe + 3 x ABWR-5 x 1100 MWe). East coast of Honshu Island, Japan. Plant grade level is at elevation OP+12 m. Original design maximum tsunami height was OP+3.7 m and OP+4.3 m was selected as the level for locating the safety related SSCs at the water intake area, which are housed by the heat exchanger buildings. The design maximum tsunami height was reassessed to OP+5.2. As a result, heat exchanger buildings were made watertight.	Tsunami generated by the 11 March 2011, magnitude 9.0, earthquake that occurred off the east coast of Honshu Island, Japan.	Tsunami waves inundated the platform of the heat exchanger buildings. The maximum tsunami height was OP+9.1 m, but maximum runup heights reaching about OP+14.5 m were observed. Inundation surrounding the main buildings (reactor building and turbine building) was caused only by the runup waves and was therefore not significantly deep.	The tsunami damaged the equipment hatch doors of seven of the eight heat exchanger buildings. Entry of water into these buildings, caused the loss of normal core cooling and pressure suppression functions in Units 1, 2 and 4. Plant operators were able to continue to provide water to the reactor cores in Units 1, 2 and 4 with the reactor core isolation cooling (RCIC) system and the make-up water condensate (MUWC) system. Mobile power trucks were brought, and more than 9 km of power cables were laid in 16 hours. Power in the damaged heat exchanger buildings was restored and replacement motors were procured for some of the flooded pumps. This allowed the normal RHR systems to be returned to service, and Units 1, 2 and 4 were brought to cold shutdown shortly after.
Tokai Daini NPP (BWR-5 1100 MWe) East coast of Honshu Island, Japan. For the original design, a maximum tsunami height of HP+2.35 m was assessed. The plant grade level was set at HP+8.9 m. Platform for accessing emergency seawater pumps motors was set at about HP+3.0 m. This platform was protected by concrete side walls, with their top at HP+5.80 m. Tsunami hazard was reassessed to a maximum height of HP+6.61 m.	Tsunami generated by the 11 March 2011, magnitude 9.0, earthquake that occurred off the east coast of Honshu Island, Japan.	Tsunami waves flooded the lower level of the site. Maximum tsunami height at the site was HP+5.50 m, with maximum runups up to HP+6.20 m.	The tsunami inundated the seawater pump bay which had some pending sealing work and, therefore, was not watertight. This caused the loss of one of the EDGs and its associated electrical loads. The other seawater pump bay had been upgraded to be watertight and was not flooded by the tsunami. As a result, only one emergency diesel generator and one source of core cooling were lost, but the other sources remained operable, which eventually allowed to reach cold shutdown of the reactor.

TABLE 2. SUMMARY OF SIGNIFICANT FLOODS AFFECTING SEVEN EXISTING NPPS WORLDWIDE (cont.)

Facility	Flood	Severity of the Event	Damage
The height of the walls protecting the seawater pumps was moved up to HP+7.0 m. On 11 March 2011, this retrofit was completed, except for the sealing at one of the two bays housing the pumps.			
Onagawa NPP (1 BWR-4 x 524 MWe + 2 BWR-5 x 825 MWe) East coast of Honshu Island, Japan. Plant grade level was set at OP+14.8 m for all units. Bottom of the pits for emergency seawater pumps was set at OP+3.0 m. However, the pits are surrounded at all sides by the plant platform at OP+14.8 m.	Tsunami generated by the 11 March 2011, magnitude 9.0, earthquake that occurred off the east coast of Honshu Island, Japan.	After the earthquake, the elevation OP+14.8 m of plant grade was reduced to about OP+13.8 m, due to crustal subsidence caused by the earthquake in the area. Maximum observed tsunami height was about OP+13 m.	Hydrostatic pressure differences between the seawater pump pit (OP+3.0 m) and the tsunami wave (OP+13 m) caused seawater to flow through penetrations in the seawater pump pit floor. Once in the pit, the water flowed through a trench into the lower level of the reactor auxiliary building of Unit 2, and flooded train B of some cooling systems. The flood caused the shutdown of train B of the EDGs and train B high pressure core spray diesel generator. Trains A of these safety systems were not affected by the flooding.
Fort Calhoun NPP (PWR 512 MWe) Missouri River, N of Omaha, Nebraska, USA. Plant grade was set at 306 m mean sea level (MSL). Design flood elevation was 306.6 m MSL. Safety related components in the plant were protected by hardened features up to a flood height of 307 m MSL. The intake structure was located at an elevation of 307.1 m MSL.	June 2011 Extraordinary flood of the Missouri river, which developed along several weeks	The river reached its peak stage at the nearby hydrologic station at Blair (about 4 km upstream of the plant) on 29 June 2011. The recorded peak stage at this station was 308.1 m MSL. Maximum river stage at the site was in the order of 307 m MSL.	The plant was in a refuelling outage since April. The reactor was shut down when the river reached a warning level stage (6 June 2011). Floodgates and sandbags considered in the flood safety assessments were deployed. Seeped-in water was pumped out. Floodwaters surrounded the main electrical transformers and operators transferred power from off-site sources to the EDGs as a precautionary measure. Fundamental safety functions were kept throughout the flood event, even though access to the plant was severely impaired during weeks.

3.3. EXPERIENCE FEEDBACK FROM SIGNIFICANT WEATHER EVENTS

This section provides details on lessons learned from existing nuclear installations that have experienced significant weather events in the past.

3.3.1. Significant events

Table 3 includes a summary of significant weather experiences for four NPPs. A more detailed description of the events and of the effects at each plant is given in Appendix A.

3.3.2. Summary and lessons learned

In the events summarized in Table 3 and Appendix A, diversity and redundancy again played a key role in keeping the overall safety of the installations. These two aspects were important contributors to robustness, especially in the cases where the main UHS was lost. In addition, use of meteorological alerts issued by national meteorological office are an important data that may make it possible to anticipate actions to limit anticipated consequence.

In the reported scenarios, it can be seen that, even with external events within the design bases, damage to non-safety related SSCs (e.g. communication systems, access routes) can challenge the plant's response to the event.

TABLE 3. SUMMARY OF SIGNIFICANT WEATHER EVENTS AFFECTING FOUR EXISTING NUCLEAR POWER PLANTS WORLDWIDE

Facility	Extreme Weather	Severity of the Event	Damage
Saint-Laurent NPP (2 PWR x 915 MWe) Loire river, upstream of Blois and downstream of Orleans, France.	12 January 1987 Exceptionally low temperatures all over Northwest of France.	Ice blocks in the Loire river clogged the cooling water intake for Unit A1.	Loss of the UHS for Unit A1. The loss caused the automatic shutdown of the reactor and the unavailability of all the auxiliary turbo blowers used for RHR. Off-site power was used to power the blowers and start RHR. The availability of all four turbo blowers was restored just before the collapse of the electrical power grid in West France, which was also traced back to the cold weather conditions. Fundamental safety functions were kept all over the event.
Davis-Besse NPP (PWR 925 MWe) Lake Eire, close to the city of Toledo, Ohio, USA.	24 June 1998 Plant site was directly hit by a tornado classified as F-2 in the Fujita scale.	Maximum wind speeds in the site were in the range from 195 to 270 km/h. These speeds are within the wind design basis of the plant for safety related SSCs.	Plant's switchyard was damaged and the reactor automatically shut down due to loss of off-site power. EDGs were started, which provided power to plant's safety systems. Fundamental safety functions in the plant were kept all over the event. The three lines connecting the plant to the grid were cut-off. The emergency response communication system was highly challenged by the damage of two of the three available telephone systems. Plant computer system failed because of loss of power.
Turkey Point NPP (2 PWR x 830 MWe) Biscayne Bay, about 40 km south of Miami, Florida, USA.	24 August 1992 Plant site was hit by Hurricane Andrew	Maximum wind speeds of 233 km/h and gusts at 282 km/h were recorded. These speeds are within the wind design basis of the plant for safety related SSCs.	Operators received early warnings and took precautionary measures. Reactors started shutdown about 10 hours before expected hurricane impact. Emergency core cooling systems performed well throughout the event. A total loss of off-site power was experienced for five days, but emergency diesel provided the required power to the plant during this period. Off-site communications were lost, and access roads blocked for some time.

TABLE 3. SUMMARY OF SIGNIFICANT EXTREME WEATHER EVENTS AFFECTING FOUR EXISTING NUCLEAR POWER PLANTS WORLDWIDE (cont.)

Facility	Extreme Weather	Severity of the Event	Damage
Maanshan NPP (2 PWR x 950 MWe) Coast at south end of the Island of Taiwan.	18 March 2001 Seasonal sea smog, rich in salt content, affected Southern Taiwan	Salt crystals transported by heavy sea winds built-up on the insulators of power lines.	Total loss of off-site power, which led to a station blackout scenario due to failure to start in emergency diesels. Power to essential buses was restored using a swing emergency diesel generator shared by both units. When the incident started, both reactors were in a hot shutdown condition. During the event, the turbine driven auxiliary feedwater pump functioned normally and the core temperature and pressure continued to reduce throughout the event.

3.4. EXPERIENCE FEEDBACK FROM OTHER SIGNIFICANT EVENTS

This section provides details on experience feedback of other significant events from existing nuclear installations.

3.4.1. Significant events

Table 4 includes a summary of other significant events at a nuclear installation. A more detailed description of the event and of the effect at the plant is given in Appendix A.

3.4.2. Summary and lessons learned

Design robustness against external fire hazard is provided by a suitable design of the ventilation systems (against ash and smoke) and against burning particles transported to the site by wind.

In addition, wide enough boundary areas free of bushes or of any other combustible vegetation contribute to the robustness of the installation against this external hazard.

During forest fires, it is common that airborne vehicles such as airplanes and helicopters are used to fight the fire. Pilots of these aircraft operate under stress and in a difficult environment (e.g. smoke, flames, rough terrain). If the fire comes close to the nuclear facility, there is a risk that one of these aircraft may crash within the perimeter of the facility. Administrative measures could be used to prevent the use of these airborne vehicles too close to the facility.

TABLE 4. SUMMARY OF SIGNIFICANT OTHER EXTREME EVENTS AFFECTING A NUCLEAR INSTALLATION

Facility	Extreme Event	Severity of the Event	Damage
Cadarache laboratories Research facility near Aix-en-Provence, France.	1 August 1989 A forest fire broke out in the woods around the site, at only 3 km distance from the outer fence.	The fire moved very quickly towards the site due to the strong wind and reached the site limits in less than one hour. Up to 130 firefighters came to help the on-site fire brigade. Air support was provided by Canadair waterbombers based in Marseille. The planes flew continuously over the site, often in dangerous routes, as close as possible to the main fire sources.	Despite the efforts, the fire penetrated into the site and affected 5 ha inside its boundary. During the event, all the nuclear facilities remained protected, and no relevant incidents were reported. Access to the site was difficult, which sometimes delayed the arrival of specialized personnel and support firefighters.

4. DESIGN OF NUCLEAR POWER PLANTS AGAINST EXTERNAL HAZARDS

4.1. GENERAL PRINCIPLES

Guidance for the design of NPPs against external hazards is provided in IAEA Safety Standards Series No. SSG-67, Seismic Design for Nuclear Installations [14], for the seismic hazard, and in IAEA Safety Standards Series No. SSG-68, Design of Nuclear Installations against External Events Excluding Earthquakes [15], for other external hazards.

The general design workflow follows a similar pattern for all hazards, namely:

(1) Define the hazard severity levels to be used for the design.

(2) Define the external hazard category of the SSCs within the nuclear installation, consistent with their safety classification. Requirements, or objectives to be reached through the design process, are different for the different categories.

(3) Select the applicable standards and guidelines, consistent with the design requirements, providing the acceptable limits and conditions of the SSCs behaviour to ensure that the intended safety functions during and after an earthquake, are performed as required.

(4) Evaluate the demand on the SSCs due to the design basis hazard level(s), according to relevant national or international codes, standards and proven engineering practices and as recommended or accepted by the national regulatory body.

(5) Verify that the total demand on each SSC, including concomitant actions, does not exceed the capacity and limits established by applicable national or international codes, standards and proven engineering practices recommended or accepted by the national regulatory body.

(6) Assess that the process above results in a design with adequate margin to cope with events that exceed the design basis levels and that no cliff edge effects may be produced. This safety assessment is performed using procedures which are different from the ones used for design purposes, as utilized in the previous steps, in that they emphasize the use of realistic and best estimate assessments.

Within this general workflow, design against each particular hazard has its own specificities, methods, and sources of conservatism. In addition, the adequacy assessment of the design margins or the definition of appropriate beyond design basis external events, may be done differently.

In the following Sections 4.2 to 4.4, design against selected external hazards and current practices to define the margin to be achieved by the design are reviewed. Particularly, separate sections are dedicated to earthquake, aircraft crash and flood. The intent is to provide the context for the following chapters, in which a framework to assess adequacy of design margins is presented.

4.2. SEISMIC DESIGN

This section provides an overall perspective about current design approach of NPPs against the seismic hazard. It describes first the general workflow and then identifies sources of conservatism embedded in the approach. Finally, some considerations are made about the margin to be achieved by the design and how it is usually checked in Member States.

4.2.1. General workflow

From a general perspective, the seismic design process of a nuclear installation consists of the following steps [14]:

(1) Define the earthquake levels to be used for the design, noted as design basis earthquake (DBE) levels.

(2) Define the seismic category of the SSCs within the nuclear installation, consistent with their safety classification.

(3) Select the applicable standards and guidelines, providing the acceptable limits and conditions of the SSCs behaviour in case of an earthquake event to ensure that the intended safety functions during and after an earthquake, are performed as required.

(4) Evaluate the seismic demand on the SSCs due to the DBE level(s), according to relevant national or international codes, standards and proven engineering practices, and as recommended or accepted by the national regulatory body.

(5) Verify that the total demand on each SSC does not exceed the capacity and limits established by applicable national or international codes, standards, and proven engineering practices recommended or accepted by the national regulatory body.

(6) Assess that the process above results in a design with adequate seismic margin to cope with earthquake events that exceed the design basis levels and that no cliff edge effects may be produced.

The last step, Step 6, even though it takes place within the integrated design process (Fig. 1), has not been part of the 'design', as this concept was traditionally understood in the past. The traditional idea about 'design' is that it uses applicable loads to size the SSCs in order to meet the limits given in the design code, that is, the design is aimed at meeting the limits given by the codes for the design level earthquake in every SSC. In this way, safety for the design level earthquake is demonstrated. The 'margin' over the design level earthquake achieved by this process is a by-product since the traditional process was not targeted at obtaining a particular 'margin' but at meeting the limits in the design codes. Step 6 is considered a necessary part of the integrated design process for any contemporary design. Results from Step 6 may iteratively feed back into the traditional design of sizing SSCs based on the design codes and the design basis demand. Alternatively, the objective of Step 6 may be achievable by explicitly considering in the previous steps a higher seismic input level than the DBE, as is the practice in some Member States, either based on deterministic or probabilistic considerations.

In Step 6 above, a seismic safety evaluation is performed on the design resulting from the previous steps. The aim of the safety evaluation is to establish the capacity of the SSCs in the 'as-designed' condition and use it in the evaluation of the seismic capacity of the installation as a whole to keep the fundamental safety functions. In doing this, experience from exposure to past seismic events, testing and analytical estimates of capacity are utilized, and expert judgement plays a significant role. Methods are, therefore, different from those used in the previous ('design') steps 1 through 5 [13].

The main result of the seismic safety assessment in Step 6 is the margin over the DBE, that is, the largest earthquake for which there is high confidence that the installation will maintain its fundamental safety functions. In addition, the results normally identify 'weak links' in the design which, if addressed, may lead to an overall improvement of the seismic safety (robustness) of the nuclear installation.

4.2.2. Sources of conservatism and consideration of uncertainties

Seismic experience of industrial facilities that have been subject to strong earthquakes, including NPPs (see Section 3.1), demonstrates that there often exists an inherent capability to resist earthquakes larger than the earthquake considered in the design of the facility. This is especially the case for adequately designed and built civil structures and for most mechanical equipment classes, or whenever an equipment item has a robust enough anchorage system.

This overall good seismic record is not only due to the conservatism of the seismic design process, since the seismic experience mentioned above sometimes correspond to facilities for which no seismic provisions were made in the design.

For NPPs, two main reasons are identified in SSG-89 [13] and Safety Reports Series No. 103, Methodologies for Seismic Safety Evaluation of Existing Nuclear Installations [6], to explain the

inherent seismic capability or seismic robustness, which is usually described in terms of 'seismic design margin':

(1) The conservatism in the seismic design and qualification procedures used according to previous or current practices in earthquake engineering;

(2) The fact that in the design of nuclear plants the seismic loads may not be the governing loads for some SSCs.

Conservatisms in regular seismic nuclear design procedures include, for instance, conservative design parameters used in the evaluation of structural response, enveloping the results of multiple soil–structure interaction analyses, the broadening of peaks at computed floor response spectra, the no consideration of inelastic energy absorption, or the enveloping of required response spectra by the actual test response spectra. In addition, seismic demand is often considered as a force, for application of stress based acceptance criteria. This practice facilitates combination with other types of loads, but it may lead to large margins, given the dynamic and imposed-displacement nature of the seismic demand.

On the other hand, nuclear installations are designed for a wide range of internal and external extreme loads, for example, pressure and other environmental loads due to accident conditions, aircraft crash, tornado or pipe break, and seismic loads may not be the governing loads for some SSCs.

Generally, final design of an SSC does not just barely satisfy acceptance criteria given in the design code. Additionally, in an existing, well-maintained[6], installation, the 'as-is' condition may be more robust than the 'as-designed' condition, for a number of reasons, for instance:

- In concrete structures, compression strength of the concrete may be larger than the 28-day strength considered in the design, due to long term hardening phenomena.
- Same equipment items are installed at different floors but qualified for the enveloping floor response spectra.
- The procurement process selected seismically overqualified equipment or components, due to supply chain considerations.
- In distribution systems (e.g. piping, cable trays), some construction details with some supporting capacity during a large earthquake are not considered to be supports in the design.

The assumption that a nuclear installation would fail in the performance of its fundamental safety functions for an earthquake that slightly exceeds its DBE is an old, very conservative concept that was abandoned several decades ago [16].

Modern nuclear seismic structural design standards, such as Refs [17] and [18], are targeted to have a small probability of unacceptable performance in case the design earthquake does occur (e.g. <1% probability) and only a slightly larger probability of unacceptable performance for earthquakes significantly larger than the design earthquake (e.g. 10% probability for an earthquake 150% larger) [17]. A common definition of 'unacceptable performance' in a structural or mechanical component is brittle failure or 'the onset of significant inelastic deformation'. Unacceptable performance of electrical and instrumentation and control (I&C) equipment can be much more subtle, like relay chatter.

These probability targets of the design standards are of a great importance in a risk informed framework since, given a probabilistic definition of the seismic hazard, these targets give a measure of the uncertainties and allow computation of approximate risk metrics and, consequently, they open the possibility of specifying a performance based design aimed at meeting risk targets accepted by the regulator body [17].

[6] The 'as-is' condition SSCs may experience a wide variety of ageing phenomena and operational degradation (e.g. cracking, corrosion, fatigue) that may reduce their 'as-designed' conservatism and hence their safety margin.

However, most design codes (structural, mechanical, electrical, etc.) do not define their design targets in probabilistic terms. Therefore, for a given set of design actions, the probabilities of unacceptable behaviour achieved through the application of the codes are not explicitly declared. They vary from code to code and even between sections of the same code.

As a result, in general, the designer does not know what level of (conditional) probability of unacceptable performance of the SSCs is being achieved by the design, in case that the design earthquake takes place. The designer just follows the rules in the design standards. However, as a matter of fact, there is a probability of unacceptable performance which is, consciously or unconsciously, embedded in the design standards.

Finding the probability of unacceptable performance of the SSCs for a given seismic motion and for different confidence levels currently requires the use of special techniques (e.g. fragility computations, see Section 5).

4.2.3. Margin to be achieved by the design

Seismic margin to be achieved by the design is usually defined by a beyond design basis earthquake (BDBE)[7], for which the seismic safety of the installation as a whole against loss of the fundamental safety functions needs to be assessed[8]. For NPPs, a common practice in Member States is that the BDBE is defined by a factor times the response spectrum corresponding to the DBE. This factor typically varies between 1.50 and 1.67 across Member States.

Derivation of these factors were based on purely qualitative arguments about what could be considered as an acceptable margin for new designs, considering the seismic margins at plant level reported by existing nuclear installations (see Refs [19] and [20]). That is, derivation of the factors was not based on the definition of acceptable seismic risk goals (see Section 5). If that had been the case, the factors would have been site dependent.

The BDBE may also be defined at a site specific hazard level represented by a given return period higher than the DBE, for example one decade. Specifying a scalar seismic margin constant over the spectral frequency range results in the BDBE and the DBE spectra having similar shapes, and the margin may be represented by a single point on the response spectrum, typically the peak ground acceleration (PGA). When the spectral shapes of DBE and BDBE are dissimilar, the margin may be represented by the average spectral acceleration over a representative frequency range.

The BDBE defines the required margin over the DBE at plant level, not at SSC level. Hence, special assessment procedures are needed to derive the seismic capacity of the installation as whole from SSC individual seismic capacities. This is in contrast with seismic design procedures, which work only at the SSC level, under the assumption that, if every SSC meets the limits given in the design code for the DBE, then the installation will be safe for the DBE.

Typical design approaches for nuclear installations against external hazards other than earthquakes, including aircraft crash, flooding, extreme winds, and explosions are discussed in Sections 4.3 to 4.5. A qualitative weighing approach such as proposed in reference [21] may be considered to define the safety margins required for these hazards.

4.3. DESIGN AGAINST AIRCRAFT CRASH

In a majority of the currently operating nuclear installations, the aircraft crash was not considered an applicable design external event. The event was screened out on the basis of low probability of occurrence.

[7] In some Member States, the ‘beyond design basis earthquake’ is designated as ‘design extension earthquake’.
[8] Core damage is normally used as a surrogate condition in NPPs.

However, in some Member States, the probability of occurrence of a crash during 'free flight' (i.e. out of airways or aviation corridors) of small general aviation aircraft or military fighters was not considered to be low enough, especially following a series of military aircraft crashes in Europe in the late 1970s. Consequently, impacts on the installation by small general aviation aircraft or military fighters were not screened out and the regulation specified the design aircraft crashes to be sustained by the nuclear installation[9].

The events of 11 September 2001 in the United States of America led to an international context in which many vendors considered the impact of a large commercial airplane in their standard plants design, irrespective of probabilistic considerations. This kind of impact is normally considered by vendors and regulators as a 'beyond design' scenario, for which 'best estimate', non-conservative acceptance criteria are used [22].

As a result, the current context is that the designer may be given two or more aircraft crash events of different severities for the 'design': design basis events and beyond design basis (or 'design extension') events. The first set is for design and the second one is for a performance evaluation of the design against predefined objectives specified by the regulatory body. In contrast with other external events, given the potentially large differences in severity between the design basis crashes and the beyond design basis crashes, the design for design basis impacts may not guarantee an acceptable performance during the beyond design basis external events.

In this context, features introduced by the designer to increase the robustness up to the required performance for the beyond design basis level are part of the 'design' process. However, it is clear that performance for the beyond design basis event needs to be assessed under rules different from those used for the design basis events [22]. Namely, the procedures are not the same as those used to verify that the design is valid for the specified design basis external event.

4.3.1. General workflow

From a general perspective, the design process against accidental aircraft crash consists of the following steps [15], as far as this external hazard is applicable to a particular installation:

(1) Define the impact scenarios to be used for the design, consistent with the site specific hazard assessment [23] and the applicable design requirements established or adopted by the national regulatory body. An impact scenario is defined by an aircraft (type, dimensions, mass, speed, angle of attack, amount of jet fuel) and an impact point within the installation. Impact scenarios need to conservatively envelope all impact possibilities.

(2) Define the design category of the SSCs within the nuclear installation, consistent with their safety classification. Requirements, or objectives to be reached through the design process, are different for the different categories.

(3) Select the applicable standards and guidelines, consistent with the design requirements, providing the acceptable limits and conditions of the SSCs behaviour in case of a crash to ensure that the intended safety functions are performed as required.

(4) Evaluate the local response, global response, induced vibration effects and secondary effects (jet fuel fire) on the SSCs due to the design basis crash scenarios, according to relevant national or international codes, standards and proven engineering practices and as recommended or accepted by the national regulatory body.

(5) Verify that the demand on each SSC does not exceed the capacity and limits established by applicable national or international codes, standards and proven engineering practices recommended or accepted by the national regulatory body.

[9] For example, in France, regulation RFS I.2.a states that impact by a general aviation aircraft can hardly be screened out within the French territory and it suggests consideration of two representative impacts in the design: a single engine CESSNA 210 (1500 kg) crash and a twin engine LEAR JET 23 (5700 kg) crash, both at 100 m/s.

(6) Assess the performance of the installation for the prescribed beyond design basis aircraft crash. This assessment is carried out using procedures which are different from the ones used for design purposes, as utilized in the previous steps in that they emphasize the use of realistic and best estimate assessments [22].

As mentioned in the previous section, in the current international context it is unlikely that design for the design basis crash provides sufficient robustness for a larger aircraft crash. Hence, Step 6 will very likely be started earlier in the process and it could govern the design.

Given the severity of the larger aircraft crashes that are currently specified, acceptability criteria are relaxed with respect to the ones used for design basis crashes (see Refs [5, 22, 24]). In general, acceptance criteria for these crashes are chosen so that, as a minimum, the safety related items of the nuclear installation that are involved in DiD Level 4 remain functional[10]. In other words, the goal is that the beyond design basis crash does not lead to early or large radioactive releases.

4.3.2. Sources of conservatism and consideration of uncertainties

There is no experience of a nuclear installation being impacted by an aircraft. Therefore, the sources of conservatism embedded in the procedures used by the designers can only be inferred. Conservatisms may include, for instance:

- Enveloping impact scenarios. The design basis aircraft is assumed to crash at the most unfavourable positions of the nuclear installation.
- Perpendicular impact of the aircraft is assumed, in which transfer of kinetic energy to deformation energy in the target is maximized. Normal impact is an idealization which can be very difficult to achieve in a real scenario, especially for impacts on spherical or cylindrical surfaces.
- Formulas used to assess local effects (scabbing, spalling, penetration) include safety coefficients with respect to empirical results [22]. In addition, these formulas were derived using tests in which the reinforced concrete targets were only lightly reinforced, if compared with regular reinforcement in, for instance, an outer containment shell.
- When assessing global effects of the crash, energy dissipation at the impact zone (e.g. cracking or fracture of concrete) is often underestimated.
- Strain-rate effects on ultimate strengths of steel and concrete are often underestimated due to lack of project specific experimental programmes. Non-specific results, coming from general experimental programmes, are usually conservatively adapted to project conditions.
- The amount of jet fuel usually considered for assessing secondary effects (e.g. fire, explosion) close to the maximum capacity of the fuel tanks, not considering the amount of fuel already consumed by the aircraft for taking-off and during the flight before the crash.

Once the required impact scenarios are specified, design against aircraft crash is deterministic. For design basis scenarios, safety factors are introduced to account for uncertainties.

For large aircraft crash scenarios, the highly non-linear nature of the response requires the use of best estimate approaches to the response computations. The numerical simulations to obtain the structural response (demand) is usually median centred. Given the level of effort required for the large aircraft crash computations, uncertainties around the best estimate values of the response are usually not investigated and quantified within a particular project. The analyst just checks compliance with performance requirements using the median response. At most, uncertainties in the response are

[10] In some States, a scenario in which either the containment function or the heat removal function is kept is considered as acceptable.

estimated using the results of research projects[11]. Capacity checks, required to assess compliance with the performance objectives, are usually performed on a best estimate (median capacity) basis, with limits derived from test results.

4.3.3. Performance to be achieved by the design

For seismic or other natural external hazards, the severity is usually defined using a single parameter with a continuous variation, for example, maximum flood level or the maximum ground acceleration. In the case of aircraft impact, the severity of the hazard depends on the size of the aircraft in the possible impact scenarios. Continuous variation of size does not occur in practice since size depends on the categories of aircraft in operation.

Given this characteristic of the hazard, the concept of 'margin' to be used in addressing the requirements established in SSR-2/1 (Rev. 1) [2], to have "an adequate margin to protect items important to safety against levels of hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects" (para. 5.21), and "an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site" (para. 5.21A), needs to be interpreted.

The approach followed in some Member States defines several categories of aircraft in terms of maximum take-off weight and velocity range at impact. Table 5 provides an example of such a categorization, with five categories of aircraft. If design is specified for aircraft within one category, 'margin' could be interpreted as linked to the next more severe category of impact that the installation is able to withstand with an acceptable performance.

For instance, the design basis crash could correspond to a Category A aircraft or to a military fighter (Table 5), whereas the required performance could be specified for an impact by a Category B, C or even D aircraft.

TABLE 5. AIRCRAFT CATEGORIES FOR AIRCRAFT CRASH CAPACITY ASSESSMENT

Category	Maximum take-off weight (kg)	Velocity range (m/s)	Examples
A	< 20 000	40 – 180	**General aviation planes** Cessna 210, LearJet 23, Canadair WaterBomber
B	< 100 000	70 – 195	**Light weight passenger planes** Boeing 720, Boeing 737, Airbus A320
C	< 200 000	70 – 215	**Medium weight passenger planes** Boeing 767, Airbus A300
D	> 200 000	70 – 175	**Heavy weight passenger aircraft** Boeing 747, Airbus A340, Airbus A380
Military fighters	< 35 000	< 220	Eurofighter, Rafale, Phantom

Note: Velocity ranges correspond to generally accepted limits for low level flying close to an industrial facility, for each aircraft category. At present, there is no international standard giving aircraft impact velocity values for assessment of beyond design conditions. Experiences with flight simulators show that large airplanes are less manoeuvrable than smaller airplanes, thus making it more difficult to impact the intended target with peak speed [25].

[11] The OECD/NEA IRIS_2012 benchmark study [26], [27] concluded that, for an experienced team using calibrated simulation tools, a coefficient of 1.4 applicable to simulation results (displacements, strains, residual velocities, …) would cover the uncertainties.

4.4. DESIGN AGAINST FLOOD

Design against external flood needs to cover several types and combinations of flooding phenomena, depending on the site. These include both natural phenomena (e.g. high river or lake water, ocean flooding such as from high tides combined with wind driven storm surges, extreme precipitation, tsunamis, seiches, flooding due to dam failure, and flooding from landslides), with due account of climate change effects, and human induced events (principally, release of flow from water control structures) [15].

The 'dry site' concept defined in para. 7.5 of IAEA Safety Standards Series No. SSG-18, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations [28] is considered the best layout approach for protection against the design basis floods. Following this approach, plant grade level around buildings and other components important to safety are located above the maximum level predicted for the flood according to the results of the flood hazard assessment.

When the 'dry site' concept cannot be applied for the design basis flood, as described in the previous paragraph, the design needs to include permanent flood barriers or protections, with carefully selected design bases (e.g. hydrodynamic effects, impacts from floating bodies, seismic qualification).

For beyond design basis floods, permanent or temporary flood barriers may be introduced to protect SSCs important to safety.

Flood barriers may not protect against local intense precipitation at the site, which could exhaust the capacity of the drainage systems at roofs and roads within the site and lead to entrance of water in buildings important to safety. Hence, maximum local precipitation intensity, and not only maximum level in water bodies, is an important parameter derived from the flood hazard assessment.

4.4.1. General workflow

From a general perspective, the design process against flood consists of the following steps [15]:

(1) Define the flood levels and maximum local precipitation intensities to be used for the design, consistent with the site specific flood hazard assessment [28], the external flood performance goal of the nuclear installation, and the applicable design requirements established or adopted by the national regulatory body.

(2) Define the design category of the SSCs within the nuclear installation, consistent with their safety classification. Requirements, or objectives to be reached through the design process, are different for the different categories.

(3) When the 'dry site' concept is used for the design basis flood level, then no particular provisions are introduced against flood in the design, except for drainage systems within the site to cater local precipitation. Drainage systems are designed to evacuate the design local intense precipitation.

(4) When the 'dry site' concept is not used for the design basis flood level, then the design needs to introduce flood protection barriers. Applicable standards and guidelines are to be selected, consistent with the design requirements, providing the acceptable limits and conditions for the barriers to ensure that the intended safety functions are performed as required.

(5) Evaluate the demand on the barriers due to the design basis flood, according to relevant national or international codes, standards and proven engineering practices and as recommended or accepted by the national regulatory body.

(6) Verify that the demand on each barrier does not exceed the capacity and limits established by applicable national or international codes, standards and proven engineering practices recommended or accepted by the national regulatory body.

(7) Assess the overall design for a 'beyond design basis' flood. The purpose is to find the flood severity (e.g. flood height or local precipitation intensity) which would cause the loss of a fundamental safety

function in the nuclear installation and, in addition, the severity that would cause the loss of SSCs ultimately necessary to prevent early radioactive release or a large radioactive release. In general terms, deterministic, semi-probabilistic and fully probabilistic approaches for external flood safety assessment are available [7].

Flood caused failure of equipment is typically due to immersion, although in some instances, particularly applicable to structures, the failure may be due to flow induced phenomena (e.g. impact by floating bodies). The designer needs to account for the ability to survive and to function for each equipment item susceptible to flooding. Usually, it is assumed that equipment submerged by the flood waters, and not specially protected, will fail.

During the safety assessment for a 'beyond design basis' flood, the analyst assesses the capacity of flood barriers, such as dikes or doors, looks for the ways through which water could reach SSCs important to safety, and computes the flow capacity of them (e.g. building penetrations) for determining times at which equipment could be rendered out of service. For exposed equipment and structural components, the analysis also involves the assessment of capacity against impact of floating bodies and sedimentation. For a particular site, both impact velocities and amount of sediments can usually be linked to the flood height.

The main result of the safety assessment for a 'beyond design basis flood' is the margin over the design basis flood, that is, the maximum flood for which there is high confidence that the installation will maintain its fundamental safety functions. In addition, the results normally identify 'weak links' in the design which, if addressed, may lead to an overall improvement of the flood safety robustness of the nuclear installation.

4.4.2. Sources of conservatism and consideration of uncertainties

There is operating experience of NPPs going through severe flood events (see Section 3.2). In one case, the Fukushima Daiichi nuclear power plant, the flood caused a severe accident. In this case, the flood level very significantly exceeded the design flood level. In other cases, where the design flood level was not exceeded or only slightly exceeded, operators were able to manage the emergency situation and no severe accident took place.

Flood hazard is the only known external hazard which has led to a severe accident in an NPP. Operating experience shows that flooding of a site above a certain level may have serious safety consequences. Flood hazard lends itself to very clear cliff edge effects. A small rise of water level may produce large effects in the nuclear installation, since a small rise over a threshold could start flooding of a significant number of SSCs important to safety.

In this case, any conservatism of the design comes mainly from the flood hazard assessment, since it determines maximum flood levels and maximum local precipitation intensities that are provided to the designer to define the layout and to design flood barriers, if applicable. Given the potential consequences, it seems advisable that those site parameters are determined with some degree of conservatism, consistent with the uncertainties in the hazard assessment. Design is performed deterministically, using applicable design standards once the site parameters are given to the designer.

Regarding flood capacity assessment, the assumption that not specially protected equipment will fail if submerged by the flood waters is close to reality. Electrical equipment may also fail due to ground failures induced by the flood. Conservatism may arise in the estimation of the water depth that would produce the failure.

4.4.3. Margin to be achieved by the design

When a probabilistic definition of the hazard is available (e.g. flood level vs. annual frequency of exceedance), a flood with a smaller AFE than the design basis flood may be used to define the margin to be achieved by the design.

Flood due to meteorological and hydrological causes results from complex temporal and spatial stochastic phenomena. The ability to predict their future occurrence is subject to data limitations and incomplete understanding of the physical phenomena [7]. As a result, despite recent developments, a unified approach for probabilistic methods is not yet generally available. Flood hazard assessment for nuclear installations is currently mostly based on statistical extrapolation of historical data. The 'reasonable' limit for extrapolation to low annual exceedance probabilities by only statistical means is a topic that has been under debate. Estimation of uncertainties in the hazard heavily relies on expert opinion.

Flood hazard due to long period waves, tsunamis and seiches is typically assessed using a deterministic or semi-probabilistic approach [7]. Even though a large research effort on the assessment of tsunami hazards was started worldwide after the 2004 tsunami in the Indian Ocean and the Great East Japan Earthquake of March 2011, the results of this effort are still in the process of being incorporated into engineering practice. Particularly, even though the basis for a probabilistic tsunami hazard assessment has been defined, in analogy to probabilistic seismic hazard assessment (PSHA), it is not yet the current practice applied by Member States for assessing tsunami hazards.

Regarding flood due to failure of water control structures, such as upstream dams, the probability of flooding at a site due to dam failures is determined by assessing the probability of failure of a dam upstream of the site and then determining the consequences of the failure [7]. SSG-18 [28] recognizes that it is generally very difficult, expensive and time consuming to assess the safety and stability of a water control structure beyond the limits of the nuclear site, not to mention the calculation of failure frequencies. Hence, when the hazard cannot be screened out, typically, the effects in the nuclear site are assessed using a deterministic approach, in which the potential dam failure modes are postulated based on the type of dam and the characteristics of the dam site.

The conclusion of the paragraphs above is that it is nowadays uncommon that the flood margin to be achieved by the design could be established with confidence based only on a probabilistic definition of the hazard.

4.5. DESIGN AGAINST OTHER EXTERNAL HAZARDS

Previous sections provide an overview of the general workflow, sources of conservatism and the margin to be achieved by the design in the case of three usually significant external hazards. SSG-68 [15] considers design against other potentially applicable hazards, which are usually less significant than the ones dealt with in the previous sections. Those include extreme winds, hazardous releases, external explosions, impact by floating bodies, electromagnetic interference, biological hazards and lightning, etc.

Except perhaps for extreme winds, it is relatively uncommon that natural hazard assessments resulting from the site investigation are given by a set of hazard curves relating a hazard severity parameter with an annual frequency of exceedance, including uncertainties (fractiles). The most common situation is similar to what has been described above for the flood hazard. Deterministic or semi-probabilistic approaches are used. Consequently, the basis to define the margin to be achieved by the design based on risk considerations is less firm than desirable; a performance based probability or agnostic approach needs to be used to some degree.

For human induced hazards, such as external explosions, chemical releases or ship impact, whenever they are not screened out during the site evaluation, it is common that design values are specified based

on the current conditions at nearby transportation routes or industrial facilities. In these cases, the margin to be achieved by the design considers transportation accidents that, even though extremely unlikely, cannot be ruled out. Margin actually achieved by the design may be assessed using the approaches described in Safety Reports Series No. 88, Safety Aspects of Nuclear Power Plants in Human Induced External Events: Margin Assessment [5].

4.6. EVOLUTION OF THE DESIGN APPROACHES

Design approaches for external hazards have evolved in the past decades. In Generation II reactors, designed in the 1970s or early 1980s, design basis events were defined deterministically with the idea that events beyond a design basis event were either 'impossible' or had a negligible likelihood. The design process was targeted to show that SSCs met the limits given in the design codes when subjected to the design basis events. When those conditions were met, it was (deterministically) assumed that failure would not occur.

In the 1970s and 1980s the idea that both external hazards and 'resistance' properties have an uncertain nature started to gain wider recognition among design code developers [29]. Semi-probabilistic approaches to safety were introduced in some codes [30]. Calculation methods, values for load and resistance factors, as well as safety margins were adjusted based on tradition, risk based calibration or a combination of both [31]. However, this was not visible for the designer since the format of the design process remained the same and the codes usually did not mention their target reliabilities (maximum acceptable probability of failure).

In the nuclear industry, the Three Mile Island accident, in March 1979, was an indication that events not considered in the design could happen. In the wake of this accident, the U.S. Nuclear Regulatory Commission (NRC) launched its severe accident policy in 1988 with the purpose of exploring beyond design basis conditions [32]. Design bases of existing nuclear installations were not changed. However, probabilistic approaches were introduced to find out what could happen, with what frequency and what would be the consequences (risk). Hence, having events beyond the design bases were not considered 'impossible' anymore.

The U.S. NRC severe accident policy was applied not only in the United States of America, but also in other Member States which closely follow U.S. NRC regulation. Therefore, risk metrics considered acceptable in the United States of America began being accepted internationally.

The U.S. NRC severe accident policy was extended to external hazards in 1991 [33], which motivated the computation of safety 'margins' above the design basis external events for existing nuclear installations and for a number of hazards, including earthquakes, external flood, high winds, and transportation and nearby facility accidents. The idea was to understand the most likely severe accident sequences that could occur in a particular plant due to external events and to find plant specific vulnerabilities that could be fixed with low cost improvements. Implicitly, there was a recognition that there might be a non-negligible probability of occurrence of events beyond the design basis event.

For new nuclear installations, new requirements were introduced with the idea that the margins above the design basis events achieved by the new designs were, at least, at the same level as the margins found for existing nuclear installations. The new requirements applied mostly to the earthquake hazard and introduced the need to assess the margin above the design basis event in the resulting new designs, even before construction [19]. This would add to the robustness of the design achieved following the traditional approach.

After the Fukushima Daiichi accident in March 2011, the nuclear industry worldwide realized the need to explore "what if" the design basis external events are exceeded, especially for natural hazards such as earthquake and flood. Such exceedances could be the result of underestimation of site hazards due to incomplete data or the use of outdated hazard assessment procedures.

Following this idea, many Member States undertook a thorough review of safety against external events was undertaken for existing nuclear installations, followed by hardware modifications in many of them to improve robustness against external hazards, either increasing capacity or adding redundancy and diversity.

Regarding new nuclear installations, the current design approach for Generation III+ or Generation IV reactors includes the need to show that the resulting designs have adequate margins above the design basis external events to avoid ‘cliff edge’ effects for small exceedances of the design basis event and, for natural hazards, there is a need to demonstrate that the margin is adequate to prevent early or large releases. IAEA safety standards include these requirements since 2016 (see GSR Part 4 (Rev. 1) [1] and SSR-2/1 (Rev. 1) [2]).

5. ADEQUACY OF DESIGN ROBUSTNESS AGAINST SEISMIC HAZARD

5.1. CHARACTERIZING INSTALLATION PERFORMANCE

5.1.1. Characteristics of seismic hazard

Seismic events, like the events resulting from many external hazards, are common cause failure (CCF) events. Earthquake shaking can cause concurrent damage of SSCs in the installation and in surrounding infrastructure. Moreover, earthquake shaking may lead to or be accompanied by geotechnical failures that affect wide areas at once (e.g. slope instability and liquefaction) and result in classic CCFs. In addition, seismic induced damage to certain SSCs can trigger hazardous events such as internal fire, explosion and flood, which are typically of CCF nature. Finally, seismic induced events can lead to consequential sitewide hazards such as landslides and external flood due to seiche, tsunami, or upstream dam breach.

The ability of operators to perform safety actions may be impeded due to the occurrence of concurrent multiple failures in the installation. The ability of on-site and off-site emergency responders to access the installation may be impeded by damage to the surrounding transportation infrastructure. Seismic events can lead to severe accidents. Even though earthquake experience does not include a major accident caused by the direct effects of the earthquake shaking, one of the worst accidents to occur at a nuclear installation was caused by the 2011 Great Tohoku Earthquake-induced tsunami inundation at the Fukushima Daiichi nuclear power plant (see Section 3).

Uncertainty in seismic hazard analysis is substantially large. It is common that the 5% to 95% bounds on the predicted AFEs of ground motions from PSHA are separated by one to two orders of magnitude. This substantial range is caused by compounded uncertainties from several input constituents of the PSHA, for instance, earthquake event occurrence rates[12], rupture geometry, relationships that model the seismic wave propagation or attenuation from rupture source to site, and local site subsurface properties. IAEA Safety Standards Series No. SSG-9 (Rev. 1), Seismic Hazards in Site Evaluation for Nuclear Installations [34], summarizes the sources of uncertainty in PSHA.

5.1.2. Seismic hazard assessment requirements

Assessment of the design robustness against seismic hazard needs to be performed on a site specific basis. A nuclear installation design that is adequate for a range of seismic activity and site conditions may not be adequate if constructed elsewhere. As discussed in Section 5.2.3, the adequate margin for design robustness against seismic hazard can be determined based in part on a comparison of the estimated annual frequency of unacceptable performance to a performance goal. A probabilistic characterization of seismic hazard at the installation site is needed to make this determination. Such characterization defines a family of hazard curves describing the AFE of one or more ground motion parameters (e.g. peak ground acceleration, PGA, and spectral accelerations, S_a). The family of hazard curves for each parameter consists of multiple fractiles representing discrete confidence intervals and a mean curve representing the best estimate AFEs [34]. Alternately, a deterministic characterization of the site specific ground motion spectrum may be used along with a conservative estimate of the mean hazard curve slope following Section 5.2.3.2.

On the other hand, there is a recognized need to evaluate design robustness on a site-generic basis, for example, for standard designs of NPPs. Adequate design robustness seismic margins for such applications can be determined without a site specific hazard by performing seismic analyses for a range of site conditions and corresponding ground motion spectra. This type of generic margin assessment may be used to qualify the robustness of a standard design against a predetermined suite of earthquake ground motions. Robustness of this design for construction at a specific site needs to be later verified on

[12] For example, future occurrence rates of earthquake with a given magnitude are modelled based on historical data over hundreds of years to estimate ground motion hazard with return periods of tens of thousands of years.

a case-by-case basis by comparing the site specific spectrum required for adequate margin at this site to the generic spectra used in the design qualification. The generic spectra need to envelop the site specific one. If they do not, then additional justification of the design robustness has to be performed.

In addition to vibratory ground motion hazard curves, hazard characterization needs to be performed for other seismic induced hazards that cannot be screened out from consideration in the margin assessment. Section 5 of SSG-89 [13] includes recommendations for characterizing these hazards for seismic margin assessment.

5.1.3. Defining performance objectives

For the robustness of the nuclear installation design, performance against seismic hazard is defined in terms of the installation's ability to maintain its fundamental safety functions[13]. Selection of the acceptable performance objective for a nuclear installation is the purview of the national regulatory bodies in each Member State. The acceptable performance objective may be specific to each safety function. For modern designs, the acceptable performance is typically more stringent for an installation's ability to maintain DiD Level 4 safety and mitigation functions than it is for maintaining DiD Level 3 safety functions [2].

Performance objectives can generally be defined using one of two formats: scenario based and annual frequency based. A scenario based performance objective requires that the installation design demonstrates the ability to maintain its required safety and mitigation functions with acceptable confidence when it experiences a given defined earthquake scenario, as is typically done using the seismic margin assessment (SMA) or the probabilistic risk assessment (PRA) based SMA methodology. The installation-level high confidence of low probability of failure (HCLPF) capacity[14] is the typical metrics of seismic margin[15] used in both SMA methodologies.

An annual frequency based performance objective requires that the installation design demonstrates that the annual frequencies of failing to maintain its required safety and mitigation functions (e.g. CDF and LERF for NPPs) do not exceed acceptable limits, as typically determined using the seismic probabilistic safety assessment (SPSA) methodology. Conceptually, the SPSA methodology calculates annual frequencies by aggregating the product of scenario based probabilities of unacceptable performance and the annual rates of each scenario occurrence over the credible range of scenarios. In addition, the SPSA methodology can also determine the installation-level HCLPF capacity. Since the logic trees of the installation failure sequences are explicitly modelled in the SPSA and PRA based SMA methodologies, correlations between seismic induced failures of SSCs due to the CCF nature of the earthquake can be more readily represented. Traditionally, strongly correlated failures can be idealized as one failure and weakly correlated failures are idealized as independent in the logic tree; additionally, methods exist to model partial correlation.

SMA, PSA based SMA, and SPSA are well established methodologies for seismic safety assessment with wide international recognition and adoption by Member States. Safety Reports Series No. 103 [6] and IAEA-TECDOC-1937 [35] provide detailed technical guidance on executing these methodologies.

Determining a HCLPF capacity as a performance measure has the advantage of utilizing seismic response and capacity analysis methods that are familiar to design engineers. These methods use procedures similar to deterministic design codes and standards to account for the effect of uncertainty on the seismic margin. Determining annual frequency based performance measures has the advantages of establishing a performance benchmark that can be universally compared across multiple installations and the explicit incorporation of uncertainty. Section 5.2 describes the selection of a margin based

[13] For NPPs, Requirement 4 of SSR-2/1 (Rev. 1) [2] lists the fundamental safety functions as: "(i) control of reactivity; (ii) removal of heat from the reactor and from the fuel store; and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases."

[14] Unless otherwise indicated, references to the HCLPF capacity in this publication are applicable to installation level.

[15] The HCLPF capacity is typically expressed either in terms of the corresponding ground motion parameter, for instance, HCLPF PGA = 0.2 *g*, or the margin above a given earthquake, for instance, the DBE (for example, HCLPF = 2 × DBE).

robustness measure that combines the relative simplicity of HCLPF capacity calculation with the more explicit annual frequency based performance objectives.

5.2. ASSESSMENT OF SEISMIC MARGIN

As mentioned in Section 5.1.3, the HCLPF capacity is commonly used as an internationally recognized measure of seismic margin. This section introduces the relationship between the HCLPF capacity and the installation-level seismic fragility, uses it to derive annual frequency performance estimates from the scenario based margin, and identifies the adequate seismic margin to achieve risk informed performance goals. Section 5.2.1 reviews the basic elements of seismic fragility functions and discusses the construction of an installation-level fragility curve using SPSA output and the estimation of this curve using SMA output. Section 5.2.2 discusses the characterization of scenario based installation performance and estimation of annual frequency based performance metrics from seismic margin. Section 5.2.3 uses the performance metrics developed in Section 5.2.2 to characterize the constraints on seismic margin such that it achieves the performance goals applicable to the installation.

5.2.1. Installation-level seismic fragility development

A fragility curve is a function that expresses the conditional probability of failure for increasing values of the hazard parameter. The hazard parameter used in a seismic fragility curve is the ground motion amplitude. Without loss of generality, the PGA will be used as the ground motion parameter of choice in this discussion since it is the most commonly used parameter in practice. The spectral acceleration at any natural period can be used instead following the same discussion. The selection of the appropriate ground motion hazard parameter for the installation is outside the scope of this publication. In an installation-level fragility curve, 'failure' is defined as discussed in Section 5.1.3.

Figure 3 shows an example seismic fragility curve from IAEA-TECDOC-1937 [35]. The median PGA, A_m, is the PGA at which the conditional probability of failure is 50%. The 5% and 95% fractile fragility curves represent uncertainty bounds on this median capacity. In Fig. 3, the median PGA, A_m, is modelled as a random variable with log-normal probability distribution that has a median value of 0.7 *g* and a logarithmic standard deviation $\beta_u = 0.4$. This uncertainty represents the combined effects of uncertainty in material properties, structure properties, soil properties, strength and other seismic qualification parameters, analysis methods, etc. The variability in failure probability due to randomness in the ground motion input and structure response to it (e.g. vibration mode combination and phasing) is modelled using a log-normal probability distribution with median equal to 1.0 (i.e. median centred analysis parameters were used) and a logarithmic standard deviation $\beta_r = 0.3$. The mean fragility curve combines the effects of randomness and uncertainty to calculate the best estimate conditional probability of failure at each PGA and has a composite logarithmic standard deviation $\beta_c = (\beta_u^2+\beta_r^2)^{0.5} = 0.5$ in this example. An important point on the fragility curve is the HCLPF capacity, characterized by the PGA corresponding to the 5% probability point on the 95% confidence-level fragility curve. When β_u and β_r have comparable values, such as shown here, the HCLPF capacity is nearly equal in value (equal or slightly higher) to the 1% point on the mean fragility curve.

An installation-level seismic fragility curve can be constructed explicitly using the SPSA methodology. Safety Reports Series No. 103 [6] provides an example fragility curve construction. The SPSA explicitly accounts for the effects of uncertainty and can therefore explicitly develop the full family of fragility curves. The PSA based SMA methodology is typically used to estimate the HCLPF capacity only, but it can be used to develop an estimate of the installation-level mean fragility curve. Reasonable assumptions may then be used to split out the estimated composite variability into uncertainty and randomness components if needed. The traditional SMA methodology can only be used to estimate the HCLPF capacity.

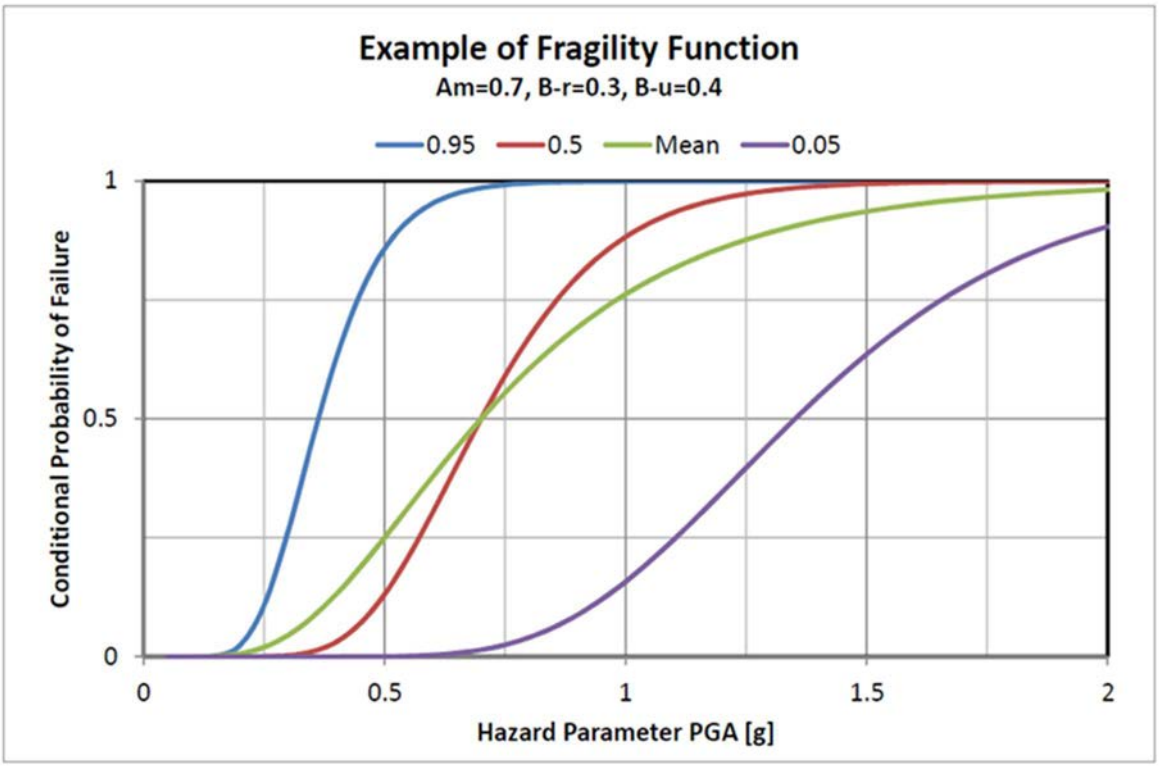

FIG. 3. Example family of seismic fragility curves [35].

If only the HCLPF capacity is determined using the SMA or PSA based SMA methodologies, the installation-level fragility curve can be approximated by fitting a representative composite logarithmic standard deviation β_c into the HCLPF capacity to estimate a median capacity. Reference [36] suggested that β_c = 0.3 is appropriate for typical installation-level seismic fragility curves[16]. Examination of installation-level seismic fragility curves compiled in Ref. [37] from recent SPSAs performed at 18 NPPs in the United States of America using modern methods, confirmed that β_c = 0.3 is representative of their range[17]. Accordingly, a HCLPF capacity can be used to generate an estimate of the installation-level mean fragility curve as follows:

$$\beta_c = 0.3$$
$$A_m = A_{HCLPF}\, e^{\beta_c\, \Phi^{-1}(0.01)} = 2.01 \times A_{HCLPF} \approx 2 \times A_{HCLPF} \quad (1)$$

This estimate of A_m considers A_{HCLPF} to correspond to the 1% point on the mean fragility curve. Estimating A_m considering the alternate definition of the HCLPF capacity gives $A_m = 2.00 \times A_{HCLPF}$, that is, the estimate remains unchanged.

An installation-level median capacity estimate of twice the HCLPF capacity is therefore considered to be a best estimate generic value in the absence of an explicit quantification. The uncertainty in the seismic fragility may be estimated by splitting the composite variability into independent components for randomness and uncertainty. The randomness component is more well constrained since it is dominated by inherent randomness due to the ground motions rather than the state of knowledge about the different parameters in the fragility evaluation. Reference [38] recommends a generic β_r value of 0.24 for individual SSCs and recommends SSC-dependent generic values for β_u that are typically higher

[16] The potential occurrence of cliff edge effects at ground motion amplitudes not sufficiently higher than the HCLPF capacity may lead to exceptionally low values of β_c. A robust design includes sufficient margin against cliff edge effects. Section 7.2 discusses the determination of the corresponding ground motion amplitude.

[17] Several studies in the literature indicate that the risk convolution integral is mildly influenced by small variations in the value of β_c. Reference [39] reported limited sensitivity to using β_c = 0.4 instead of 0.3.

than β_c. Reference [36] indicates that variability in the installation-level fragility curves is typically lower than that for individual SSCs, which is confirmed by review of recent SPSAs. Accordingly, the following generic values of installation-level randomness and uncertainty that produce a composite variability, β_c, equal to 0.3 are considered reasonable estimates to consider in establishing guidance for adequate seismic margins to achieve design robustness:

$$\beta_r = 0.18$$
$$\beta_u = 0.24 \quad (2)$$

5.2.2. Margin based performance prediction

5.2.2.1. Scenario based performance characterization

Seismic margin is described using the installation-level HCLPF capacity, namely, the ground motion amplitude at which the conditional probability of failure is 5% on the 95% fractile fragility curve, or 1% on the mean fragility curve. These conditional probabilities define the scenario based performance achieved by the installation when the ground motion spectrum anchored to the HCLPF capacity defines the scenario (i.e. HCLPF capacity spectrum). The HCLPF capacity may be determined using SMA, PSA based SMA, or SPSA. The conditional probabilities of installation failures to maintain safety functions are higher for earthquake scenarios more severe than the HCLPF capacity spectrum and lower for less severe ground motions, as seen in Fig. 3.

5.2.2.2. Annual frequency based performance characterization

Quantification of annual frequency based performance involves combining the mean seismic hazard curve and mean fragility curves for the installation (one fragility curve for each safety function in the evaluation). The hazard and fragility curves are convolved, that is, integrated to compute the mean annual frequency of unacceptable performance of the installation, which represents the performance metric [36].

When the following input data is known for an installation site, the frequency based performance metric can be estimated based on the margin assessment, as described below:

Input data:

- A_{DBE} — DBE ground motion parameter (PGA or S_a)
- Mean hazard curve:
  - T_{DBE} — Mean return period for the DBE
  - A_R — Increase in the ground motion parameter value corresponding to a 10-fold reduction in annual exceedance frequency, in the hazard range of interest
- A_{HCLPF} — HCLPF ground motion capacity (PGA or S_a)
- β_c — Estimated composite variability (see Section 5.2.1)

Calculated parameters:

In Ref. [40], the following closed form solution of the convolution integral for typical fragility and hazard curve shapes (Annex I) was derived:

$$\lambda_f = K_1 \ (A_m)^{-K_H} \ e^{0.5\,(K_H\,\beta_c)^2} \quad (3)$$

where:

λ_f = mean annual frequency of installation failure (e.g. CDF for an NPP);
K_H = $1/\log_{10}(A_R)$, it is the slope of the hazard curve in log-log space;

$K_1 =$ $(A_{DBE}{}^{K_H} / T_{DBE})$, it is the constant that anchors the hazard curve;

$A_m =$ $(A_{HCLPF})\ e^{2.33\ \beta_c}$, it is the estimated median capacity (see Section 5.2.1).

Annex I presents the details of developing this frequency based performance estimate from the seismic margin and hazard curve and discusses the influence of parameters A_R and β_c on the outcome, given the seismic margin capacity characterized by HCLPF.

5.2.3. Adequacy of seismic margin

For a robust design, the installation-level HCLPF capacity is required to be higher than the DBE scenario. The minimum acceptable margin between the HCLPF capacity and the DBE needs to be sufficient to achieve the required scenario based and annual frequency based performance objectives for the nuclear installation (see Section 5.1.3). The seismic margin over the DBE is defined by the ratio $R = A_{HCLPF} / A_{DBE}$.

Adequacy of the seismic margin for a scenario based performance objective can be readily assessed by comparing the ratio R to the target minimum set by the national regulatory body (see Section 5.1.3). Adequacy of the seismic margin for an annual frequency based target set by the national regulatory body can be assessed using the relationships presented in Section 5.2.2.

As seen in Section 5.2.2, the annual frequency based performance metric outcome is a function of the slope of the seismic hazard curve at a site. In order to achieve the same annual frequency, the adequate margin at an installation where the hazard curve has a relatively flat slope would be different, namely, larger than that for the same installation if the hazard curve has a relatively steep slope. Section 5.2.3.1 presents the margin required to achieve the target annual frequency. Section 5.2.3.2 discusses considerations for minimum and maximum required margins independent of the site specific hazard. Section 7.2 discusses margin adequacy considerations to protect against cliff edge effects.

5.2.3.1. Target frequency based margin adequacy for site specific hazard

Input data:

$\lambda_{f,T}$ Annual performance goal (e.g. CDF)

A_{DBE} DBE ground motion parameter (PGA or S_a)

T_{DBE} Mean return period for the DBE

A_R Increase in A_{DBE} value corresponding to a 10-fold reduction in mean annual exceedance frequency, in the hazard range of interest

β_c Estimated composite variability (see Section 5.2.1)

Since the seismic margin is relative to the DBE (typically), a larger seismic margin is required in order achieve a more stringent annual performance goal. Specifically, the required target depends on the ratio of the mean AFE at the DBE, $H(A_{DBE})$, and the performance goal, $\lambda_{f,T}$. This ratio is expressed by the parameter R_{DP}.

$$R_{DP} = H(A_{DBE}) / \lambda_{f,T} = 1 / (\lambda_{f,T}\ T_{DBE}) \quad (4)$$

where R_{DP} is the ratio between hazard frequency corresponding to DBE and the performance goal.

The relationship between the HCLPF capacity and the annual frequency presented in Eq. (3) can be used to identify the HCLPF capacity and, therefore, the margin R, required to achieve a target annual frequency $\lambda_{f,T}$. Annex II presents the mathematical derivation of this required margin and discusses its sensitivity to the hazard slope parameter A_R and the ratio R_{DP}.

Calculated parameters:

$$
\begin{aligned}
K_H &= 1 / \log_{10}(A_R), \text{ it is the slope of the hazard curve in log-log space} \\
F(A_R) &= \exp[0.5\,\beta_c^2\,(K_H)^2] \,/\, \exp[2.33\,\beta_c\,K_H] \\
R &= [R_{DP} \times F(A_R)]^{1/K_H} \\
A_{HCLPF} &= R \times A_{DBE} = \text{minimum margin to achieve the performance goal, } \lambda_{f,T}
\end{aligned}
\tag{5}
$$

For the typical value of 0.3 for β_c, this required margin can be simplified as follows (Annex II):

$$
\begin{aligned}
R(R_{DP}=10) &= 1.0 \quad \text{at } A_R \le 1.6 \\
&= 3.0 \quad \text{at } A_R = 5.6 \\
&\qquad \text{with linear interpolation for } 1.6 < A_R < 5.6
\end{aligned}
\tag{6}
$$

$$
R(R_{DP}\neq 10) = R(R_{DP}=10) \times (R_{DP} / 10)^{1/K_H} \ge 1.0 \tag{7}
$$

If another value of β_c is desired to be used, the process presented in Annex II can be followed to derive similar equations. For installations with β_c higher than 0.3, the required margin as calculated above may be conservative. For installations with β_c lower than 0.3, the required margin as calculated above may be unconservative. Practically, the latter situation is addressed by ensuring adequate seismic margin against cliff edge effects, which is discussed in Section 7.2.

5.2.3.2. Alternative margin adequacy considerations

This Section discusses establishing a floor and a ceiling for the required margin, R.

As shown in Section 5.2.3.1, the seismic margin needed to achieve a certain annual frequency based performance objective may be equal to or near unity in relatively uncommon situations when the target annual frequency is not sufficiently high relative to the hazard slope and level of the DBE. However, a minimum margin above the DBE has to exist for a robust design (see Section 2.1). A scenario based performance goal sets a floor for a minimum acceptable margin above the DBE. The national regulatory body needs to establish this performance goal (see Section 5.2.1).

$$
R \ge R_{floor} \tag{8}
$$

As shown in Annex II, the annual frequency based adequate seismic margin unboundedly increases with the slope of the hazard curve, A_R. Within a given geographic region or Member State, knowledge of how high this parameter may get can be used to establish a ceiling on the adequate margin by the national regulatory body. This ceiling can depend on the installation type and the affected safety function.

$$
R \le R_{ceiling} = \left[R_{DP,max} \times F(A_{R,max})\right]^{log10(A_{R,\max})} \tag{9}
$$

where $R_{DP,max}$ is the maximum ratio of R_{DP} permitted by the national regulatory body for the installation and safety function being evaluated. This relationship can also be used to replace Eq. (6) if site specific A_R is not characterized at the installation (e.g. if deterministic hazard analysis is used for the safety assessment).

The adequate seismic margin for meeting performance objectives can therefore be concisely given by:

$$
R_{floor} \le R \le R_{ceiling} \tag{10}
$$

If specification of a single margin value is desired[18], the more stringent margin governs, and R has to be chosen as $R_{ceiling}$.

In the unlikely event that the value of $R_{ceiling}$ is lower than R_{floor}, which may happen in regions with steep hazard curves combined with relatively high DBE levels, the latter governs, and R has to be chosen as R_{floor}.

5.3. OTHER CONSIDERATIONS

To complete the ideas about adequacy of seismic robustness, this section provides a connection with the DiD philosophy and a series of remarks about uncertainty in the assessment of seismic margin.

5.3.1. Consequences to defence in depth

To be consistent with the DiD philosophy, the installation design has to be more robust for the last barrier against large releases (DiD Level 4) than for the control of the design basis accidents (DiD Level 3, e.g. core melting in an NPP). Accordingly, the seismic HCLPF capacity for a nuclear installation for DiD level 4 needs to be larger than HCLPF capacity of DiD level 3. The determination of adequate margin needs to consider the consequences of failure of the functions represented by the installation-level seismic fragility (see Section 5.2.1) and the corresponding DiD level. This consideration is applicable to both scenario based and annual frequency based performance margin adequacy.

The minimum scenario based performance goal is set by the national regulatory body (see Section 5.1.3). This target and the corresponding minimum seismic margin (see Section 5.2.3.2) has to be set higher for installation performance required to maintain DiD Level 4 than for DiD Level 3.

The seismic margin required to achieve an annual frequency based performance objective is determined according to Section 5.2.3.1. Requiring a higher margin for DiD Level 4 than DiD Level 3 failures has to be achieved by setting the target performance frequency smaller for DiD Level 4 than for DiD Level 3. The target annual frequency is set by the national regulatory body (see Section 5.1.3). Table 2 in IAEA-TECDOC-1791 [9] provides indicative values of frequency of occurrence of individual plant states with regard to postulated initiating events. It is expected that the target annual frequency for a large release is at least ten times lower than the frequency of core damage.

5.3.2. Treatment of uncertainty

Prediction of seismic performance includes aleatory (i.e. random) variability and epistemic uncertainty[19]. Design robustness requires predictability of the outcome, that is, safety, in the face of uncertainty. Predictability is achieved by requiring high confidence in the outcome, since certainty is not feasible (e.g. there is always a small but non-zero probability that the earthquake ground motion will be higher than considered in the safety assessment, such that a design that achieves 'certain' safety is prohibitive to construct). The selection of HCLPF capacity to characterize seismic margin addresses this consideration. The HCLPF capacity corresponds to 95% concurrent confidence in the effects of the sources of randomness and epistemic uncertainty. These two sets of variability sources are not statistically correlated and, therefore, unlikely to attain values that correspond to the worst 5% of their possible effect at the same time. Setting the HCLPF capacity at this high confidence limit for both sets combined can be shown to result in approximately 99% confidence in achieving the desired performance at the hazard severity level for the seismic margin.

Prediction of the annual frequency based seismic performance integrates (i.e. convolves) the hazard and fragility curves. The mean hazard and fragility curves represent best estimates of each, and their

[18] This may be desired to streamline regulatory requirements, especially if $R_{ceiling}$ is not unduly higher than R_{floor}.
[19] 'Aleatory' is inherent and not reducible by more data or knowledge advancement, while 'epistemic' refers to the limits of available data and/or knowledge.

convolution as described in Section 5.2.2 results in a point estimate of the annual frequency of installation failure. Due to the non-symmetric shapes of the hazard and fragility distributions, this point estimate of the mean performance corresponds to a higher than 50% confidence, typically between 70% and 85% confidence for NPPs. There is a minor probability that this best estimate may be significantly exceeded. However, setting a target annual frequency based seismic performance at a confidence level as high as 99%, similar to HCLPF capacity, is prohibitive for design. Current regulations in most Member States use the mean annual frequency to define the goals for acceptable performance.

Use of the mean annual frequency in conjunction with the installation-level HCLPF capacity as performance objectives provides considerable confidence against uncertainty. The HCLPF capacity can be estimated using deterministic methods and is not strongly sensitive to subjective judgment and estimates of variability parameters. Once the seismic margin is characterized by the HCLPF capacity, the estimation of the installation-level annual frequency of unacceptable performance shows limited sensitivity to the estimate of variability parameters, β_r, β_u, and β_c, whose estimated values are typically set to be conservative biased. Accordingly, determining the adequate margin expressed by HCLPF capacity to achieve a target mean annual frequency was found to have relatively limited sensitivity to the assumptions and judgment that influence the characterization of uncertainty (Annex II).

6. ADEQUACY OF DESIGN ROBUSTNESS FOR OTHER HAZARDS

The approach described in Section 5 for the adequacy assessment of seismic margins may be generalized to other external hazards. A generalization of this methodology is presented in Section 6.1. Section 6.2 provides hazard specific recommendations. Section 6.3 briefly presents considerations for applying this methodology to new and existing nuclear installations.

6.1. GENERAL METHODOLOGY

This section provides the general methodology for assessing adequacy of design robustness. It is one of the key sections of the present publication. The methodology makes a distinction between different classes of external hazards, and it focusses on those for which performance objectives can be established in terms of maximum AFE. Requisites for assessment of external hazards and installation-level capacities are given. From the results of the assessments of hazard and capacity, performance of the installation can be derived and compared with performance objectives.

6.1.1. Classification of external hazards

For assessing adequacy of design robustness, this publication makes a distinction between three categories of external hazards:

A. Hazards whose severity can be defined using a single parameter (e.g. ground acceleration, wind speed, water level), for which an AFE can be assessed following well established practices.

   This is the case of many natural hazards, for which the standard practices are able to define a 'hazard curve' which gives the AFE as a continuous function of the parameter defining the severity of the hazard, with due consideration to uncertainties (see SSG-18 [28] and SSG-9 (Rev. 1) [34]).

B. Hazards which are scenario based, and where the AFE of a given scenario can be estimated using well established practices.

   In scenario based hazards, severity of an event cannot be associated with a single parameter, since severity depends on the combination of several parameters which cannot be easily correlated with each other. This is the case of accidents in transportation routes, for which the severity depends on distance, amount of transported hazardous substance, nature of the substance, etc. In this kind of accidents, distances and statistics about traffic can be used to associate AFEs to a set of predefined scenarios with increasing levels of severity [23].

C. Hazards which are scenario based and whose realizations (events) are introduced in an agnostic way in the design process, that is, there is no annual frequency explicitly or implicitly associated to them.

   These hazards are usually introduced to cover postulated human induced external events. That is, they are specified to the designer irrespective of any probability of occurrence, as if they were sure events, together with a set of acceptability conditions for the behaviour of the plant in case those events happen.

The present publication addresses the adequacy of resulting design margins only for external hazards within categories A and B, that is, for external hazards whose severity can be linked to a frequency of occurrence. In these cases, an estimate of the overall frequency of failure due to the external hazard can be derived from the design margin and compared with the performance goal against the hazard considered acceptable for the installation. The process is explained in detail in the following Sections 6.1.2 to 6.1.6.

For external hazards in Category A, with hazard severity and installation capacity against the hazard defined as a function of the same parameter, overall performance (annual frequency of failure) due to the external hazard can be obtained by means of a convolution integral [7]. This is a standard practice.

For hazards in Category B, considering a range of possible discrete scenarios (e.g. several possible accidental explosions: type of truck or railroad wagon, mass of explosive material, type of accident, and distances), with an increasing level of severity, the design margin over the design scenario is given by the most severe scenario that can be sustained without (reasonably) losing the intended safety functions at plant level. For each of these scenarios, an estimate of the probability of failure (i.e. losing the safety functions) can be obtained, which, if convolved with the annual frequency of the different possible scenarios, would give a performance (annual frequency of failure) to be compared with a performance goal for acceptability. In contrast with hazards in Category A, convolution integral is now discrete (i.e. sum over possible discrete scenarios). The required design margin could be adjusted to meet the performance goal.

For external hazards in Category C, it is necessary to assume that the events to be considered in the design process have been specified as maximum credible events and the design needs to meet certain conditions in case of those events happening. Such conditions are expressed by engineering attributes such as ‘no penetration of containment wall’, or ‘one safety train remains functional’, so that it can be demonstrated with adequate confidence that a severe accident and/or large release are avoided if the conditions are met. For external hazards in Category C, acceptable behaviour (compliance with specified conditions) is used for assessing design robustness adequacy.

Table 6 provides examples of hazards in each of these categories. For each category, approaches to determine design margin, or to demonstrate compliance with specified conditions, are similar. In the Table, main ‘design provisions’ intended for achieving an appropriate performance are mentioned for each hazard. Generally, demonstration of the appropriate performance of the installation against a specific hazard is done using safety assessment methods.

TABLE 6. EXAMPLE HAZARDS IN EACH CATEGORY

Hazard	Category	Hazard Severity Parameter(s)	Annual Frequency of Design Events (yr^{-1})	Challenges	Challenging Mechanisms	Performance Targets	Design Provisions	Ref.
Seismic motion	A	Spectral acceleration	10^{-4} to 10^{-5}	All SSCs, including redundant trains	Induced acceleration and relative displacement	No damage up to design basis earthquake (SL-2) Maintain safety functions and reparable damage for margin capacity	Qualification by test and/or analysis for design basis earthquake. Margin assessment for the resulting design	IAEA SSG-67 IAEA SSG-89
Accidental explosion	B	Scenario-based (Nature and mass of explosive material, distance, type of accident, intermediate obstacles)	10^{-4} to 10^{-5}	SSCs located in exterior areas + building structures	Pressure waves and secondary missiles	Maintain safety functions and minor damage for design basis event. Maintain safety functions and limited reparable damage for beyond design basis external event.	Design of exposed SSCs and protective structures to maintain structural integrity for the design basis event. Protect exposed SSCs if distance between redundant trains is not sufficient.	IAEA SSG-68
Aircraft crash	C	Scenario-based (Mass and speed at impact, aircraft dimensions, attitude at impact, amount of fuel)	N/A	SSCs located in exterior areas + building structures. Induced vibration may affect SSCs within impacted structures. Fuel fire may affect SSCs not directly impacted by the aircraft.	Direct impact, induced vibration and fuel fire	Prevent breach of containment. Prevent initiation of a severe accident. Damage accepted, but one safety train maintains functionality.	Protective barriers and global structural resistance. Separation of safety trains. Avoid direct transmission paths for induced vibration	IAEA SSG-68

6.1.2. Performance objectives

As introduced in Section 5.1, performance objectives can be defined either as annual frequency based or as scenario based.

6.1.2.1. Hazards in Categories A and B

For hazards in Categories A and B, performance objectives can be readily defined as annual frequency based.

For a given external hazard, the annual frequency of a particular SSC failing to maintain the intended safety functions due to that external hazard depends both on the annual frequency of the hazard (e.g. hazard curves) and on the capacity of the SSC against the hazard (e.g. conditional probability of failure for any given level of hazard severity). The frequencies of failure of the SSCs combine with each other to yield a frequency of failure of the nuclear installation as a whole to meet the intended safety functions (see Section 6.1.4 below). The performance goal for a nuclear installation in relation to a specific external hazard is thus defined as the maximum acceptable annual frequency of failing to maintain the installation-level intended safety functions due to that external hazard.

Performance goals may be different for safety functions contributing to DiD Level 3 (control of accidents within the design basis) and for safety functions contributing to DiD Level 4 (control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents).

Performance goals vary from one Member State to the other. Typical performance goals for new NPPs are 10^{-5} yr^{-1} for external event induced CDF (a surrogate for DiD Level 3 performance), and 10^{-6} yr^{-1} for external event induced large early release frequency (LERF, a surrogate for DiD Level 4 performance)[20].

6.1.2.2. Hazards in Category C

In contrast, for hazards in Category C, performance objectives can only be defined as scenario based objectives. A scenario based performance objective normally requires that the installation design demonstrates the ability to maintain its required safety and mitigation functions with acceptable confidence when it goes through the given scenario. Design robustness is adequate if this is the case.

6.1.3. Hazard assessment prerequisites

For hazards in categories A and B, computation of annual frequencies of failure requires the external hazard to be assessed. The severity of the realizations of the hazard (events) needs to be linked to an annual frequency of occurrence (e.g. hazard curves). A broad overview of hazard assessment techniques for the most common external hazards is provided in IAEA-TECDOC-1834, Assessment of Vulnerabilities of Operating Nuclear Power Plants to Extreme External Events [7].

The level of detail required for the hazard assessment depends on the particular application. In most cases, the mean hazard (curve) will be sufficient for the purposes of assessing adequacy of design margins or to define beyond design basis external events for safety assessments. Mean hazard will yield a point estimate of the performance (annual frequency of failure) of the installation, to be compared with the performance goal.

6.1.4. Installation-level capacity assessment

In general terms, capacity is expressed as a conditional probability of failure, provided that a certain level of hazard severity is attained. The term ‘fragility curve’ was coined in the seismic safety assessment field (see Section 5) but the idea can be generalized to other hazards. The fragility curve provides the conditional probability of failure as a function of the severity of the hazard.

[20] Performance goals for existing NPPs are typically one order of magnitude higher.

Techniques to obtain fragility curves are well developed in the seismic field and less developed in other fields. However, conservative assumptions can be used to address the lack of development (e.g. the use of step functions in flood fragility analyses, associated with levels of inundation).

As shown in Section 5 for the seismic hazard, there exists a number of well-established and practiced procedures that allow going from the SSC-level capacity against a hazard to the installation-level capacity.

For hazards in Category A, the concept of 'design margin' is tightly linked to the concept of 'fragility'. The metrics of the 'design margin' is commonly associated to a point in the fragility curve. For instance, 'seismic margin' is commonly defined by the seismic hazard severity corresponding to a 1% conditional probability of failure on the mean fragility curve. The selected point is somewhat arbitrary, but the idea is that it has to correspond to a severity of the hazard for which there is 'high confidence' that the probability of failure is 'low'. By the definition of a "margin", this hazard has to be larger than the severity of the design basis event.

A key point is that, in order to have a 'low' probability of failure in an SSC there are some conditions that need to be met. For instance, permanent deformations in structural components need to be under a threshold, or hydrostatic pressure on seals needs to be smaller than proof values. Those acceptability conditions are less demanding than those considered in the design against the design basis event. Establishing those conditions may not be a trivial task, since they need to result in a probability of failure consistent with the metrics selected for the 'design margin' (e.g. 1% conditional probability of failure on the mean fragility curve).

In this way, it can be said that having a particular 'design margin' is a surrogate for meeting those acceptability conditions in the SSCs, at the hazard severity corresponding to that particular design margin.

For hazards in Category B, which are scenario based hazards, the concept of fragility is the same, but it cannot be visualized as simply as in Category A hazards, since fragility is not a function of a single hazard parameter. A possible working alternative is to define a series of scenarios with increasing severity and to find the first one for which there is no longer 'high confidence' that the probability of failure is 'low' [7]. This scenario would define the 'design margin' in terms of a scenario. For instance, if the tornado hazard is considered a scenario based hazard, a series of scenarios with increasing severity could be defined by the Enhanced Fujita tornado intensity scale and the design margin could be defined based on this scale. A similar approach can be followed for accidental aircraft crashes, using aircraft categories.

Thus, for hazards in Category B, the 'design margin' could be defined by the severity scenario at which the thresholds for a 'low' probability of failure are crossed.

For hazards in Category C, where agnostic scenarios are defined, the concept of design margin is difficult to establish. However, it is not required for the purposes of this publication, since the adequacy of design robustness is assessed based on the compliance with acceptability conditions established by the regulatory body for the given scenario.

6.1.5. Assessment of performance against the hazard and adequacy of design margins

For Category A hazards, frequency of failure due to the hazard can be obtained by convolution of the hazard and the installation-level fragility.

Given a mean hazard curve *H(a)* and a mean installation-level fragility curve *F(a)*, then a point estimate of the mean frequency of failure λ_f is given by either of the following two analytically equivalent equations (convolution integrals) [7]:

$$\lambda_f = -\int_0^{+\infty} F(a)\,\frac{dH(a)}{da}\,da$$

$$\lambda_f = \int_0^{+\infty} H(a)\,\frac{dF(a)}{da}\,da \qquad (11)$$

where *H(a)* is the mean hazard exceedance frequency corresponding to hazard severity parameter *a*. As described in the previous sections, installation-level fragility *F(a)*, is closely related to the design margin of the nuclear installation and it can be approximately obtained from that margin [7].

Estimated frequency of failure is to be compared with the applicable performance goal. If the frequency of failure is larger than the performance goal, then the design margin is not adequate.

If the purpose were to define a beyond design basis external event for consideration in the design process, then, in the equations above, frequency of failure λ_f would be made equal to the performance goal. The installation-level fragility *F(a)* would be introduced as a function of the severity of the beyond design basis external event. The required severity would then be determined with the condition that the integral yields the required performance goal.

For Category B hazards, the ideas are the same, but convolution of hazard and fragility cannot be performed in such an elegant, continuous way. Convolution is instead performed using a discrete sum of products of occurrence frequencies and conditional failure probabilities, corresponding to the scenarios defined for each hazard. To make sure that the frequency of failure is not underestimated, an important point is that the considered scenarios need to cover all the range of severities relevant to the installation safety assessment and that each scenario needs to be independent of the others (i.e. mutually exclusive and collectively exhaustive).

As pointed out above, performance goals may be different for DiD Level 3 and DiD Level 4. Likewise, installation-level fragility may be different for intended functions in DiD Level 3 and DiD Level 4.

For hazards in Category C, there is no hazard definition in annual frequency terms. As mentioned above, compliance with scenario based acceptability conditions is used for assessing design robustness adequacy.

6.1.6. Dealing with uncertainties

The general methodology described in the paragraphs above provides a framework to fully consider the uncertainties, both in the hazard and the capacity against the hazard.

In the most general case, hazard is defined by a family of hazard curves, each one corresponding to a percentile in a probability distribution, and capacity against the hazard is defined by a family of fragility curves, each one corresponding to a level of confidence. A probability distribution of the annual frequency of failure due to the hazard can be obtained by the convolution of these two families of curves.

In practice, however, the difficulty is in the correct estimation of all involved uncertainties. In many cases, for assessment of adequacy of design margins, it may be acceptable to work only with mean values of hazards and fragilities, to compute a best estimate of the mean annual frequency.

6.2. EXTERNAL HAZARDS OTHER THAN EARTHQUAKES

The following external hazards have been selected to illustrate the general methodology presented in Section 6.1 because they are known from experience to be potentially significant hazards to the safety of nuclear installations. The selection is below, and various aspects are given in Tables 7 and 8:

- Meteorological hazards:
  - Extreme air temperature
  - Extreme UHS (e.g. seawater) temperature
  - Extreme wind
  - Extreme humidity in case of cooling towers
- External flooding hazards:
  - Coastal (sea, lakes) flooding
  - Riverine flooding
  - Local intense precipitation
- Human induced hazards:
  - Aircraft crash
  - External explosion

Each external hazard has its own metric(s) for design margins. For a given design, these can be calculated and used to derive an installation-level design margin, as introduced in Section 6.1. The following Sections 6.2.1 to 6.2.3 describe the features and common plant issues relevant to defining these metrics and margins for each selected hazard.

The design margins metrics developed below of individual hazards are formulated as excess capacity or capability over the design basis up to a threshold value; this threshold value indicates the degree of beyond design basis capability. The preferred approach in this publication is to use these design margins in a similar way to that used in the seismic hazard case and develop a 'low probability of failure' capacity from a probabilistic or semi-probabilistic analysis [7]. This is possible, at least in principle if underlying data allows, for Category A hazards, and it is considered to be a challenge for scenario based hazards, as mentioned in Section 6.1.

It is a matter of discussion and ongoing research as to how to define the threshold values of 'low probability of failure' for each external hazard. While the seismic hazard case has seen much research and development and is considered relatively mature, this is not so for other hazards. Thus, criteria for defining threshold values for other hazards are somewhat arbitrary with the current state of practice and judgement is needed to establish the overriding condition that, for the threshold value, a 'small likelihood' of failure exists. Such criteria need ideally to be explicitly stated in probabilistic terms, since this is required for the estimation of the installation-level fragility used to assess compliance with performance goals (see Section 6.1). If this is not possible, then an understanding of failure potential is still needed to support a qualitative assessment of compliance with performance goals.

TABLE 7. SELECTED EXTERNAL HAZARDS, DESIGN ROBUSTNESS METRICS AND POTENTIAL ACCIDENT INITIATING CONDITIONS

Hazard	Category[1]	Hazard Parameter[2]	Hazard Parameter Range[3]	Design Margin Metric[4]	Design Event[5]
High and/or low ambient air temperature	A	Ambient temperature T[6]	Limited by physical process	$\Delta T = T_{TV}\text{-}T_{DB}$	Design Basis Event & Beyond Design Basis Event
UHS seawater temperature	A	Intake temperature T	Limited by physical process	$\Delta T = T_{TV}\text{-}T_{DB}$	Same as above
Extreme wind	A	Ambient wind speed V_W	Limited by physical process	$\Delta V_W = V_{W\,TV} - V_{W\,DB}$	Same as above
Coastal flooding	A	Still water level + 0.5 × wave height H_W	Limited by physical process	$\Delta H_W = H_{W\,TV} - H_{W\,DB}$	Same as above
Riverine flooding	A	River level H_R	Limited/accentuated by physical process and/or topography	$\Delta H_R = H_{R\,TV}\text{-}H_{R\,DB}$	Same as above
Local intense precipitation	A	Precipitation per unit time I_{DB}, and duration t_{DB}	Limited by physical process	$\Delta I = I_{TV} - I_{DB}$	Same as above
Aircraft crash	B or C	Derived from scenario	Scenario based	Scenario based	Same as above
Off-site explosion[7]	B	Derived from scenario	Scenario based	Scenario based	Scenario based

Notes related to Table 7:

(1) *Type of hazard* – See classification in Section 6.1.

(2) *Hazard parameter* – A measure of the severity of the hazard that can be related to potential damage effects on the nuclear installation.

(3) *Hazard parameter range* – Intended to give a qualitative indication of the range of values realistically available to the hazard parameter. Most natural hazards are represented by parameters whose values are limited by a physical process. For example, sea water freezes at about -1.8°C and, therefore, flowing seawater is limited to this low temperature. At this point, solid material (frazil or pack ice) starts to form and the ability of seawater to act as a heat transfer medium becomes increasingly impaired, but its temperature does not change. Many meteorological hazard parameters have physical limits to their value range, indicating that values outside this range are not credible under any reasonably foreseeable circumstances.

(4) *Design margin metric* – A hazard related parameter selected to quantitatively measure design robustness. Generally, these metrics are hazard parameter margins that quantify the delta above a design basis value, and the margin as the difference between a threshold value (TV), for which failure is considered relatively unlikely, and design basis values.

(5) *Design event definition* – The design event or accident initiating event is defined either in terms of a hazard parameter, or in terms of other parameters that are based on an assumed accident scenario. Typically, for natural hazards defined by a hazard curve, the design events are defined in terms of a hazard parameter values. For a properly formulated hazard curve, the value of the hazard parameter at a given frequency is a lower bounded exceedance value. So, for high ambient air temperature, T_H, the design basis value, actually represents the lower bounded range $T_{HDB} \rightarrow$ some physical maximum value. For human induced hazards, accident initiating events are generally defined in terms of accident scenarios, where each scenario is defined by one of more hazard parameters appropriate to the particular site and hazard in question.

(6) Design metrics for heating, ventilation and air conditioning (HVAC) systems may be more complex than a single parameter (see Section 6.2.1.1).

(7) For human induced external explosion hazard, two approaches are possible. Either a maximum credible event can be selected based on, say, maximum inventory of explosive materials, or a range of explosive events representing different severity events, each with a different frequency can be selected.

TABLE 8. SELECTED EXTERNAL HAZARDS. PROTECTION/MITIGATION AS PART OF DEFENCE IN DEPTH AND SPECIAL FEATURES TO BE CONSIDERED

Hazard	Defence in Depth		Special Features		
	Level 3[1]	Level 4[2]	Common Cause Failures[3]	Uncertainty[4]	Severe Accident[5]
High ambient air temperature	– Design of cooling systems to T_{HDB}[6] – Confirm that design meets design robustness metric[10] – RDS[7] – T_H limit on operations[8]	– Backup cooling equipment – Severe accident release mitigation systems	Y	High	N
UHS high temperature (e.g. seawater)	– Design of cooling systems to T_{HDB} – Confirm that design meets design robustness metric – T_H limit on operations[8]	– Backup cooling equipment	L	High	N
Extreme wind	– Design of weather envelopes to V_{WDB} – Confirm that design meets design robustness metric – RDS[7] – V_w limit on operations	– Backup equipment – Severe accident release mitigation systems	Y	High	Y
Coastal flooding	– Design of site platform to H_{WDB} (dry site) – Confirm that platform meets design robustness metric – RDS[7] – H_w limit on operations[8]	– Backup equipment – BDB flood protection measures – Severe accident release mitigation systems	Y	High	Y
Riverine flooding	– Design of site platform to H_{RDB} (dry site) – Confirm that platform meets design robustness metric – RDS[7] – H_R limit on operations[8]	– Backup equipment – BDB flood protection measures – Severe accident release mitigation systems	Y	High	Y
Local intense precipitation	– Design of drainage systems for I_{DB} and t_{DB}	– BDB flood protection measures – Layout/features that prevent water accumulation in roofs	Y	High	Y
Accidental aircraft crash	– Design of protection of structures/SSCs to resist scenario – Confirm structures/SSCs meet design robustness metric – RDS[7]	Scenario based	M	Low	Y/N[9]
Off-site explosion	– Design of protection of structures/SSCs to resist scenario – Confirm structures/SSCs meet design robustness metric	Scenario based	M	Low	N

Notes to Table 8:

(1) *DiD Level 3* – Examples of how DiD Level 3 (design basis accident control) can be implemented for the given external hazard.
(2) *DiD Level 4* – Examples of how DiD Level 4 (severe accident mitigation) can be implemented for the given external hazard.
(3) *Common cause failures* – The potential of the external hazard to create CCFs or multiple design events in the nuclear installation. A qualitative measure is used – High/Medium/Low – to indicate the likelihood that the hazard will generate multiple design events and therefore will present multiple ways to fail the plant simultaneously and undermine the concept of design robustness.
(4) *External hazard uncertainty* – Uncertainty in the underlying data used to assess the external hazard and derive hazard parameter metric values. A qualitative measure of uncertainty is used here – High/Medium/Low – to indicate the level of uncertainty and to indicate, in a qualitative sense, how reliable the metric is as a measure of design robustness.
(5) *Severe accident* – The potential that the external hazard has to cause a severe accident. This is not the probability of the hazard event to cause a severe accident but a qualitative measure of whether a severe accident is credible from the hazard or not. A qualitative measure is used – Y/N –.
(6) Design metrics for HVAC systems may be more complex than a single parameter (see Section 6.2.1.1).
(7) RDS – Redundancy, diversity, and segregation of plant systems.
(8) Meteorological and water level hazard parameters are generally forecastable with sufficient accuracy to enable operational precautions to be taken in advance of a hazard event occurring, such as shutdown and provision of additional temporary flood barriers. Therefore, operational procedures are an important part of managing the risk from these hazards. This is different from seismic hazard, which is not predictable with an accuracy that allows procedural risk mitigation.
(9) Aircraft crash events may progress to severe accident if the events are considered as a Category C hazard, since these are defined as beyond design basis external events subject to DiD Level 4 requirements. Category B events are considered as a design basis event and designed for according to DiD Level 3 requirements.
(10) SSR-2/1 (Rev. 1) [2] requires verification that design robustness against a design external event (design margin) is adequate. This is done at the design stage.

6.2.1. Meteorological hazards

Meteorological hazards can generally be classified as Category A hazards (see Section 6.1), with the exception perhaps of rare meteorological events such as volcanic ash clouds[21], which could be Category B or C.

6.2.1.1. Extreme air temperature

General considerations

Extremes of ambient outside air temperature can adversely affect SSCs. Temperature is a meteorological hazard whose daily and seasonal variation is common, and designers are familiar with developing design solutions to mitigate or eliminate the normal operation effects of extremes in temperature.

Hazard features affecting ability to implement robust designs are as follows:

- Temperature is not a force or stress related ‘load function’ onto SSCs, so cannot be protected simply by a strong external envelope. Unless widespread thermal insulation and HVAC systems are provided, extreme external temperatures will eventually affect all plant areas, although the rate at which this phenomena occurs will depend on the thermal inertia of building materials. SSCs internal to buildings will therefore be afforded some protection depending on the design of the enclosing buildings.
- *CCF potential*: This hazard will affect the entire site simultaneously and off-site regions as well.

[21] The Eyjafjallajökull volcanic eruption on 14 April 2010 caused a large ash cloud to spread across western Europe and presented a potential hazard to SSCs with air intakes such as backup diesel and gas turbine generators.

- *Uncertainty*: Temperature is easy to measure instrumentally but design values depend on the ability to predict future extremes at a given site.
  - Extreme temperature can be predicted statistically from available (normally) instrumental weather data, but data sets, even in developed Member States, are often limited to about 50 years duration. Therefore, the degree of statistical extrapolation required to predict 10^{-4}/yr and lower values is high and possibly excessive for the traditional 'extreme value' statistical methods used. This leads to a large uncertainty in low frequency predictions, increasingly so as frequencies are pushed lower, say to 10^{-7}/yr hazard screening levels. Alternatively, stochastic weather generators can be used, but a large number of years of actual records is still needed for calibration of such models for low annual frequency extreme weather predictions. Data from similar parts of the world can be used to artificially extend observation times, but similarity needs to be demonstrated.
  - It is likely that temperature is a hazard whose severity, both high and low, is limited for physical reasons such that values beyond these limits can be considered incredible.
- *Severe accident potential*: It is not anticipated that temperature hazard, by itself, is likely to lead to severe accidents, because the weather systems that create the conditions for extremes of temperature are forecastable and nuclear activities can be shut down or additional protection measures implemented before the extreme event occurs at the site, although this would require suitable operating instructions to be implemented at the site.
- *Correlation with other external hazards*: Extremes of temperature are positively correlated with other meteorological parameters such as high or low levels of solar radiation (sunshine) and negatively correlated with others, such as wind speed and precipitation. Temperature is likely to be positively correlated with UHS (sea and river) temperatures or drought.

Hazard category

Extreme air temperatures will normally be considered a hazard in the Hazard Category A, since the severity of the hazard can be defined using a single parameter, the dry bulb temperature (T_A), for which AFEs can be assessed following established practices.

For HVAC systems, the formulation of design metrics has to measure the efficiency of such systems, which is affected by both ambient air temperature and humidity. Efficiency in this case is best expressed as a two-dimensional metric, rather than the one-dimensional temperature metric discussed above. Hence, for HVAC applications, the hazard could be classified as Hazard Category B. SSG-68 [15] identifies a number of related parameters that can form a suitable design metrics, including:

- Ambient dry bulb temperature (T_A);
- Ambient wet bulb temperature;
- Ambient humidity;
- Dew point temperature;
- Ambient enthalpy.

These parameters collectively express the temperature of the ambient air and its moisture content. Ambient dry bulb temperature (T_A) is used in combination with one or more of the other parameters to calculate the rate at which heat can be absorbed or released by the air processed by an HVAC system. Turning these parameters into a useful design metric for HVAC systems is a specialist area and beyond the scope of this publication; however, it is assumed here that these more complex HVAC design metrics can still be expressed in terms of a design basis and a threshold function of the metric, thus allowing the same principles of design robustness to be employed.

Hazard assessment prerequisites

Application of the general framework defined in Section 6.1 requires the assessment of the hazard in terms of hazard curves, effectively linking the severity of the hazard to an annual frequency of exceedance.

SSG-18 [28] provides general guidance on how to assess the hazard of extreme temperatures. In a general case, para. 4.11 of SSG-18 [28] states:

"The results of a hazard assessment for extreme air temperatures include identifying maximum dry bulb temperatures and coincident wet bulb temperatures, maximum non-coincident wet bulb temperatures and minimum dry bulb temperatures. The appropriate extreme temperatures should be characterized by the annual frequency of exceedance of given thresholds with an associated confidence interval. The persistence of very high or very low temperatures may also be a factor that needs to be considered".

For example, 1.0% and 2.0% values, that are exceeded on average for 88 and 175 hours per year, respectively, are typical design conditions.

Procedures to assess the hazard are based on extrapolation to larger return periods of climate models developed from recorded data. Typically, statistical theory of extreme values is used based on the available data, and uncertainties are introduced corresponding both to the reliability of the records and to the statistical fitting and extrapolation.

Design margin metrics

Temperature is defined in terms of both design basis and a threshold value for which there is a small likelihood that the facility loses its intended safety functions. It is straightforward to define a design margin metric as:

$$\Delta T_A = T_{ATV} - T_{ADB} \tag{12}$$

where ΔT_A is the design margin.

It is a matter of discussion how to define the threshold capacity value T_{ATV}, which could be assimilated to the HCLPF concept used in seismic safety assessments (see Section 5). The criteria for defining the threshold capacity value will normally be based on judgement, being the only condition that for the threshold value there exist a 'small likelihood' of failure. The criteria need to be explicitly stated in probabilistic terms, since this is required for the estimation of the installation-level fragility used to assess compliance with performance goals (see Section 6.1).

Assessment of installation-level design margin

Section 4 of IAEA-TECDOC-1834 [7] describes a general methodology which can be used to assess installation-level capacity against external hazards. Deterministic and semi-probabilistic procedures are given, which can be used to estimate the installation-level design margin ΔT_A against extreme air temperatures. Deterministic procedures are based on the 'success path' concept, whereas semi-probabilistic procedures use event tree and/or fault tree models to represent the plant behaviour during extreme temperature events.

Irrespective of the selected procedure, temperature capacity of temperature sensitive SSCs will need to be determined, based on design information and technical specifications. Finding the temperature demand on the SSCs, for a given set of outer environment parameters, may require simulation of heat transfer and ventilation conditions.

Potential failure modes to consider may include freezing in piping and/or tubing (flow reduction), malfunction of instruments, overloading of HVAC systems, or absence of required cooling in control rooms, electrical and/or battery rooms.

As a result, following the general principles given in Section 6.1.5, an estimate of the installation-level temperature design margin and the corresponding 'fragility curve' will be obtained.

Assessment of installation performance

Using the mean hazard curve and the estimate of the fragility curve, Eq. (11) will provide the installation-level performance, which is to be compared with the applicable performance goals. The design margins will be acceptable if the performance goals are met.

Common problems in nuclear plants

Nuclear installations are generally robust to atmospheric temperature variations, but certain types of SSC and the ability of operators to perform safety related tasks can be hindered by extreme high or low temperatures. The following aspects are considered typical for nuclear sites:

- Inability to maintain environmental conditions for functionality of SSCs:
  - Applies for example, to rooms and compartments with heat generating SSCs that require active cooling during periods of high ambient temperature;
  - Poor habitability for operators.
- SSCs that require protection from extreme cold:
  - Water containing systems sensitive to freezing temperature levels. Typically, this includes external water containing pipework, valves and similar;
  - Freeze–thaw cycles on exposed concrete surfaces containing cracks and cavities;
  - SSCs, such as cranes, with exposed metal components subject to brittle failure in very cold conditions.

Loss of off-site power can occur in cold weather if power lines become coated in ice, but this event is covered as a specific accident sequence for other reasons, so is not considered further here.

Additional off-site issues with extreme air temperatures are that the hazard is likely to affect a large region around the site and, consequently, could impact directly on the ability to implement emergency arrangements.

Common design solutions

Design solutions depend on the specific SSCs sensitive to temperature and the nature and location of operator safety related tasks that may be required during periods of extreme temperature.

The following aspects are considered to be representative of a typical NPP site:

- Passive features:
  - Thermal insulation can be applied and consists of various materials with very low thermal conductivity. The design and use of these materials is considered industry standard practice and their maintenance is a housekeeping issue.
  - Thermal inertia of building envelopes is a significant passive temperature moderation system. It depends on the high heat capacity of common building materials used on NPP sites, the most important of which is mass concrete. Major NPP buildings are massive concrete structures with very high thermal capacity. This tends to smooth out the short

term (days) variation in ambient air temperature and should slow the tendency for external air temperature extremes to penetrate internal areas and, therefore, adversely affect SSCs and environmental conditions for operators.

- Active systems:
  - HVAC systems;
  - Electrical trace heating;
  - Administrative measures;
  - Administrative control, including restricting temperature sensitive operations to within set temperature limits.

6.2.1.2. Extreme ultimate heat sink temperature

General considerations

Extremes of UHS temperature can adversely affect SSCs involved in reactor cooling. The UHS can rely on one or a combination of water bodies or, via cooling towers, it can rely on the atmosphere. In the latter case, much of the previous section applies, so here we concentrate on the more common situation where the UHS is provided by either sea or river. The nuclear process cannot protect itself from the state of the UHS because it forms an integral part of the cooling process and changes to it have a direct effect on the ability of relevant SSCs to perform their cooling function.

UHS temperature is generally highly correlated to air temperature but the correlation is complex and depends on many factors, not least of which is the large thermal inertia of water, which imposes a time lag between the onset of atmospheric temperature and any corresponding changes in sea and river temperatures. In addition, the condition of river water especially, is highly dependent on weather conditions upstream of the site, which can be quite different from those at the site itself.

Hazard features affecting the ability to implement robust designs are as follows:

- The UHS temperature cannot be protected against, since it forms an integral part of the cooling process, so it needs to be accommodated by this process.
- *CCF potential*: This hazard will not affect the entire site simultaneously, although the UHS temperature may be correlated with meteorological conditions that do.
- *Uncertainty*: Temperature is easy to measure instrumentally but depends on accurate prediction of weather systems relevant to the UHS to predict extremes at a given site.
  - Extreme water temperature can be predicted statistically from available (normally) instrumental hydrological data, but data sets, even in developed Member States, are often limited to about 50 years duration. See comments under extreme air temperature.
  - It is likely that UHS temperature is a hazard whose severity, both high and low, is limited for physical reasons such that values beyond these limits can be considered incredible[22].
- *Severe accident potential*: It is anticipated that UHS temperature hazard, by itself, is unlikely to lead to severe accidents, because the weather systems that create the conditions for extremes of temperature are forecastable and, in extreme circumstances, nuclear activities can be shut down or additional protection measures implemented before the hazard occurs at the site.
- *Correlation with other external hazards*: Extremes of the UHS temperature are positively correlated with meteorological parameters such as air temperature, and with meteorological

[22] For example, water freezes at a bulk temperature of 0°C (-1.8°C for sea water) at normal atmospheric pressure, which is the limiting low level value for this hazard, although further heat transfer from the liquid induces ice formation, which is a separate hazard.

conditions in the upstream catchment area of rivers. High UHS temperature is therefore positively correlated with drought conditions and potential for low UHS water levels in rivers and lakes. Low UHS temperature is correlated with ice formation and the potential for intake blockage.

Hazard category

Extreme UHS temperature will normally be considered a hazard in the Hazard Category A, since the severity of the hazard can be defined using a single parameter, the heat sink temperature T_{HS}, for which AFEs can be assessed following established practices.

Hazard assessment prerequisites

As for other Category A hazards, application of the general framework defined in Section 6.1 requires the assessment of the hazard in terms of hazard curves, effectively linking the severity of the hazard to an annual frequency of exceedance.

For extreme UHS temperatures, the common approach is similar to the one used for extreme air temperatures. Procedures are generally based on extrapolation to larger return periods of correlations developed from recorded data.

Design margin metrics

The UHS temperature is easily defined numerically and cast in terms of both design basis and a threshold value for which there is a small likelihood that the facility loses its intended safety functions. It is straightforward to define a design margin metric as:

$$\Delta T_{HS} = T_{HSTV} - T_{HSDB} \tag{13}$$

where ΔT_{HS} is the design margin.

It is a matter of discussion how to define the threshold capacity value T_{HSTV}, which could be assimilated to the HCLPF concept used in seismic safety assessments (see Section 5). The criteria for defining the threshold capacity value will normally be based on judgement, the only condition being that for the threshold value there exist a ‘small likelihood’ of failure. The criteria need to be explicitly stated in probabilistic terms, since this is required for the estimation of the installation-level fragility used to assess compliance with performance goals (see Section 6.1).

Assessment of installation-level design margin

As for extreme air temperatures, Section 4 of IAEA-TECDOC-1834 [7] describes a general methodology which can be used to assess installation-level capacity against extreme UHS temperatures. In this case, the analysis can be simpler, since it is typically a single safety related system which is directly linked with the UHS (e.g. the EWS system), and this system feeds a number of safety related heat exchangers. Design information and technical specifications can be used to determine the range of temperatures in the UHS within which the safety functions of the connected systems can be maintained with a ‘small likelihood’ of failure.

As a result, following the general principles given in Section 6.1.5, an estimate of the installation-level UHS temperature design margin and the corresponding ‘fragility curve’ can be obtained.

Assessment of installation performance

Using the mean hazard curve and the estimate of the fragility curve, Eq. (11) will provide the performance at installation level, which is to be compared with the applicable performance goals. The design margins will be acceptable if the performance goals are met.

Common problems in nuclear plants

Typical problems arising from high UHS temperature are as follows:

- Insufficient flow or temperature difference (delta T) in cooling system, therefore, inability to maintain sufficient reactor cooling capability.

Typical problems arising from low UHS temperature are as follows:

- Icing (frazil and pack) leading to partial or complete blockage of cooling water intakes, leading to inability to deliver sufficient cooling water.

Common design solutions

The most important risk control measure is the provision of operating instructions/technical specifications placing high and/or low UHS temperature limits on reactor operations.

6.2.1.3. Extreme wind

General considerations

Extremes of wind speed can adversely affect unprotected SSCs. Wind is a meteorological hazard whose variation is common, and designers are familiar with developing design solutions to mitigate or eliminate the normal operation effects of extremes in wind speed.

Hazard features affecting the ability to implement robust designs are as follows:

- Wind is a force or stress related 'load function' onto SSCs, so protection can be afforded simply by a strong external envelope.
- *CCF potential*: This hazard will affect the entire site simultaneously and off-site regions as well. Localized effects such as orography, neighbouring structures, obstacles, closely spaced buildings, and turbulences may result in a non-uniform effect through the site.
- *Uncertainty*: Wind speed is easy to measure instrumentally but prediction of future extremes at a given site can be difficult.
  - Extreme wind speed can be predicted statistically from available (normally) instrumental weather data, but data sets, even in developed Member States, are often limited to about 50 years duration. Therefore, the degree of statistical extrapolation required to predict 10^{-4}/yr and lower recurrence values is high and possibly excessive for the traditional 'extreme value' statistical methods used. This leads to large uncertainty in low frequency predictions, increasingly so as frequencies are pushed lower, such as 10^{-7}/yr hazard screening levels.
- *Severe accident potential*: It is anticipated that wind hazard could lead to severe accidents, because the weather systems that create the conditions for extremes of wind imply a strong correlation with other hazards, particularly flood related hazards. Such weather events are forecastable, and such forecasts can inform operator actions to mitigate the effects of wind before the hazard occurs at the site.
- *Correlation with other external hazards*: Extreme wind is positively correlated with other meteorological parameters such precipitation and lightning. Wind is also positively correlated

with high water levels because of the effects of low pressure surge and wind driven waves. Therefore, the wind hazard is positively correlated with coastal flooding.

- Extreme wind can create consequential missile hazards.

Hazard category

Extreme winds will normally be considered a hazard in the Hazard Category A, since the severity of the hazard can be defined using a single parameter, the wind speed V_w, for which AFEs can be assessed following established practices.

Hazard assessment prerequisites

As in the previous cases, application of the general framework defined in Section 6.1 requires the assessment of the hazard in terms of hazard curves, effectively linking the severity of the hazard to an annual frequency of exceedance.

SSG-18 [28] provides general guidance on assessing the high winds hazard. The publication covers strong 'straight' winds, tropical cyclones (typhoons and hurricanes), and tornadoes. Available methods are based either on extrapolation to larger return periods of extra-tropical cyclone and climate models developed from recorded data, or on phenomenological models of tornadoes and hurricanes.

The output of the wind hazard analysis is the hazard curves for wind speed (median, mean and fractiles) in open terrain and at a specified height.

High winds associated with any meteorological event can cause debris to become wind-borne missiles. Debris can be transported in any high wind event.

Design margin metrics

Wind hazard is usually characterized by long term wind speed and additionally by short term gust speed and gust duration (a few seconds). Wind speed is easily defined numerically and cast in terms of both design basis and a threshold value for which there is a small likelihood that the facility loses its intended safety functions. It is straightforward to define a design margin metric as:

$$\Delta V_W = V_{WTV} - V_{WDB} \tag{14}$$

where ΔV_W is the design margin.

As with temperatures, it is a matter of discussion how to define the threshold capacity value V_{WTV}, which could be assimilated to the HCLPF concept used in seismic safety assessments (see Section 5).

Assessment of installation-level design margin

Advice is provided in IAEA-TECDOC-1834 [7] on how to assess the design margin. Extreme winds PSA is performed in some Member States.

IAEA-TECDOC-1834 [7] recommends deriving HCLPF capacities for SSCs using an adaptation of the conservative deterministic failure margin (CDFM) method developed for seismic margin assessments. The HCLPF capacity would then be associated with V_{WTV}. This can be combined with the design basis wind speed to compute the margin, ΔV_{W}.

As noted above, wind related hazards include both the direct application of aerodynamic forces and pressure drops to exposed structural surfaces and the impact effects of airborne missiles. The metric defined above applies directly to aerodynamic forces (proportional to V_{W}^2) but only indirectly to missile impact effects, because one-to-one relationships between wind speed and the size and mass of objects

that may become missiles in extreme wind conditions are not commonly available. Often, engineers make assumptions regarding the type of object that can become a missile in terms of its mass and size and the nature of the impact process (see Refs [41] and [42]). Armed with these assumptions it is then possible to use a metric of the form above. See IAEA-TECDOC-1834 [7], Section 5.2.3.3, for more details.

Assessment of installation performance

As in the previous cases, using the mean hazard curve and the estimate of the installation-level fragility curve, Eq. (11) will provide the installation-level performance, which is to be compared with the applicable performance goals. The design margins will be acceptable if the performance goals are met.

Common problems in nuclear plants

Extreme winds have the potential for over-stressing even well-designed building elements that are exposed to the hazard.

Typical problems arising from extreme winds are as follows:

- Potential for damage arising directly from overstressing of building exposed surfaces, or indirectly through the action of missiles and missile impact;
- Loss of off-site power;
- Poor working environment for operators.

An additional off-site issue with extreme wind is that the hazard is likely to affect a large region around the site and, consequently, could have impacts on communications and on the ability to implement emergency arrangements.

Common design solutions

To address these problems, designers make provision for strong external building envelopes and minimize the potential for missiles on the site such as loose objects and poorly connected cladding panels. In addition, there normally exist administrative controls placing wind speed limits on machinery and human operations.

6.2.2. External flooding hazards

External flood hazards can be classified as Category A hazards when they occur as the result of natural processes, but river flooding can also occur as a result of human induced hazards (e.g. a dam break), in which case designation as Category C is generally most appropriate (see Section 6.1).

6.2.2.1. Coastal flooding

General considerations

Coastal flooding caused by extreme water level can adversely affect unprotected SSCs. Water level is subject to several causal mechanisms, including gravitational tide, atmospheric pressure changes (low and high), wind driven waves, swell waves and long period waves (tsunamis and seiches). Designers are familiar with developing design solutions to mitigate or eliminate the effects of water level during normal operation to prevent or limit flooding.

Hazard features affecting the ability to implement robust designs are as follows:

- Water level is not a force or stress related ‘load function’ onto SSCs, so protection cannot be provided simply by a strong external envelope. The approach generally taken is to raise the

entire site above a designated water level or provide barriers external to the site high enough to withstand this water level or utilize a mixture of both approaches. However, although water level is not itself a force parameter, the movement of sea water by tide and wave creates very large forces that are absorbed by the coastline and any protective barriers.

- *CCF potential*: This hazard has the potential to affect the entire site simultaneously and off-site regions as well.
- *Uncertainty*: The main contributions to water level are tide and the interaction of tidal movement with local bathymetry, and wind driven waves.
  - Tidal controls are well understood and largely predictable for regions with established marine industries, where water level records can be up to 100 years long. For this reason, the tidal contribution to water level can usually be calculated with little uncertainty and is often considered to be deterministic.
  - However, wind driven waves are a consequential hazard of meteorological conditions, in particular low pressure storm cells. Wave height is therefore subject to the large uncertainties associated with wind.
- *Severe accident potential*: It is anticipated that sea flooding hazard could lead to severe accidents. The effect of water inundation on SSC electrical systems and the large forces associated with flowing water can overwhelm structures not specifically designed to resist them.
- *Correlation with other external hazards*: Extremes of water level are positively correlated with meteorological parameters such as wind, precipitation, and lightning. Extreme water levels could also induce flooding of nearby hazardous facilities or increase the likelihood of ship collision. In addition, extremes of water level could lead to a massive accumulation of debris in front of the cooling water intake.

Hazard category

Coastal flooding will normally be considered a hazard in the Hazard Category A, since the severity of the hazard can be defined using a single parameter, the water level H_{SW}, for which AFEs can be assessed following established practices.

Hazard assessment prerequisites

As with other Category A hazards, application of the general framework defined in Section 6.1 to coastal floods requires the assessment of the hazard in terms of hazard curves, effectively linking the severity of the hazard to an annual frequency of exceedance.

SSG-18 [28] provides general guidance on how to derive the frequencies of inundation from hydrological causes, such as runoff resulting from precipitation or snow melt, high tide, storm surge, tsunami, or wind waves. The external flood hazard analysis involves the evaluation of the annual exceedance probability of different external flood severities based on a site specific probabilistic model reflecting recent available data and site specific information.

The desirable output of the hazard assessment includes the hazard curves for flood level (median, mean and quantiles). Tsunami hazard is usually assessed separately, even though the hazard severity parameter is the same.

Design margin metrics

Water level is easily defined numerically and cast in terms of both design basis and a threshold value for which there is a small likelihood that the facility loses its intended safety functions. It is straightforward to define a design margin metric as:

$$\Delta H_{SW} = H_{SWTV} - H_{SWDB} \quad (15)$$

where ΔH_{SW} is the design margin.

The water level is primarily formed from the instantaneous combination of tide, half the time averaged wave height and other effects, such as storm surge and tsunami. Tide gauges simply measure water level, which is a combination of all the effects.

Assessment of installation-level design margin

Advice is provided in IAEA-TECDOC-1834 [7] on how to assess the design margin. IAEA-TECDOC-1834 [7] recommends deriving HCLPF capacities for SSCs using an adaptation of the CDFM method developed for seismic margin assessments. The HCLPF capacity would then be associated with H_{SWTV}. This can be combined with the design basis maximum water level to compute the margin, ΔH_{SW}. HCLPF capacities can then be used to derive estimates of the flood installation-level fragility curve.

Performing an external flood PSA is an alternative which would provide more accurate results in terms of the installation-level fragility curve. This alternative could be considered a refinement when a simpler alternative does not result in an acceptable performance.

Flood hazards include both the direct effects of high water levels (inundation) and the indirect effects of hydrostatic loads, waves and even debris. The design margin metric above is only directly related to high water level hazard but is indirectly linked to these other hazards. Moreover, there are several ways to define the failure modes of SSCs to flood hazard. Submergence is the simplest to implement and is generally conservative for unprotected SSCs, but hydrostatic loading, leak rate into equipment compartments and other SSC specific failure modes can be used. See IAEA-TECDOC-1834 [7], Section 5.3.3.2, for more details.

Assessment of installation performance

As for other Category A hazards, using a mean hazard curve and the estimate of the installation-level fragility curve, Eq. (11) will provide the installation-level performance, which is to be compared with the applicable performance goals. The design margins will be acceptable if the performance goals are met.

Common problems in nuclear plants

Typical problems arising from coastal floods are as follows:

- Failure of electrical systems associated with SSCs inundated by sea water;
- Failure of structures not specifically designed to resist flood water;
- Poor working environment for operators.

In addition to the potential for breach of flood barriers by overtopping and/or failure and flooding directly onto site platform, a very extreme water level is able to cause a flood event which may change the local bathymetry and coastline and undermine the future ability of flood protection systems to operate effectively.

The flood event is likely to affect a large region around the site and have impact directly on the ability to implement emergency arrangements.

Common design solutions

The above problems are typically addressed as follows:

- Design the plant's platform in accordance with the IAEA's dry site principle (see para. 7.5 of SSG-18 [28]);
- Provide local on-site flood protection for vulnerable SSCs and buildings;
- Make provision for temporary flood defences to be implemented through administrative controls on warning of potential for flooding;
- Administrative control to limit operations and mitigate SSC damage on warning of potential for flooding.

6.2.2.2. Riverine flooding

General considerations

Flooding caused by extreme river level can adversely affect unprotected SSCs. River level is subject to several natural causal mechanisms, including the rate of upstream precipitation into the river catchment, sudden changes to upstream or downstream river (or flood plain) cross-section such as might be caused by landslides, and seasonal effects such as thawing of snowfall in the upstream catchment.

River level can also be affected by human activities on the river and by human induced hazards that derive from these activities. The most significant of these is envisaged as due to upstream dam failure which, depending on the volume of retained water relative to the size of river, could lead to a very severe but temporary increase in volume flow rate in the river downstream.

Designers are familiar with developing design solutions to mitigate or eliminate the normal operation effects of water level to prevent or limit flooding.

Hazard features affecting the ability to implement robust designs are as follows:

- River level is not a force or stress related 'load function' onto SSCs, so protection cannot be provided simply by a strong external envelope. However, although the river level is not itself a force parameter, the movement of river water creates very large forces that are absorbed by the riverbanks and any protective barriers.
- *CCF potential*: This hazard is likely to affect the entire site simultaneously and off-site regions as well, but this the extent of flooding will be very dependent on the site and regional characteristics.
- *Uncertainty*: The main contributions to river level are upstream precipitation rate and seasonal effects such as thawing of snow, and human induced hazards such as upstream dam failure.
  - Precipitation rates are subject to significant uncertainty similar to those associated with other meteorological hazards, namely short data sets requiring significant extrapolation to obtain design and beyond design basis (threshold) values, see Section 6.2.1.
  - Human induced hazards such as dam failures are difficult to predict probabilistically and, therefore, as noted in Section 4.4.3, it is unlikely that frequency of failure can be calculated and reliance on scenario based deterministic assessment will be required. There is therefore likely to be very large uncertainty in any estimate of dam (or other large water retaining structure) failure frequency.
- *Severe accident potential*: It is anticipated that river flooding hazard could lead to severe accidents, because of the effect of water inundation on SSC electrical systems and the large forces associated with flowing water can overwhelm structures not specifically designed to resist them. The cooling water intake might also be affected due to the accompanying potential debris flow with a river flooding.
- *Correlation with other external hazards*: Extremes of river level are positively correlated with meteorological parameters such as precipitation and with seasonal factors.

Hazard category

Riverine flooding will normally be considered a hazard in the Hazard Category A, since the severity of the hazard can be defined using a single parameter, the water level H_{SW}, for which AFEs can be assessed following established practices.

Hazard assessment prerequisites

As with other Category A hazards, application of the general framework defined in Section 6.1 requires the assessment of the hazard in terms of hazard curves, effectively linking the severity of the hazard to an annual frequency of exceedance.

SSG-18 [28] provides general guidance on how to derive the frequencies of inundation from hydrological causes, such as local precipitation and runoff resulting from precipitation or snow melt in the river water shed. The external flood hazard analysis involves the evaluation of the annual exceedance probability of different external flood severities based on a site specific probabilistic model reflecting recent available data and site specific information.

The desirable output of the hazard assessment includes the hazard curves for flood level (median, mean and quantiles) or, at least, a best estimate hazard curve built from statistical extrapolation of river level historical data.

Design margin metrics

River level is easily defined numerically and cast in terms of both design basis and a threshold value for which there is a small likelihood that the facility loses its intended safety functions. It is straightforward to define a design margin metric as:

$$\Delta H_{RW} = H_{RWTV} - H_{RWDB} \tag{16}$$

where ΔH_{RW} is the design margin. This is expected to apply to both naturally induced and human induced flood events.

Assessment of installation-level design margin

Advice is provided in IAEA-TECDOC-1834 [7] on how to assess the design margin. IAEA-TECDOC-1834 [7] recommends deriving HCLPF capacities for SSCs using an adaptation of the CDFM method developed for seismic margin assessments. The HCLPF capacity would then be associated with H_{RWTV}. This can be combined with the design basis maximum river level to compute the margin, $\Delta H_{RW.}$ HCLPF capacities can then be used to derive estimates of the flood installation-level fragility curve.

As with coastal flood, performing an external flood PSA is an alternative which would provide more accurate results in terms of the installation-level fragility curve. This alternative could be considered a refinement when a simpler alternative does not result in an acceptable performance.

As already noted above, flood hazards include both the direct effects of high water levels and the indirect effects of hydrostatic loads, waves and even debris. The design margin metric above is only directly related to high water level hazard but is indirectly linked to these other hazards. Moreover, there are several ways to define the failure modes of SSCs to flood hazard. Submergence is the simplest to implement and is generally conservative for unprotected SSCs, but hydrostatic loading, leak rate into equipment compartments and other SSC specific failure modes can be used. See IAEA-TECDOC-1834 [7], Section 5.3.3.2, for more details.

Assessment of installation performance

As for other Category A hazards, using a mean hazard curve and the estimate of the installation-level fragility curve, Eq. (11) will provide the installation-level performance, which is to be compared with the applicable performance goals. The design margins will be acceptable if the performance goals are met.

Common problems in nuclear plants

Typical problems arising from riverine flood are as follows:

- Failure of electrical systems associated with SSCs inundated by water;
- Failure of structures not specifically designed to resist flood water;
- Poor working environment for operators.

In addition, the flood event is likely to affect a large region around the site and impact directly on the ability to implement emergency arrangements.

Common design solutions

The above problems are typically addressed as for sea flooding, as follows:

- Design the plant's platform in accordance with the IAEA's dry site principle (see para. 7.5 of SSG-18 [28]).
- Provide local on-site flood protection for vulnerable SSCs and buildings.
- Make provision for temporary flood defences to be implemented through administrative controls on warning of potential for flooding.
- Administrative control to limit operations and mitigate SSC damage on warning of potential for flooding.

6.2.2.3. Local intense precipitation

General considerations

Episodes of local intense precipitation may induce flood in the nuclear installation, when the level of water in the site reaches the thresholds of doors or enters the buildings through seals in the penetrations. Accumulation of water can take place not only at plant grade level, but also in roofs, when the capacity of drainage systems is exceeded.

The effects on safety may be similar to those resulting from coastal or riverine floods.

Hazard features affecting the ability to implement robust designs are as follows:

- Water level is not a force or stress related 'load function' onto SSCs, so protection cannot be provided simply by a strong external envelope.
- *CCF potential*: This hazard will affect the entire site simultaneously.
- *Uncertainty*: The main contributions to water level are the precipitation rate and its duration.
  - Local precipitation rates (intensities) are subject to significant uncertainty, since they may be the result of local phenomena, not adequately captured by the records from the meteorological station networks.
- *Severe accident potential*: It is anticipated that water accumulation could lead to severe accidents, because of the effect of water inundation on SSC electrical systems and the large

forces associated with hydrostatic pressure can overwhelm structures not specifically designed to resist them.

- *Correlation with other external hazards*: Extremes of local precipitation are positively correlated with hydrological parameters such as river levels and meteorological phenomena, such as lightning.

Hazard category

Local precipitation will normally be considered a hazard in the Hazard Category A, since the severity of the hazard can be defined using a single parameter, the precipitation intensity I for a given duration, for which AFEs can be assessed following established practices.

Hazard assessment prerequisites

As with other Category A hazards, application of the general framework defined in Section 6.1 requires the assessment of the hazard in terms of hazard curves, effectively linking the severity of the hazard to an annual frequency of exceedance.

SSG-18 [28] provides general guidance on how to derive the frequencies local precipitation intensities and associated durations. The hazard analysis involves the evaluation of the annual exceedance probability of different precipitation intensity and duration severities.

The desirable output of the hazard assessment includes the hazard curves for precipitation intensity (median, mean and quantiles) or, at least, a best estimate hazard built from statistical extrapolation of historical data following the guidance of the World Meteorological Organization (WMO) [43].

Design margin metrics

For a given duration, the precipitation intensity is easily defined numerically and cast in terms of both design basis and a threshold value for which there is a small likelihood that the facility loses its intended safety functions. It is straightforward to define a design margin metric as:

$$\Delta I = I_{TV} - I_{DB} \tag{17}$$

where ΔI is the design margin.

Assessment of installation-level design margin

Assessment of installation-level design margin requires a first step, which is the conversion of a precipitation intensity and duration into maximum water levels at plant grade level and the roofs of the buildings. This step is dependent on the design of the installation drainage systems.

Once the water levels associated with each hazard severity are determined, the assessment of the design margin follows the same approaches as for coastal and riverine floods.

Assessment of installation performance

As for other Category A hazards, using a mean hazard curve and the estimate of the installation-level fragility curve, Eq. (11) will provide the installation-level performance, which is to be compared with the applicable performance goals. The design margins will be acceptable if the performance goals are met.

Common problems in nuclear plants

Typical problems arising from local flood at the site are as follows:

- Failure of electrical systems associated with SSCs inundated by water;
- Poor maintenance of rainwater drainage system;
- Poor working environment for operators.

Common design solutions

The above problems are typically addressed as follows:

- Oversizing of drainage systems;
- Waterproof seals in access doors;
- Limited parapet heights in roofs or elimination of parapet at one or more sides of the roof.

6.2.3. Human induced hazards

Human induced hazards will normally be classified as Category B or Category C external hazards, depending on the basis used for the definition of the level of severity of the design events. If the definition is based on the frequency of occurrence, then they are Category B. If the design events are defined irrespective of the frequency of occurrence, then they are Category C.

6.2.3.1. Accidental aircraft crash events

General considerations

There are two connected hazards associated with any aircraft crash: impact where the aircraft acts as a missile, especially the hard parts of the aircraft such as the engines, and fire caused by the ejection of aviation fuel when the fuel tanks rupture during the impact event. The fire event is generally assumed to be a deflagration, so that thermal effects rather than blast effects dominate.

Designers can develop design solutions to mitigate these effects, although it is expected that significant damage may be caused to non-safety critical SSCs and to the site generally from a beyond design basis external event.

Hazard features affecting ability to implement robust designs are as follows:

- Impact is a force or stress related ‘load function’ onto SSCs, so protection can be afforded simply by a strong external envelope. However, the mechanical effects of impact lead to vibrational loads internal to the structure and these can potentially affect SSCs. The thermal effects from fire are not a force or stress related ‘load function’ and can affect vulnerable SSCs.

  IAEA-TECDOC-1834 [7], Section 5.4.2, discusses the use of the “zone of influence” concept to identify SSCs that might be affected by a crash event, and also how redundancy and segregation of equipment can assist in maintaining safety functions.

- *CCF potential*: Hazards caused by aircraft crashes are generally not considered as having CCF potential in the same way that a seismic event is, but clearly if a major crash event occurred, it could cause damage to part of the site around the impact zone, even if critical safety functions were maintained.

- *Uncertainty*: The main contributors to uncertainty in the hazard definition are related to details of the source mechanism and to the way impact and deflagration events develop. Uncertainty in the hazard definition in terms of event frequency, impact velocity and fuel load are considered to be low, since these are well understood, and good data exists within Member States on past aircraft crash events. Uncertainty in structural impact response and subsequent fire progression is considered to be high since the physical processes involved with both aspects are highly non-linear.

- *Severe accident potential*: Beyond design basis aircraft crash is considered to be a potential initiator of a severe accident.
- *Correlation with other external hazards*: Aircraft crash is not correlated with other external hazards. However, weather conditions and smoke from forest fires may affect the probability of having a crash, especially for general aviation flights not using navigation aids.

Hazard category

An aircraft crash onto a nuclear site is defined by one or more event scenarios that together are considered to encompass the hazardous nature of aircraft crash events relevant to nuclear safety. The hazard can be considered either as a Category B or a Category C hazard:

- As a Category B hazard, the scenarios are derived from crash frequency data.
- As a Category C hazard, the scenarios are based purely on deterministic considerations.

Hazard assessment prerequisites

For a Category B hazard, IAEA Safety Standards Series No. SSG-79, Hazards Associated with Human Induced External Events in Site Evaluation for Nuclear Installations [23], includes guidance to assess the hazard corresponding to accidental aircraft crashes. In general, three types of accidents are considered:

(1) Crash of a general aviation aircraft, which corresponds to small aircraft, like business jets, helicopters, or sport airplanes. This kind of aircraft could fly out of established airways and without using navigation aids.

(2) Crash of an aircraft flying along an airway, making use of navigation aids. This category corresponds to most commercial aviation, using small, medium and large airplanes.

(3) Crash during a take-off or landing operations at a nearby airport.

These accident scenarios can have different annual frequencies.

When accidental aircraft crashes are considered an applicable external hazard for a particular site, the annual frequency of an aircraft crashing on the site is determined for each class of aircraft considered (small, medium and large civil and military aircraft), making use of the applicable aircraft crash statistics.

Scenarios derived from a Category C hazard are agnostic, that is, they are specified with no consideration given to annual frequencies of occurrence.

Design margin metrics

In case the hazard can be classified as Category B, in a range of possible discrete scenarios with an increasing level of severity, the design margin over the design scenario would be determined by the most severe scenario that can be sustained without losing the intended safety functions at plant level.

In case the hazard is classified as Category C, the events considered in the design process will have been specified as maximum credible events and the design needs to meet certain acceptability conditions in case of those events happening. Thus, the concept of ‘design margin’ is less meaningful in this case, since maximum credible events have already been specified for the design.

Assessment of installation-level design margin

Advice is provided in Section 5.4 of IAEA-TECDOC-1834 [7] on how to assess the installation-level capacity. More detailed guidance is given in Safety Reports Series No. 88 [5].

For a given crash scenario (aircraft type, size, angle of attack, and amount of fuel), a set of impact events needs to be defined (impact locations), to conservatively envelope all impact possibilities. Once the aircraft and its configuration has been selected, impact velocity is the key parameter to define the severity of the event. Maximum credible impact velocity depends not only on the aircraft, but on the site configuration, which may introduce limitations on flight possibilities.

Then, at each selected location of impact, SSCs that are within the zone of influence need to be identified. Some SSCs may be directly affected by the impact, while others may be affected only by secondary missiles, vibration or heat generated by a fuel fire.

While assessing capacities, failure modes derived from local and global structural effects, as well as from vibration and fire need to be considered.

To assess the installation-level capacity, installation-level performance objectives need to be defined. Compliance with those objectives define a 'fail'/'no fail' condition for each crash scenario. The level of confidence associated to this condition may depend on the severity of the crash scenario. For the less severe scenarios, close to the design basis events, the level of confidence will be high (e.g. less than 1% probability of failure). However, for the more severe scenarios, due to the highly non-linear nature of the response and the use of best estimate approaches, the level of confidence will be smaller. This is considered to be unavoidable, at the current state of practice.

Assessment of installation performance

For a Category B hazard, an estimate of the installation performance can be obtained by adding the annual frequencies of the crash scenarios leading to a 'fail' condition. Specified crashes need to cover all scenarios considered to be possible (i.e. with a significant annual frequency of occurrence).

Design margin will be acceptable if the performance goals are met.

For a Category C hazard, installation performance will be acceptable if compliance with acceptability conditions established by the regulatory body for the given scenario is demonstrated.

Common problems in nuclear plants

Typical problems arising from aircraft crash are as follows:

- Impact effects to exposed SSCs;
- Vibrational effects to SSCs not directly exposed to the impact but mechanically connected to the impact location;
- Thermal effects from fire to exposed SSCs.

Additionally, an aircraft crash event would likely render at least parts of the nuclear site untenable and possibly limited off-site areas as well, depending on the direction of aircraft approach. Such events may therefore limit the effectiveness of emergency arrangements.

Common design solutions

Typical solutions to address these problems are based on the provision of specific protection for exposed SSCs. Generally, these include one or a combination of:

- A strong envelope able to withstand the impact event without penetration, or with limited penetration;
- The use of site layout to ensure that sensitive SSCs and the buildings housing them lie in the shadow zones of other (sacrificial) buildings for likely aircraft approach directions;

- Fire barriers and fire compartmentalization to limit the zone of influence of a crash event;
- Redundancy and segregation of SSCs providing a given safety function, say core cooling, to ensure that a single crash event is highly unlikely to adversely affect all systems simultaneously.

6.2.3.2. External explosion events

General considerations

Explosions caused by transportation routes or industrial complexes external to the site can adversely affect unprotected SSCs. Explosion events (source assumed to be near the ground surface and venting into atmosphere) are characterized by blast (pressure) waves that expand outward from the source, associated thermal effects and possibly secondary missiles. The case in which an explosive cloud develops off the site and enters a safety related building through the ventilation system is not considered here.

Designers can develop design solutions to mitigate or eliminate blast effects. Industrial explosions are best considered as scenario based hazards; developing design solutions will therefore depend on specific details and factors for each example relevant to a site.

Hazard features affecting the ability to implement robust designs are as follows:

- Blast (and secondary missile impact) is a force or stress related 'load function' onto SSCs, so protection can be afforded simply by a strong external envelope. The thermal effects from explosions are not a force or stress related 'load function', so protection cannot be provided simply by a strong external envelope. However, thermal effects are generally considered to be of lesser significance than blast effects at distant explosions. If thermal effects are considered significant then special design features would be required to protect vulnerable SSCs.
- *CCF potential*: This hazard could affect the entire site simultaneously depending on the relative location and distance to the source. It could also affect off-site regions within the range of the explosion. However, explosive effects decrease quickly with distance from the source; therefore, off-site effects and their implications for the site's emergency arrangements will depend on local factors.
- *Uncertainty*: The main contributors to uncertainty in the hazard definition are related to details of the source mechanism and to the way the explosive event moves from the source to the site.
- *Severe accident potential*: Industrial explosion events can lead to severe accidents only if the attenuating distance from the source to the nuclear installation site is small. However, this is clearly dependent on local factors.
- *Correlation with other external hazards*: Explosion hazard is not considered to be strongly correlated to other external hazards, but this is subject to local factors.

Hazard category

External explosions can be classified as either Category B, if it is possible to establish a set of frequency and severity explosion scenarios, or Category C, if a representative explosion scenario is assumed and treated deterministically (see Section 6.1).

External explosion could also be considered a hazard in the Hazard Category A, since the severity of the hazard can usually be defined using a single parameter, the side-on overpressure (P_{SO}), for which AFEs could be assessed.

Hazard assessment prerequisites

SSG-79 [23] gives guidance on the assessment of the external explosion hazard.

The explosion hazard can be originated from stationary or mobile sources. Probability of occurrence of an explosion can be derived from data about the frequency of explosions in industrial facilities or on transport routes in the vicinity of the site. Normally, due to the lack of site specific data, reference has to be made to general accident statistics.

Typically, for transportation routes, frequency of explosion is derived from the length of transportation route closer than the safe distance (km), the traffic of vehicles carrying explosive materials (vehicles/year), the accident rate (accident/vehicle km) and the conditional probability that an accident leads to an explosion (explosions per accident).

For industrial facilities, when enough information is available, frequency of explosion can be obtained from the frequency of ruptures leading to breach of pressure boundary, combined with the probability of immediate ignition, late ignition, and explosion.

The final result of the explosion hazard assessment is a list of potential explosion sources, including the amount and nature of the explosive substance, the distance to the site, and the annual frequency of explosion for each source. This information is enough for dealing with the hazard as a Category B hazard. However, from these values, probabilistic analysis procedures can be used for calculating the frequency of exceeding different levels of overpressure at the installation structures from accidents in stationary or mobile sources. This would allow the hazard to be treated as a Category A hazard.

If the hazard is dealt with as a Category C hazard, explosion scenarios are specified with no consideration given to annual frequencies of occurrence.

Design margin metrics

An explosion can be defined in terms of a blast wave side-on overpressure (P_{SO}), which is dependent on the source to site distance. This overpressure is easily defined numerically and cast in terms of both design basis and a threshold value for which there is a small likelihood that the facility loses its intended safety functions. It is straightforward to define a design margin metric as:

$$\Delta P_{SO} = P_{SOTV} - P_{SODB} \tag{18}$$

where ΔP_{SO} is the design margin.

However, the hazard is more commonly classified as Category B. Following this approach, in a range of possible discrete scenarios with an increasing level of severity, the design margin over the design scenario would be determined by the most severe scenario that can be sustained without losing the intended safety functions at plant level.

In case the hazard is classified as Category C, the events considered in the design process will have been specified as maximum credible events and the design needs to meet certain acceptability conditions in case of those events happening. Thus, the concept of ‘design margin’ is less meaningful in this case, since maximum credible events have already been specified for the design.

Assessment of installation-level design margin

Off-site explosions can exhibit a variety of hazards effects on a nuclear site, including blast overpressure, missile impact and thermal effects. Different SSC failure modes will be possible for each of these hazards. Assessment of design margin will therefore be a combination of both the assumed hazard scenarios and the likely failure modes of vulnerable SSCs.

Advice is provided in IAEA-TECDOC-1834 [7] on how to assess the design margin. Following these recommendations, it will be possible to estimate a HCLPF-like capacity of both vulnerable SSCs, and at installation level.

As for the aircraft crashes, to assess the installation-level capacity, installation-level performance objectives need to be defined. Compliance with those objectives define a 'fail'/'no fail' condition for each blast scenario. In a simplified approach, the HCLPF-like capacity can be used as the threshold value for each scenario.

Assessment of installation performance

For a Category B hazard, an estimate of the installation performance can be obtained by adding the annual frequencies of the blast scenarios leading to a 'fail' condition. Specified blasts need to cover all scenarios considered to be possible (i.e. scenarios with a significant annual frequency of occurrence).

Design margin will be acceptable if the performance goals are met.

For a Category C hazard, installation performance will be acceptable if compliance with acceptability conditions established by the regulatory body for the given scenario is demonstrated.

Common problems in nuclear plants

Typical problems arising from industrial explosions are as follows:

- Blast and thermal effects to exposed SSCs.

Additionally, an off-site explosion event that affects the nuclear site will likely cause off-site damage as well, depending on the relative locations of event source and site. The event may limit the effectiveness of emergency arrangements.

Common design solutions

Typical solutions to address these problems are based on the provision of specific protection for exposed SSCs.

6.3. APPLICATION TO NEW AND EXISTING NUCLEAR POWER PLANTS

The main focus of the present publication is on new nuclear installations since the purpose is to address the new IAEA design safety requirements. Particularly, the requirement to have an "adequate design margin" against external hazards (see Refs [1–4]).

However, the general methodology introduced in Section 6.1 is applicable to both new and existing NPPs. Differences may arise in implementation, mainly, in the selection of performance objectives and in the determination of the plant level capacity.

Typically, performance objectives could be less ambitious for existing plants, since there are less uncertainties about the actual plant condition which will see the external event and shorter time at risk.

Methods for obtaining the plant level capacity may be different in new and existing NPPs. However, the final outcome required for assessing the adequacy of the 'design margin', that is, the high confidence plant level capacity or the plant level fragility, will be the same irrespective of the method.

7. HAZARD SEVERITY INITIATING CLIFF EDGE EFFECTS

7.1. DESIGN ROBUSTNESS AND CLIFF EDGE EFFECTS

External hazard induced failure events that meet the following descriptions can lead to cliff edge effects:

- Sudden CCF events that result in concurrent loss of key safety and mitigation functions, such that the installation's ability to recover to a safe state is prevented;
- Failure events with abrupt increase in the probability of occurrence due to a small increase in the external hazard level.

SSR-2/1 (Rev. 1) [2] states that the design needs to provide adequate margins to avoid cliff edge effects. Generally, the safety margin against an external hazard that is considered in the design is a surrogate for the performance objective of the installation, that is, if the design demonstrates the minimum adequate margin, the performance objective of the installation is automatically achieved. The performance objective can be expressed in several ways specific to each hazard category. Further details are provided in Section 6.1.

For Category A hazards:

- The installation performance objective can be expressed by an annual frequency, such as CDF (for reactor facilities) or frequency of failure of barriers against releases. The metrics used for the design margin are a function of the hazard severity parameter, e.g. the installation-level HCLPF capacity.
- Initiation of the cliff edge effect can be expressed by the hazard severity parameter corresponding to the HCLPF capacity of the corresponding failure event.

For Category B hazards:

- The installation performance objective can be expressed in a similar way to Category A hazards, with the difference that the hazard is not represented by continuous hazard curves. It is represented by a number of discrete scenarios, each scenario defined by a discrete value of the hazard intensity parameter and an associated frequency of occurrence (generalized hazard parameters). The fragility is represented by conditional probabilities of exceeding the failure criteria at the discrete values of the hazard intensity parameter defining each scenario (generalized fragility parameters).

For Category C hazards:

- Hazards in this category may not have a frequency of occurrence associated with the hazard scenarios, and the concept of 'design margin' in the classical meaning may not be valid.
- The performance objectives for avoiding cliff edge effects are expressed using engineering attributes, such as the following:
  - The installation should not experience a severe accident condition following the postulated Category C hazard scenarios;
  - The main safety functions that prevent and mitigate the severe accidents should not be lost;
  - One safety train should remain functional;
  - The containment of NPPs should not be compromised;
  - Either the cooling or the containment function should be protected in NPPs if the plant is shut down.

Section 7.2 describes an approach for margin adequacy assessment for avoiding cliff edge effects induced by seismic hazard, which is a Category A hazard. Section 7.3 discusses margin adequacy

assessment for avoiding cliff edge effects induced by other external hazards.

7.2. CLIFF EDGE EFFECTS INDUCED BY SEISMIC EVENTS

This section provides an overview of seismic induced cliff edge failures, recommendations for identifying potential cliff edge failures using safety assessment of an NPP design, and strategies for determining the adequacy of seismic margins against cliff edge failures.

7.2.1. Seismically-induced cliff edge failure events

For typical seismic induced failure events, the demands imposed on SSCs due to vibratory ground motions and the SSC capacities to withstand their effect involve sufficient randomness and uncertainty (e.g. due to conservatism in the design) to result in gradual increases in conditional failure probabilities with the increase in the seismic hazard intensity parameter. Accordingly, considering the characteristics of cliff edge failures in Section 7.1, seismic induced failures that can lead to cliff edge effects are therefore not as common as in some other external hazards, such as external flood. However, such seismic induced failures that can lead to cliff edge effects are possible.

Classic cliff edge failures are often triggered by seismic induced failure mode with widespread consequences of SSC failures from which the installation cannot recover. The following are examples of classic seismic induced failure events that can lead to cliff edge effects:

- Strong impact between adjacent structures can result in failure of multiple housed SSCs due to shock waves and/or severe damage or penetrations of the structures due to collision;
- Widespread soil liquefaction can lead to ground failures or settlement across the installation site and the concurrent loss of multiple safety functions;
- Other seismically induced geotechnical failure modes, such as lateral spreading, slope instability, ground subsidence, and surface rupture due to capable fault displacement can lead to similar outcomes to liquefaction induced settlement;
- Seismic induced breach of upstream dams or tsunami that can flood the installation site.

A common characteristic of these examples (and other classic cliff edge effects) is that the resulting demands on the SSCs (e.g. relative displacements) are highly non-linear relative to the hazard severity parameter. They can abruptly increase to levels that lead to almost certain SSC failure upon occurrence of the CCF event that triggers them. Only limited variability exists in the seismic fragility due to randomness and uncertainty in the relationship between the hazard intensity parameter and the triggering CCF event. The shapes of the fragility functions for classic cliff edge events are often non-log-normal and may approach a step function. They may be represented using log-normal probability functions with steep slopes, that is, with a small composite logarithmic standard deviation β_c.

A non-classic cliff edge scenario may be possible whereby the accumulation of uncorrelated probabilities of several individual SSC failures with commensurate SSC HCLPF capacities that are close to the installation-level HCLPF capacity leads to an abrupt increase in the installation-level seismic fragility without these SSC failures being triggered by a single failure event. It is conceivable that, if a considerable number of such failures are combined using an OR logic gate, the resulting installation-level fragility curve could have a steep slope at hazard intensity parameter values that slightly exceed the HCLPF capacity even though the individual SSC fragilities show gradual increases in their conditional probabilities of failure. This non-classic cliff edge scenario is considered in this publication, though in less detail.

7.2.2. Identification of potential cliff edge failures in design

Robust designs are expected to have adequate seismic margins to avoid potential cliff edge effects. New nuclear installation designs increasingly rely on passive safety systems with sufficient redundancy against single points of failure to make the presence of cliff edge failure events significantly unlikely, but it may not be feasible to deterministically eliminate them for all sites. If a potential cliff edge failure event is identified in the design, it has to have a capacity sufficiently high to avoid it being a significant consideration for the installation risk to safety. Safety assessment of the design is used to demonstrate this adequacy by assessing the margin against potential cliff edge effects.

The design margin adequacy assessment proposed here consists of reviewing the safety assessment output to identify: (1) whether a potential cliff edge effect failure is identified for the design that is not deterministically screened out of explicit fragility evaluation as practically eliminated, and (2) whether this potential failure has sufficient margin above the DBE hazard level to avoid unacceptably influencing the performance of the installation.

Review of the safety assessment output needs to include, to the extent practical:

- Review of seismically-induced failure modes and their consequences to identify known potential cliff edge events (see Section 7.2.1);
- Review of individual cutsets[23] and their seismic fragilities for significant risk contributors;
- Review of the installation-level seismic fragility output;
- Review of sensitivity analyses performed for potential cliff edge event triggers.

The output of the SMA methodology does not include cutsets since it includes only seismic fragilities for SSCs on the credited success paths. However, it includes screening or HCLPF capacity evaluations for failure modes that may lead to classic cliff edge type failures (see Section 7.2.1) and can disrupt a success path. In general, the SMA methodology is less capable of identifying potential cliff edge failure events than the other two safety assessment methodologies (see Section 5.1.3) since it uses a success path approach instead of a PSA model of all credible accident sequence combinations.

Figure 4 shows an idealized example representation of an installation-level seismic fragility curve. Shown also in Fig. 4 are the fragility curves for the individual cutsets. The failure event of any cutset leads to failure of the installation, and the installation-level fragility is the union probability of the conditional probabilities from the constituent cutsets. All the fragility curves have smooth shapes without abrupt increases. Figure 4 is an example of an installation design that does not have a potential cliff edge failure event at the hazard severity levels of interest to the installation performance.

Figure 5 introduces one additional cutset fragility to the installation design shown in Fig. 4. The latter fragility is for a failure event that can lead to a cliff edge effect in the classic sense of Section 7.2.1. The installation-level fragility curve shows a smooth transition with respect to the hazard intensity parameter up to shortly after the initiation of the cliff edge failure event, then it shows an abrupt increase to certain failure for a subsequent small increase in the hazard severity. The comparison between Fig. 4 and Fig. 5 illustrates the need for a robust design to have adequate margins against potential cliff edge effects. The abrupt increase in installation level fragility slope invalidates the assumptions of the margin adequacy based on installation-level HCLPF capacity developed in Section 5.2.3.1, which are predicated on conventional seismic fragility curves that can be represented by log-normal functions (considered to have β_c variability parameters of 0.3 or higher) in the hazard range of interest to the performance goal. This may lead to the installation performance objective exceeding the annual frequency based goals unless the cliff edge failure event has a sufficiently large margin to avoid this (i.e. such that the deviation

[23] A 'cutset' is a combination of initiating events (failures and/or human errors) whose sequence causes the accident to occur. Occurrence of all events in the cutset is necessary and sufficient for the accident to take place.

from the log-normal shape in the installation-level fragility curve has no significant consequence for the achieved annual frequency based performance).

Figure 6 shows the fragility curves for the same installation when the potential cliff edge failure event has a larger seismic margin. The installation-level fragility curve shows a smooth transition with respect to the hazard intensity parameter over the entire hazard severity range of possible interest to the installation performance. This potential cliff edge failure event can therefore be readily assessed to have an insignificant consequence to the installation performance and be screened out for further consideration of cliff edge effects. The comparison between Fig. 4, Fig. 5, and Fig. 6 illustrates the importance of the installation design having adequate margin to avoid cliff edge effects.

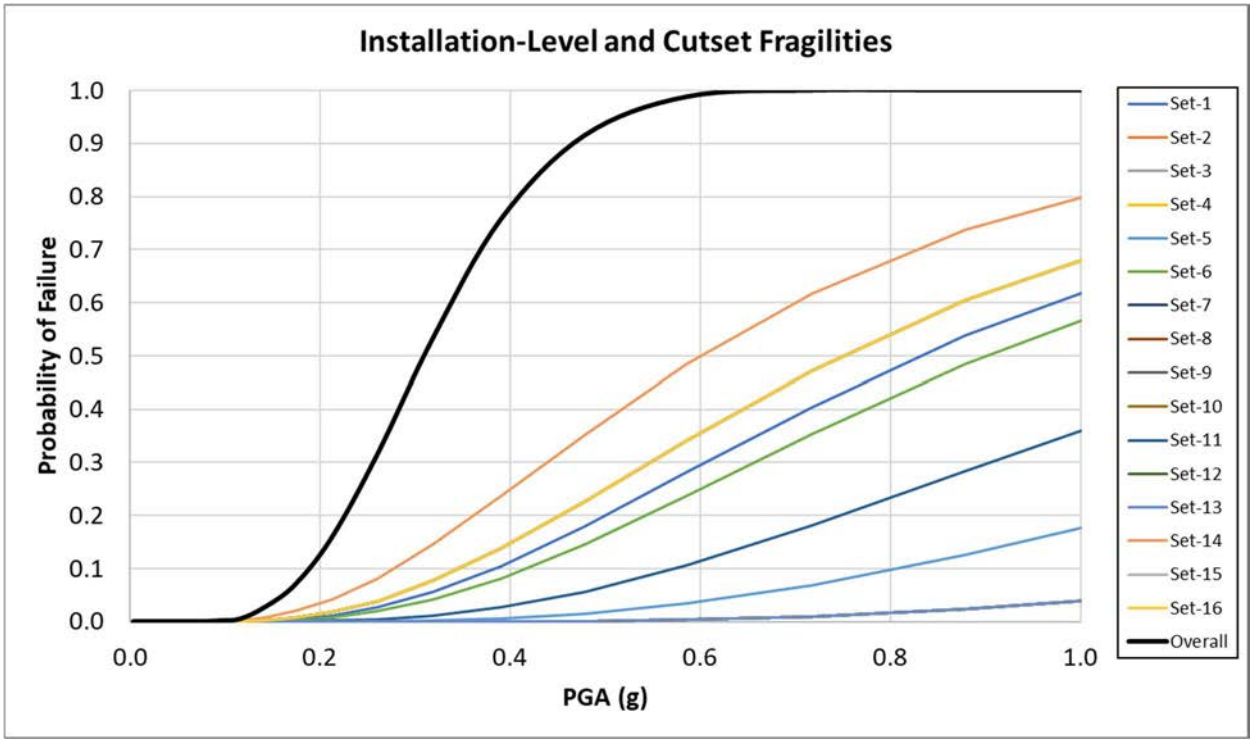

FIG. 4. Example installation-level fragility without cliff edge failure. The discrete conditional probabilities defining the installation-level fragility function are connected using splines to produce a continuous fragility curve.

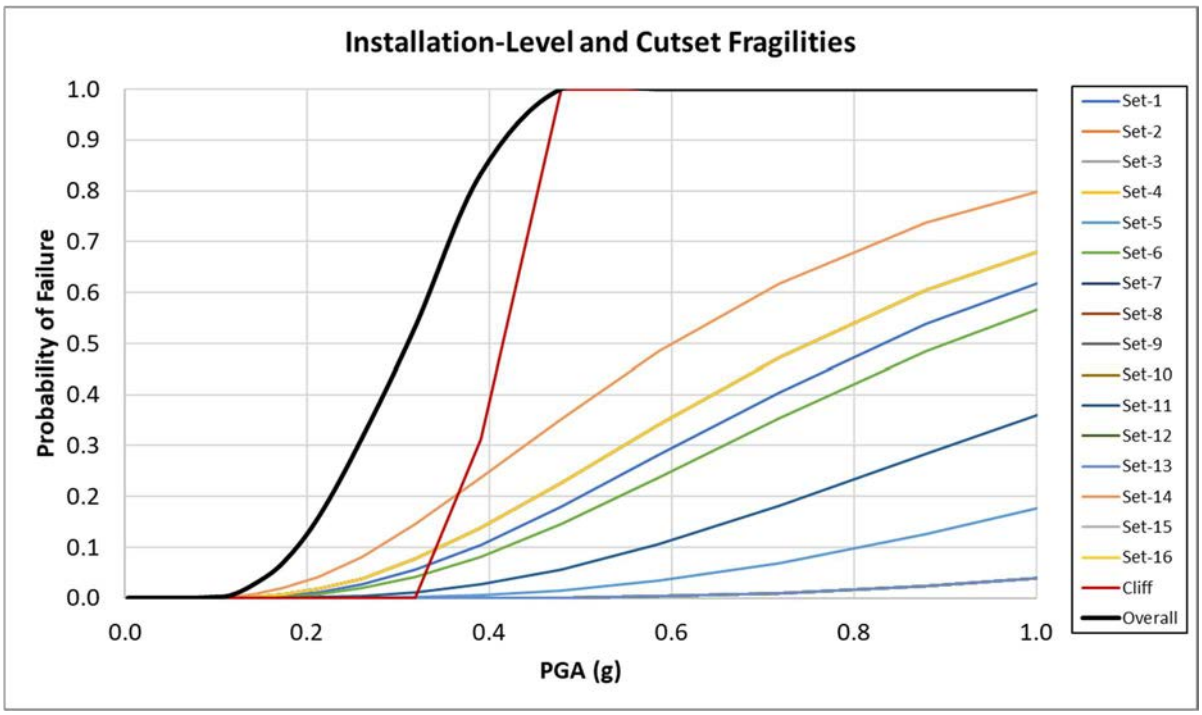

FIG. 5. Example installation-level fragility with potential cliff edge failure.

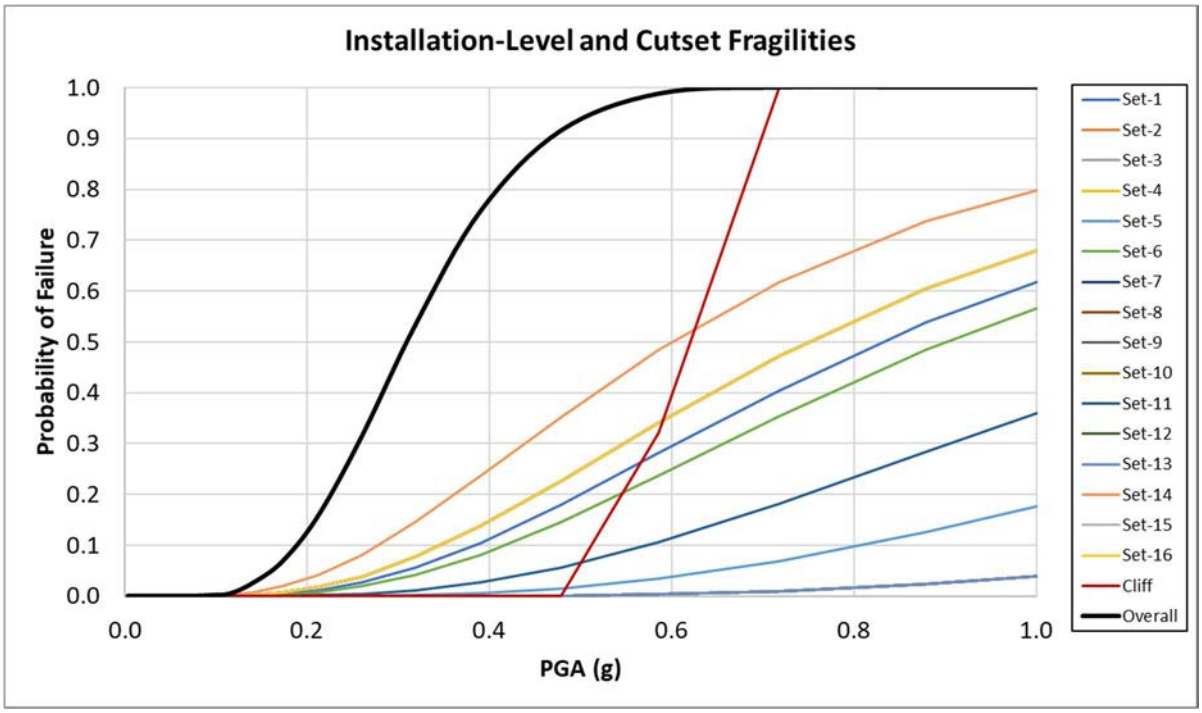

FIG. 6. Example installation-level fragility with less consequential cliff edge failure.

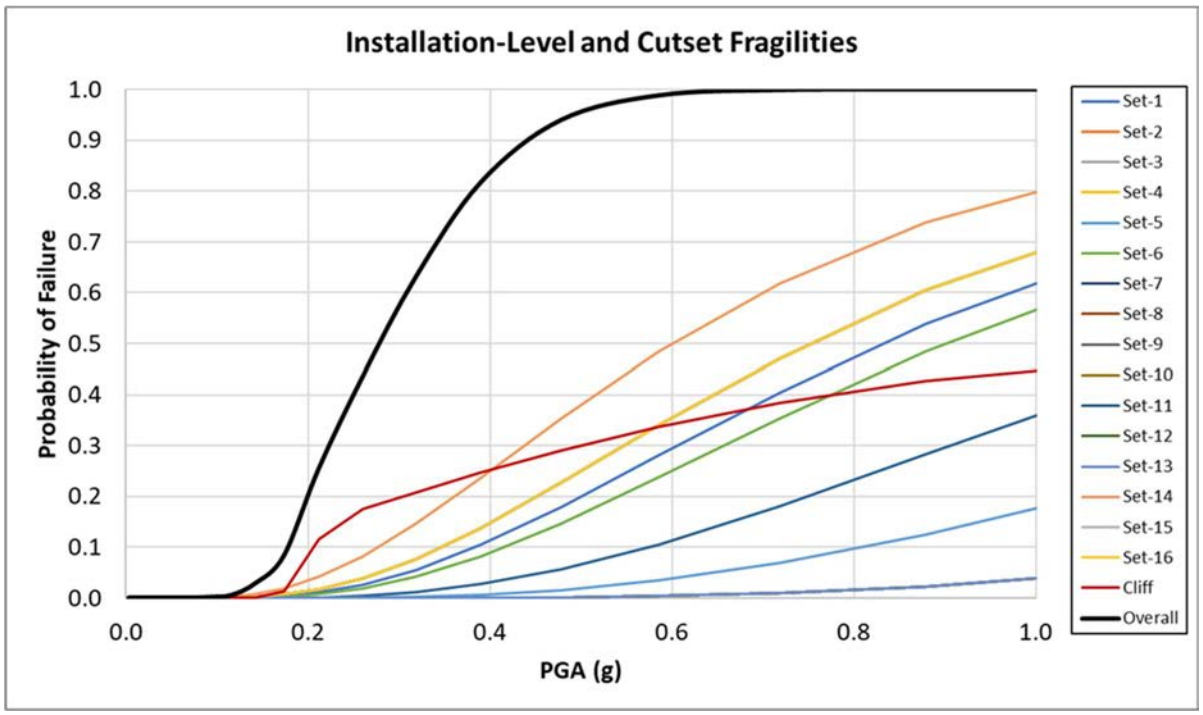

FIG. 7. Example installation-level fragility with non-log-normal cliff edge failure fragility.

As stated in Section 7.2.1, seismic fragility curves for failure events that can lead to classic cliff edge failures often have non-standard shapes that do not follow a log-normal distribution. Moreover, these fragility curves do not necessarily increase abruptly to 1.0 over a short interval of the hazard severity parameter. For example, liquefaction settlement induced fragilities may never reach a conditional failure probability of 1.0 because the settlement is physically constrained even at very high values of the hazard severity parameter by the geotechnical configuration, including the thickness of the liquefiable layer. Figure 7 shows an example such fragility curve for a cliff edge failure event.

Finally, the potential existence of a non-classic cliff edge failure scenario as described in Section 7.2.1 is not straightforward to identify by review of individual cutset fragilities. An efficient alternative to assess this potential, and the design margin adequacy thereto, can be based on review of the installation-level mean fragility curve. This technique can also be used to perform an initial screening for potential presence of other types of cliff edge events before reviewing individual cutset fragilities. The annual frequency based seismic margin adequacy recommendations developed in Section 5.2 rely on the empirical observation from recent SPSAs that β_c is typically equal to or greater than 0.3. Steeper installation-level fragility curves violate this basis.

An installation-level fragility curve explicitly developed using PSA methods often consists of discrete conditional probability values determined at specified increments of the hazard parameter and interpolated in between. A practical technique to characterize β_c for an installation-level fragility is by using the ratio of $A_{10\%}$ to the HCLPF capacity, where $A_{10\%}$ is the seismic hazard parameter value corresponding to 10% mean conditional probability of failure.[24] Using this ratio is robust since: (1) installation-level fragilities are developed in a discrete form rather than a functional form with log-normal parameters, and (2) the relatively narrow hazard parameter range between the HCLPF capacity and $A_{10\%}$ typically contributes about 50% at least of the computed annual frequency of failure (i.e. more than the rest of the hazard space). For β_c equal to 0.3, this ratio is equal to:

$$A_{10\%}/A_{HCLPF} = A_M . exp(-1.28\beta_c) / A_M . exp(-2.33\beta_c) \quad = 1.37 \approx 1.4 \tag{19}$$

[24] The $A_{10\%}$ capacity is a metric introduced and used in other international standards and seismic design criteria for nuclear facilities, e.g. ASCE 43-19 [17].

Accordingly, a ratio of $A_{10\%}/A_{HCLPF}$ less than 1.4 on the mean installation-level fragility curve can signify the potential presence of an abrupt failure event for further review and consideration in the cliff edge margin adequacy assessment. While this technique offers a powerful and simple screening tool for cliff edge effects, using this technique requires the availability of the mean installation-level fragility curve from the explicit solution of a PSA logic model, that is, it cannot be used with the output of the SMA methodology.

7.2.3. Margin adequacy assessment for cliff edge failures

The criteria for assessment of design margin adequacy against potential cliff edge failures depend on whether this failure is a result of a single failure event that results in widespread SSC failures in the classic sense of the term or a result of a non-classic cliff edge failure scenario due to abrupt accumulation of failure probabilities of many individual SSC failures with commensurate HCLPF capacities (see Section 7.2.1). Sections 7.2.3.1 and 7.2.3.2 present these criteria and summarize the difference. In addition, the tools available to the analyst for implementing these criteria depend on the methodology and results available from the safety assessment, as discussed in Sections 7.2.3.3 and 7.2.3.4. Annex III presents example implementations.

Assessment of the adequacy of seismic margins for potential cliff edge effects can follow several strategies. The strategy selection will be constrained with the available information from the safety assessment and the feasibility of implementing the criteria and tools introduced in Sections 7.2.3.1 to 7.2.3.4. The possible strategies include the following:

- For classic cliff edge failure events:
  - Demonstrating that one of the two criteria in Section 7.2.3.1 is satisfied. This requires availability[25] of SPSA, PSA based SMA, or SMA output for the installation and the seismic fragility function or HCLPF capacity for the cliff edge failure event.
  - Demonstrating that no potential cliff edge failure event has a HCLPF capacity lower than the lowest HCLPF capacity that guarantees satisfying one of the two criteria in Section 7.2.3.1. This requires availability of SPSA, PSA based SMA, or SMA output for the installation and it produces only a screening evaluation of potential cliff edge failures.
- For non-classic cliff edge failure scenarios:
  - Demonstrating that one of the two criteria in Section 7.2.3.2 is satisfied. This requires availability of the explicitly calculated installation-level fragility.
  - Justification that the first criterion in Section 7.2.3.2 is satisfied with high confidence based on qualitative review of applicable success paths or accident sequences (see Section 7.2.3.4). This is an alternative strategy where only the installation-level and SSC HCLPF capacities are available from PSA based SMA or SMA output.

7.2.3.1. Classic cliff edge failure events

When a potential cliff edge failure event in the classic sense is identified in the safety assessment of the design, the minimum adequate design margin for precluding it can be set to be the lesser HCLPF capacity for this failure event needed to satisfy either of the following two criteria:

- The contribution of the potential cliff edge effect to the annual frequency of failure characterizing the performance of the installation is less than a low percentage of the performance goal (on the order of 10%, or as specified by the national regulatory body); or

[25] Sections 7.2.3.3, 7.2.3.4, and Annex III present implementation specifics and limitations that depend on the available information.

- The annual frequency performance metric of the facility, computed using the installation-level fragility with the potential cliff edge effect included, is below the established performance goal used in Section 5.2.3.1.

The use of the lesser margin from both criteria above recognizes that, for significantly flat hazard curves (i.e. relatively high A_R parameter values), the seismic margin required to achieve the first criterion may be impractically large while not significantly contributing to the installation risk reduction. Meanwhile, if only the first criterion is satisfied, then the potential cliff edge failure has a small contribution to risk, and the performance goal may be more effectively achieved by improving the installation-level fragility through other means, for instance, by hardening risk significant SSCs against vibratory ground motions.

7.2.3.2. Non-classic cliff edge failure scenarios

A finding that the ratio $A_{10\%} / A_{HCLPF}$ is less than 1.4 does not conclusively identify a cliff edge failure event. It primarily identifies that the installation-level fragility curve is steeper than considered in developing the installation-level HCLPF capacity based margin adequacy recommendations developed in Section 5.2 and, therefore, indicates that further adequacy considerations need to be included. Review of the cutsets to understand what is causing the abrupt increase in the installation conditional probability of failure between the A_{HCLPF} and $A_{10\%}$ capacities may identify a classic cliff edge failure event, a scenario in which many individual SSCs with commensurate HCLPF capacities result in rapid aggregation of the installation conditional failure probability, or another underlying reason. When a classic cliff edge failure event is not identified but the ratio $A_{10\%} / A_{HCLPF}$ is found to be less than 1.4, the installation-level seismic margin can be considered adequate to preclude a cliff edge failure in the design if either of the following conditions is met:

- The $A_{10\%}$ capacity is higher than or equal to 1.4 times the minimum adequate HCLPF capacity determined according to Section 5.2.3; or
- The annual frequency performance metric of the facility, computed using the installation-level fragility, is below the established performance goal used in Section 5.2.3.1.

These criteria recognize that the installation HCLPF capacity may be higher than the minimum needed to achieve the annual frequency based performance objectives assuming the generic β_c value of 0.3. The potential reserve in this margin may therefore offset the invalidation of the earlier assumption by the ratio $A_{10\%} / A_{HCLPF}$ ratio being lower than 1.4.

7.2.3.3. Margin adequacy assessment using SPSA results

If the results of a SPSA are available to the safety assessment, the installation-level and cutset fragility curves can be directly constructed. Confirmation of the margin adequacy to avoid cliff edge effects, using any of the criteria presented in Sections 7.2.3.1 or 7.2.3.2, can therefore be performed explicitly, based on the computed performance metrics as described above.

7.2.3.4. Margin adequacy assessment using SMA results

While the results available to the safety assessment are from a SMA or PSA based SMA, the fragility curves will likely not be available (i.e. only the HCLPF capacities will be available in conjunction with generic values of β_c).

For identified potential cliff edge failure events to which Section 7.2.3.1 is applicable, the installation-level HCLPF capacity and the HCLPF capacity of the potential cliff edge failure event can be used to confirm the margin adequacy to avoid cliff edge effects according to the criteria presented in Section 7.2.3.1 using the following idealizations (see Section 5.2.2):

- The installation-level fragility curve without the potential cliff edge being included can be idealized as a log-normal probability function anchored to the installation-level HCLPF capacity as described in Section 5.2.1.

- The cliff edge failure event fragility curve can be idealized as a log-normal probability function anchored to its HCLPF capacity and the lowest value of β_c considered to be irreducible for the effect of ground motion randomness given knowledge of the failure event and site seismicity.
  - For seismic induced failures, a generic minimum value of 0.1 is suggested for the β_c parameter from review of previous cliff edge fragility evaluations.
  - Alternatively, this fragility curve may be idealized as a step function going abruptly from 0 to 1, which is likely conservative for seismic induced failures but may be appropriate for other external hazards.
- The installation-level fragility curve with the potential cliff edge included can be derived by computing the union conditional probabilities of the two idealized fragility curves above.
- The performance metrics for the assessment criteria in Section 7.2.3.1 can be computed by convolving these idealized fragility curves and the mean seismic hazard curve at the site.

If the results available to the safety assessment are from a PSA based SMA, they may include an estimate of the installation-level fragility curve and/or others. In such case, the explicit margin adequacy assessment described in Section 7.2.3.1 can be implemented in accordance with Section 7.2.3.3 and supplemented only as needed with the idealizations presented in this section.

For non-classic cliff edge failure scenarios to which Section 7.2.3.2 is applicable: if such scenario exists, then computing the ratio $A_{10\%} / A_{HCLPF}$ to identify it is not feasible if only the installation-level HCLPF capacity and a generic β_c are available. If an explicit estimate of the installation-level fragility is produced from a PSA based SMA, it may be used for this computation. The estimate of the corresponding ratio $A_{10\%} / A_{HCLPF}$ has to be either realistic or conservative, e.g. based on conservatively biased (i.e. low) generic β_c parameters assigned to the SSC fragilities when quantifying the PSA model.

Alternatively, if only the HCLPF capacities are available and computing the ratio $A_{10\%} / A_{HCLPF}$ is not feasible, a qualitative review may be possible to justify concluding with confidence that the first criterion in Section 7.2.3.2 is satisfied. One approach to conducting this review is as follows:

- Identify SSCs whose HCLPF capacities are lower than 1.4 times the minimum adequate HCLPF capacity determined according to Section 5.2.3.
- Review the success paths (for SMA) or accident sequence cutsets (for PSA based SMA) which include these SSCs.
- Assign a conservatively biased (i.e. low) generic β_c to these HCLPFs. A generic β_c of 0.3 for individual SSCs is considered to be low. Exceptions can be made on a case-by-case basis for SSC failure modes for which experience with previous evaluations justifies them.
- Based on the success path or accident sequence logic, confirm by inspection or by developing a simplified conservative estimate that the installation-level conditional probability of failure is less than 10% at 1.4 times the minimum adequate HCLPF capacity per Section 5.2.3.

This alternative evaluation in the absence of an explicit fragility function is clearly one which relies in larger part on judgment. Appropriate conservatism needs to be considered in exercising this judgment.

7.3. CLIFF EDGE EFFECTS INDUCED BY OTHER EXTERNAL EVENTS

Cliff edge failure events due to other external hazards follow the same descriptions introduced in Section 7.1. Some external hazards have characteristics that are more likely to cause classic potential cliff edge failure events than others. Examples of such potential cliff edge effects include the following:

- External flood that overcomes protective barriers and inundates multiple SSCs;

- Aircraft crash that penetrates containment (for NPPs) or causes widespread damage such that fundamental safety functions cannot be maintained.

Cliff edge adequacy assessment strategies and criteria for external hazards depends on the hazard categorization identified in Section 6.1. Hazard specific criteria are not developed for each external hazard in this publication. The following Sections 7.3.1 to 7.3.3 identify assessment strategy considerations applicable to each of these external hazard categories. Hazard specific criteria can be developed based on these considerations, hazard specific margin requirements presented in Section 6, and the example criteria developed for seismic hazard and presented in Section 7.2.

7.3.1. Category A hazards

Potential cliff edge failure identification and adequacy assessment for Category A hazards can directly follow the strategies and example of the performance based criteria presented in Section 7.2. Detailed criteria and implementation methods for individual external hazards need to be developed to correspond to the particular knowledge of the effects of each hazard. For example, minimum variability parameters depend on the randomness, uncertainties, and SSC failure modes associated with the effects of each hazard; minimum margin requirements for installation-level fragilities need to be in accordance with Section 6; and annual frequency based performance goals may or may not be hazard specific.

7.3.2. Category B hazards

Cliff edge adequacy assessment for Category B hazards can follow the principles and general strategies presented in Section 7.2 with appropriate adjustments to account for the characterization of each hazard using discrete scenarios with corresponding annual frequencies of occurrence (generalized hazard characterization) instead of continuous curves of annual exceedance frequencies.

Identification of potential cliff edge effects can generally follow the guidance presented in Section 7.2.2. Review of the installation-level fragility function is replaced with review of the installation-level conditional probabilities of failure and the significant cutsets at the discrete hazard scenarios to identify scenarios at which the probability may show abrupt increases and identify the underlying reasons. Review of the ratio $A_{10\%} / A_{HCLPF}$ is not applicable. There is no distinction needed between classic and non-classic cliff edge failure events in this hazard category, since the review of concurrent failures that may lead to cliff edge effects is performed at discrete individual hazard scenarios.

Margin adequacy assessment for a potential cliff edge failure event can generally follow the criteria presented in Section 7.2.3.1. An installation-level HCLPF capacity may not be available for Category B hazards. However, either (1) individual conditional probabilities of failure for each hazard scenario, or (2) knowledge of the hazard scenarios where the HCLPF capacity is not exceeded has to be available. The determination of the acceptable HCLPF capacity margin for a potential cliff edge effect is replaced with identifying the discrete hazard scenario with the highest corresponding annual frequency of occurrence (if any) for which the initiation of the cliff edge effect is acceptable.

The implementation steps using output from PSA, PSA based margin assessments, and margin assessments presented in Sections 7.2.3.3 and 7.2.3.4 can be followed as applicable with minor adjustments, including the following:

- External hazard curves are replaced with the generalized hazard frequencies of occurrence.
- Installation-level fragility curves are replaced with the generalized fragilities composed of the conditional failure probabilities corresponding to the discrete external hazard scenarios;
- Generic β_c variability parameters are replaced with a step function if it is only known which hazard scenarios exceed or do not exceed the HCLPF capacity, unless otherwise justified.

7.3.3. Category C hazards

Cliff edge adequacy assessment for Category C hazards cannot rely on annual frequency based performance objectives. The performance objectives for Category C hazard are defined deterministically using engineering attributes, such as those listed in Section 7.1. For Category C hazards, the required engineering attributes need to be satisfied for the deterministic external hazard scenarios used in the safety evaluation. These deterministic scenario evaluations can use success path models or PSA models to propagate the effects of these hazards on the installation and the consequences of SSC failures on the achievability of the required engineering attributes.

These deterministic evaluations have to use appropriate levels of confidence for characterizing the demand and capacities of SSCs resulting from each external hazard scenario. These levels of confidence are typically specified by the national regulatory body. Since these hazard scenarios represent extreme rare conditions to be experienced by the installation, these confidence levels are typically allowed to be more relaxed than those used for the design basis conditions of the installation.

8. PLANT IMPROVEMENTS BASED ON THE ASSESSMENT OF DESIGN ROBUSTNESS

Starting from the flow diagram in Fig. 1, the present section deals with the return loop where the question has been asked: 'Are design margins adequate?' To which the answer is NO, plant improvements are needed to enhance the robustness of the facility. The safety analysis of the original design indicates that the level of design robustness is not optimal and needs to be improved, if at all possible, to meet the performance objectives set for the nuclear installation.

8.1. EXISTING FACILITIES

As with all safety improvements to existing nuclear installations, the application of pragmatism is essential. Implementing significant modifications in existing nuclear sites is often an exercise in managing competing interests and requirements. Where several options exist, balancing these competing interests to select potential modification(s) in a way that demonstrably leads to the optimal enhancement to facility or site robustness is often challenging to achieve in practise.

As noted above, existing sites, especially larger multifacility sites, can present very challenging issues in this respect. However, that will not prevent the implementation of some improvements. Enhancing the robustness of one facility on the site benefits not only that facility but the site as a whole.

It is unlikely that an existing facility will be able to meet all the expectations of a comparable new design because codes and standards will have progressed, and the facility will have aged, and may have suffered corrosion and other forms of degradation, over time. Nor is it necessary for full 'as-new' compliance to be enforced. What has to be expected is the closest approach to the 'as-new' condition that can reasonably be achieved, subject to a minimum standard below which further operation of the facility is undesirable.

A representative sample of modifications that could be implemented to improve existing facility robustness against external hazards is discussed below. These are considered here as a way of examining the practical implications of making improvements to the robustness of an existing facility.

8.1.1. Engineering modifications

8.1.1.1. Strengthening building envelopes

Advantages:

- Strengthening buildings is a way of enhancing robustness of all stress based design robustness metrics.
- Strengthening building envelopes enables internal equipment to be protected without itself needing to be strengthened. Enhancing robustness of buildings containing SSCs to extreme wind is a typical example.

Constraints:

- Any large scale construction work on a nuclear site can create challenges if it takes place in and around a nuclear installation, because of the potential for interference with existing safety systems and because of concerns about worker dose uptakes. The existence of contaminated ground is a particular issue of concern here. In many cases, these reasons can make such modifications impractical. Major structural changes to enhance robustness are therefore unlikely to be justifiable, except in highly unusual situations such as, for example, the Chernobyl New Safe Containment structure, where there were overriding public safety reasons to consider.

- Likely to be a costly option.

- Interactions with existing safety systems. It is unlikely to be practical to implement major structural changes to containment and/or shielding structures, especially if such work is required to the internals of these structures. In many cases, these internal volumes will be inaccessible because of space and access constraints, and because of the radiation environment.
- Worker dose uptake can be a severe constraint if the modification takes place in a controlled radiation environment.

8.1.1.2. Strengthening of equipment anchorages

Advantages:

- Strengthening equipment SSC anchorages to building structures is a way of enhancing robustness of all stress based design robustness metrics, especially those related to seismic vibration hazard. Non-seismically designed electrical equipment and pipework are vulnerable, and modifications to improve robustness have been implemented extensively and successfully on existing NPPs. Typical examples would be the addition of pipe snubbers, improved anchorage of electrical equipment, and the strengthening of emergency access and exit routes.

Constraints:

- Modifications to large numbers of equipment SSCs in congested areas can lead to very challenging interaction problems and potential inability to deliver safety functions. This can happen while the modification work is ongoing where working room, access etc. is limited, and also in designing the modification where congested spaces make the location of strengthening members and fixings difficult. On the other hand, after the implementation of modifications, it needs to take into account the potential maintenance and control during the operational lifetime of the installation.
  - Likely to be a costly option if implemented in challenging radiation or hazardous environments.
- Worker dose uptake if the modification takes place in a controlled radiation environment. Widescale implementation of strengthening works in radiation environments is unlikely to be practical and consideration on a case-by-case basis will be needed.

8.1.1.3. Missile protection

Advantages:

- Addition of strong structural forms able to resist missile penetration eliminates the potential for missile hazard for SSCs in the shadow of the protection structure.

Constraints:

- Off-site missiles with potential to reach the site will likely be large and massive, e.g. aircraft, wind turbine blades. Protection barriers would need to be substantial structures to resist such items, needing sufficient space for construction and being relatively costly.

8.1.1.4. Blast and thermal protection

Advantages:

- Likely to be limited to selected vulnerable SSCs in area close to the site boundary, therefore relatively cheap and easy to implement.

Constraints:

- Access restrictions may make such modifications impractical.

8.1.1.5. Control of temperature and environmental conditions

Advantages:

- The addition of new HVAC equipment to enclosures that require a temperature controlled environment represents a significant enhancement to facility robustness when temperature sensitive SSCs are present.
- The addition of thermal insulation or trace heating to protect external equipment from cold weather conditions is generally relatively inexpensive to install and offers predictable operational improvements under extreme cold weather conditions. This is mostly used for water containing pipework and similar to protect from freezing conditions.

Constraints:

- Introducing HVAC systems into facilities where none previously existed is likely to be very expensive. Modifying existing systems in radiation controlled areas can be very challenging because the ducting and fans can become contamination hot spots.
- Space limitations for HVAC plant and ducting are likely to be significant constraints on the practicability of implementing such modifications.
- In a controlled radiation environment, it is generally undesirable to introduce additional material in bulk unless overriding good reasons exist to do so. Good procedural management of such areas normally involves the minimization of additional materials to what is absolutely necessary, thereby minimizing the future waste burden during the decommissioning phase.
- Interactions with existing safety systems, for example if modifications to HVAC systems in contaminated areas are proposed, needs very careful planning and management if containment safety function is to be maintained through the implementation work.
- Worker dose uptake if the modification takes place in a controlled radiation environment can be a significant constraint.
- Heat trace system for pipes needs to be considered equally important as the pipes for protection of pipes, maintenance and control as needed.

8.1.1.6. Modifications to improve flood protection

Advantages:

- Raising the primary flood barrier height eliminates the hazard up to a given level, therefore providing permanent safety enhancement.
- Permanent flood barriers normally protect the entire site, or the most significant parts of it. Improving flood protection in this way provides benefit to the entire protected region simultaneously.
- Temporary flood protection generally involves removable barriers at building entrances. It is generally relatively inexpensive and easy to modify buildings to take such barriers.
- Temporary flood barriers and devices (e.g. pumps) can be put in place quickly in response to flood warnings and then removed when the flood hazard has reduced.

Constraints:

- Raising the primary flood barrier height is likely to involve significant civil engineering works at large cost and possibly major disruption to parts of the site.

- Unlikely to be cost effective to increase barrier height to cover very low frequency flood events, so additional flood protection, or mitigation measures may still be needed.

- Temporary flood protection usually impedes access and exit routes from buildings when barriers are in place. May require alternative personnel access routes to be identified, whenever safety functions and/or emergency arrangements require this.
  - Not suitable for protecting radiation controlled areas directly because barriers may not be waterproof and there may be dose uptake issues with their use. Also, breach of barriers may lead to a contamination problem after the flood event.

8.1.1.7. Provide portable emergency mitigation equipment

Advantages:

- Requires only minor plant modifications in the safety related SSCs (connection points with the portable equipment).
- Portable equipment is versatile enough to cope with a wide range of potential scenarios, which could result from different hazards.
- Portable equipment can add to the diversity, redundancy, and physical separation already introduced by the design.

Constraints:

- A storage area or building for portable equipment needs to be constructed, able to protect the equipment against design and beyond design external events.
- At the storage place, the equipment itself needs to be qualified for the design and beyond design external events, for which the intended safety functions will need to be performed.
- The routes from the storage place to the connection points in the safety related buildings need to be practicable after the events which could motivate the need to deploy the portable equipment.
- The staff need to be trained to use this equipment as under realistic conditions.

8.1.2. Modifications involving changes to safety procedures and operating limits

Advantages:

- Where sufficient engineered protection cannot be implemented, limiting operations is a safety management process that effectively limits the consequences from any fault condition arising from a hazard, and reduces the burden on the engineered protection and mitigation systems that do exist.
- It may be cheaper and easier to change safety management arrangements than to implement new engineered measures but see constraints below.
- Difficulties regarding performing surveillance and periodic testing.

Constraints:

- Safety management actions are low hierarchy safety features. They should not be used as a substitute for engineered measures unless compelling reasons apply. Such actions need only to be considered when additional engineered protection is not practical, or when they provide an additional layer of safety protection.

8.2. DESIGNS OF NEW FACILITIES

As noted above, more control can be exercised over the ability to implement modifications to new designs than is the case for existing facilities. However, similar problems exist in terms of constructability, increased costs etc, although to a lesser extent. The following points are noted by comparison with the more detailed lists above of advantages and constraints for existing plants:

- Implementing modifications to the design before construction has started means that the changes are paper based and constructability issues (e.g. access) can be managed more effectively, for example by making corresponding changes to other parts of the facility design.
- Implementing modifications to the design before construction or making provision for such modifications at the design stage, so they can be implemented through the installation's lifetime, greatly can eliminate the need to implementing modifications at a later date.

  A classic example of this is the potential need to raise primary sea defences due to climate change effects on sea level. There may be no need during the early lifetime of the facility to fully protect against projected sea level rise, and the large degree of uncertainty surrounding how severe this effect will be may make designers reluctant to engage in costly civil engineering work at an early stage. However, by making provision at the design stage to enable modifications to be implemented later if the need is identified, say through a periodic safety review process, will assist in future proofing the new design against coastal flooding hazard.
- There are no worker dose uptake issues involved with implementing modifications as part of a new design, even if it is undergoing construction, so long as active commissioning has not commenced. Thus, modifications to highly active and/or inaccessible areas when the facility becomes operational remain possible at the design stage.
- Significant cost may still be incurred, especially if the modification also requires corresponding changes to major civil structures.

9. CONSIDERATIONS FOR MULTI-UNIT SITES

The use of PSA in supporting the safety related decision making for NPPs is most often based on analyses of a single reactor unit. However, the majority of NPP sites with operating reactor units worldwide have more than one nuclear unit on them (138 out of 192 NPP sites worldwide are multi-unit sites). Safety analyses are usually confined to a single unit, therefore the potential for accident sequences involving two or more reactor units, such as occurred during the Fukushima Daiichi NPP accident, is not explicitly considered.

In the multi-unit PSA (MUPSA) context, PSA is an important tool that is used for getting risk insights. In addition, other quantitative and qualitative considerations (based on deterministic safety analysis) may be used within the broader perspective of NPP site safety and risk assessment.

MUPSA is now referred to in a number of IAEA safety standards which were revised after the Fukushima Daiichi accident. MUPSA is aimed to identify and analyse multi-unit risk contributors needed to support the site wide risk management.

Risk assessment for multi-unit sites is more relevant for sites with a relatively large number of nuclear installations (many NPPs) and/or with NPPs that credited a significant amount of shared systems and resources. Reactors at multi-unit plants typically share an electrical grid and may share other SSCs that provide vital safety related functions, such as an emergency supply of water used to cool a reactor.

These shared systems can be both beneficial and disadvantageous during an accident. The MUPSA methodology can help Member States investigate and assess multi-unit site designs, covering both the positive and potentially negative aspects of shared systems in a balanced way.

MUPSA may provide a technical basis for maximizing the benefit of sharing systems and resources in the multi-unit context and minimizing the multi-unit accidents contribution (due to shared systems and resources) to the overall site risk. Moreover, MUPSA may support a risk informed assessment of the adequacy of the DiD in multi-unit context.

The IAEA has developed and tested a methodology providing step-by-step guidance to experts on conducting a MUPSA. Safety Reports Series No. 110, Multi-Unit Probabilistic Safety Assessment [44], provides a methodology for conducting MUPSA and assessing multi-unit contribution to the site risk. It also presents the methodology and results of a case study. Ultimately, this methodology will help decision makers decide where to focus their resources within a multi-unit context to get the most benefit in terms of safety and cost efficiency.

10. INSTALLATIONS OTHER THAN NUCLEAR POWER PLANTS

10.1. HAZARD CATEGORIES AND GRADED APPROACH

The likelihood that an external event will give rise to radiological consequences depends on the characteristics of the nuclear installation (e.g. its use, design, construction, operation and layout) and on the event itself. Such characteristics include the following [14]:

(1) The amount, type and status of the radioactive inventory (e.g. solid, liquid and gaseous, processed and stored);

(2) The intrinsic hazard (e.g. criticality) associated with the physical processes and chemical processes that take place at the installation;

(3) The thermal power of the nuclear installation, if applicable;

(4) The configuration of the installation for activities of different kinds;

(5) The distribution of radioactive sources within the installation (e.g. in research reactors, most of the radioactive inventory will be in the reactor core and fuel storage pool, while in processing and storage facilities it may be distributed throughout the facility);

(6) The changing nature of the configuration and layout of installations designed for experiments;

(7) The engineered safety features necessary for preventing accidents and for mitigating the consequences of accidents, including the need for active safety systems and/or operator actions to prevent accidents and to mitigate the consequences of postulated accidents;

(8) The characteristics of the structures of the nuclear installations and the means of confinement of radioactive material;

(9) Any characteristics of the process or of the engineered safety features that might lead to a cliff edge effect in the event of an accident;

(10) The potential for on-site and off-site contamination.

The nuclear installations can be categorized into hazard categories based on the potential consequences of failures induced by external hazards. Four categories are considered in this publication:

- High hazard nuclear installations (e.g. NPPs);
- Medium hazard nuclear installations;
- Low hazard nuclear installations;
- Conventional installations.

Table 9 gives a qualitative description of the consequences of the external hazard induced failure associated with each category.

A graded approach may be taken to ensure that design criteria are commensurate with the consequences of the installation accidents due to the external hazard. If a graded approach is applied to the design of the installation against external events, design requirements and procedures will need to be commensurate with the hazard category assigned to the installation, as suggested in the last column of Table 9.

Simplified methods for external hazard assessment, based on a more restrictive data set associated with a lower return period, and which is applicable to medium and low hazard facilities, will need to be considered. The level of effort, complexity of analysis, and the thoroughness of documentation has to be commensurate with the magnitude of the radiological hazards associated with the installation accident conditions.

TABLE 9. HAZARD CATEGORY BASED ON THE CONSEQUENCES OF EXTERNAL HAZARD INDUCED FAILURE OF A NUCLEAR INSTALLATION

Category	On-site Consequences	Off-site Consequences	Engineering and Safety Analysis
High radiological hazard	Radiological or other exposures that might cause loss of life of workers in the facility.	Potential for significant off-site radiological and/or non-radiological consequences.	Similar rules as used for NPPs apply. Engineering and safety analyses are needed to determine the preventive and mitigating features and to determine if safety objectives are met.
Medium radiological hazard	Potential for significant on-site consequences. Unmitigated release would necessitate on-site evacuation.	Small potential for off-site radiological or non-radiological consequences. Radiological/toxicological exposures off the site would not be expected to cause health consequences but may require emergency plans.	Engineering and safety analyses are needed to determine if safety objectives are met.
Low radiological hazard	Potential for only localized consequences (within 30–100 m from the point of release).	Radiological/toxicological exposures off the site are small enough to require no warnings to public concerning health effects.	Limited engineering safety analyses are needed to determine if safety objectives are met. Conventional design codes with some enhancements.
No radiological hazard (conventional installations)	No radiological or chemical release but failure of the SSC could place workers at risk of physical injury.	No off-site radiological or non-radiological consequences.	Conventional design codes and practices.

10.2. PERFORMANCE OBJECTIVES

The general framework to assess design robustness presented in Sections 2, 5, 6 and 7 for NPPs is dependent on the performance objectives set for the different external hazards. Thus, the general framework is applicable to installations other than NPPs once performance objectives are defined for them.

Table 10 (taken from SSG-67 [14]) provides suggested performance goals (i.e. annual frequency based performance objectives) for the radiological hazard categories defined in Table 9. These are directly applicable to assess adequacy of the design margins of the installation, for external hazards in categories A and B (see Section 6.1).

For external hazards in Category C, a scenario based performance objective will need to be defined, as for NPPs. Robustness will be adequate if the installation meets the objectives for the given scenario.

TABLE 10. SUGGESTED PERFORMANCE GOALS FOR EACH INSTALLATION RADIOLOGICAL HAZARD CATEGORY

Category	Design Codes and Standards	Design Hazard Level	Performance Goal for External Hazards
High radiological hazard	Nuclear	10^{-4} per year	Frequency of failure < 10^{-5} yr^{-1}
Medium radiological hazard	Nuclear, with some relaxation	10^{-3} per year	Frequency of failure < 10^{-4} yr^{-1}
Low radiological hazard	Conventional, with enhancements	National hazard code, for critical facilities	Frequency of failure < 5×10^{-4} yr^{-1}
No radiological hazard (conventional installations)	Conventional	National hazard code	Frequency of failure < 10^{-3} yr^{-1}

10.3. ASSESSMENT OF PERFORMANCE

Assessment of performance for the different external hazards may follow the general guidance given in Section 5 (seismic hazard) and Section 6 (other hazards). The level of effort has to be commensurate with the radiological hazard category of the nuclear installation. For this purpose, simplifications may be introduced in the general methodologies used for NPPs (see, for example, Safety Reports Series No. 94, Approaches to Safety Evaluation of New and Existing Research Reactor Facilities in Relation to External Events [8], for research reactors).

11. CONCLUSIONS

As it can be inferred from design practices (Section 4) and has been demonstrated by the available operating experience (Section 3), design margins against beyond design basis external events are present in nuclear installations.

In the light of the Fukushima Daiichi accident, which occurred in March 2011, the IAEA established revised safety requirements. To comply with them, an assessment has to be performed to evaluate the 'adequacy' of those design margins to protect nuclear installations against external events more severe than those selected for the design basis, and to avoid cliff edge effects. In current IAEA publications, limited guidance is provided to assess quantitively the adequacy of these margins.

In order to facilitate the practical application of the revised requirements, Sections 5 and 6 present a general framework and quantitative criteria for defining what design safety margins against external hazards are 'adequate'. Additionally, practical guidance and information are provided in Section 7 to identify the external hazard severity corresponding to the onset of cliff edge effects, using qualitative and quantitative approaches, and to assess the adequacy of the margins against them.

The strategy of the present publication is to look first to seismic hazard, for which well developed and practiced methods for hazard assessment and design margin assessment are available. For this hazard, it was shown that the design margin can be linked to the installation-level performance against the hazard, that is, its annual frequency of seismic induced failure (Section 5). The consequence is that the design margin will be 'adequate' if it results in compliance with the frequency based installation-level performance goals set by the regulatory body. This is a quantitative definition of 'adequacy'.

To generalize this approach to other external hazards, the present publication distinguishes between three categories of hazard (Section 6). Hazards in the first category, Category A, are conceptually similar to seismic hazard, in the sense that hazard severity can be defined using a single parameter (e.g. ground acceleration, wind speed, water level) for which an AFE can be assessed following established practices. Therefore, for hazards in this category, the approach for assessing design margin adequacy defined for seismic hazard remains valid, even though practical methods of hazard assessment and design margin determination are less developed.

At the other end of the hazard category scheme, Category C hazards are scenario based hazards. Realizations (events) representing these hazards are introduced in an agnostic way in the design process, that is, there is no annual frequency explicitly or implicitly associated with them. The severity of these 'scenario based' hazard cannot be defined using a single parameter and, therefore, it needs the definition of a set of parameters which, all together, define the severity.

For external hazards in Category C, the events considered in the design process are specified deterministically and the design needs to meet certain conditions if those events happen. Such conditions are expressed by engineering attributes, so that it can be demonstrated with adequate confidence that a severe accident and/or large release are avoided if the conditions are met. Thus, the concept of 'design margin' is less meaningful. For external hazards in Category C, acceptable behaviour (compliance with specified conditions) is used for assessing design robustness adequacy.

Category B hazards are in between categories A and C. Category B hazards are scenario based hazards, but AFEs can be determined for each scenario. In other words, instead of having a continuous function of the parameter defining the severity of the hazard as in Category A, there is a discrete number of scenarios, each one with an associated level of severity and annual frequency of occurrence. Thus, the same concept to assess adequacy for Category A hazards can be used. However, now the installation-level performance (i.e. the annual frequency of failure) needs to be obtained using a summatory instead of a convolution integral.

Regarding cliff edge effects (Section 7), an approach was presented to identify the presence of potential cliff edge failures qualitatively and quantitatively for a given design, in connection with seismic hazard. Several criteria to assess adequacy of the design margin with respect to it were proposed in Section 7.2. These criteria are based on the influence of the potential cliff edge failure mode on the installation-level performance. The corresponding design margin is considered adequate if the potential cliff edge failures have a limited contribution to the annual frequency of failure (on the order of 10% or less, where not specified by the regulatory body), or if the total annual frequency of failure meets the performance goals set by the regulatory body.

For other external hazards, the categorization into A, B or C hazard categories is used to generalize the cliff edge margin adequacy concepts developed for the seismic hazard.

The general framework summarized above is directly applicable to both new and existing nuclear installations as well as to nuclear installations other than NPPs, once the performance goals for these installations have been set by the national regulatory body.

APPENDIX: NUCLEAR INSTALLATIONS THAT HAVE EXPERIENCED SEVERE EXTERNAL EVENTS

A.1. SIGNIFICANT SEISMIC EVENTS

This section provides details of experience feedback of significant seismic events from existing nuclear installations.

A.1.1. Humboldt Bay nuclear power plant (1980)

The Humboldt Bay Power Plant, Unit 3 was a 65 MWe[26] boiling water reactor just south of Eureka, California, that started operation in 1963.

On 8 November 1980, while the plant was in an extended outage, an earthquake of a reported surface wave magnitude of 7.0 occurred off the coast, at about 120 km from the site. Free field PGA at the site was between 0.20 and 0.25 *g* (horizontal).

The original plant DBE had 0.25 *g* PGA, which was upgraded in 1975 to 0.5 *g*. Significant modifications were implemented to structural steel and lateral restraint to piping.

No visible damage due to the earthquake was recorded at SSCs. The reconnaissance team of the U.S. NRC concluded that the effects of the earthquake on the plant were minimal and did not endanger the health and safety of the public [45].

A.1.2. Perry nuclear power plant (1986)

The Perry nuclear power plant is a BWR-6 General Electric reactor, with a Mark III containment design and 1300 MWe. It is located on the coast of Lake Eire, 64 km northeast of Cleveland, Ohio, in the United States of America.

On 31 January 1986, before the commissioning of the plant[27], an earthquake of magnitude 5.0 occurred at about 17 km south off the site, which generated relatively high accelerations (0.18–0.19 *g*) of short duration at the site [46]. The strong motion duration of the earthquake was 1 second with a total earthquake duration of 2.7 seconds.

The PGA at the site was 0.19 *g*, which was higher than the design value of 0.15 *g* [47]. The cumulative absolute velocity (CAV) parameter registered a value of 0.08 *g* sec, which is well under the value of 0.16 *g* sec, normally considered as a threshold for the potential onset of relevant damage in an NPP. Relative displacement between basemat and containment shell was 0.1 cm while the design value was 0.36 cm.

Inspection teams were dispatched into the plant, just after the earthquake, to survey for any major damage. Detailed plant walkdowns were performed, which did not find damage to any structure, system or component. The plant systems, both safety and non-safety related, operated properly during and following the seismic event.

A.1.3. Kashiwazaki-Kariwa nuclear power plant (2007)

The Kashiwazaki-Kariwa nuclear power plant, on the West Coast of Japan, is one of the largest in the world. It has seven units, with a total of 7965 MWe installed power. Five units are boiling water reactors (BWRs), each with 1100 MWe. The other two reactors are advanced boiling water reactors (ABWRs), each with 1356 MWe. The BWR units entered commercial operation between 1985 and 1994, whereas

[26] Reactor powers are given as gross electrical capacities (MWe).
[27] Official date of commissioning of the plant is November 1987.

the ABWR units were connected to the grid in 1996 and 1997, respectively. The site covers an area of 4.2 km^2.

On 16 July 2007, an earthquake with moment magnitude 6.6 occurred off the coast, with epicentre at about 16 km from the site (Niigata-Ken Chuetsu-Oki earthquake). The effects of this earthquake on the plant have been studied by many experts and organizations, including three expert missions of the IAEA. The details can be found elsewhere [48]. What follows is a brief summary of the points that are relevant in the framework of the present publication.

At the time of the earthquake, four reactors were in operation (Units 2, 3, 4 and 7) and three were in a shutdown condition for scheduled outages (Units 1, 5 and 6). Automatic seismic reactor trip systems were activated in all units and all reactors in operation were immediately shut down.

The strong motion duration of the earthquake was about 8 seconds. The largest PGA at free field surface in the horizontal direction was 1.25 *g* (E-W), and in the vertical direction, 0.73 *g*. These values cannot be directly compared with design values since the Japanese S2 DBE was specified at a virtual bedrock outcrop[28]. The S2 DBE was specified as a broadband response spectrum with 0.45 *g* zero-period ground acceleration. Deconvolving ground surface records to the bedrock at which the DBE had been specified resulted in large exceedances of the design basis horizontal spectrum, especially for Unit 1, in the E-W direction and for frequencies above 7 Hz. In this case, a deconvolved zero-period ground acceleration of about 1.8 *g* was obtained by the plant owner.

TABLE A.1. MAXIMUM ACCELERATION VALUES OBSERVED AT BASEMAT SLABS OF REACTOR BUILDINGS OF UNITS 1–7 OF THE KASHIWAZAKI-KARIWA NPP – COMPARISON WITH VALUES DERIVED FROM DESIGN BASIS (see Refs [48] and [11])

Unit	Maximum recorded acceleration (Gal)			Maximum response acceleration (Gal)			Static horizontal acceleration (Gal)
				Derived from design basis (S2)			
	N-S	E-W	U-D	N-S	E-W	U-D	
1	311	680	408	274	273	408	
2	304	606	282	167	167	282	
3	308	384	311	192	193	311	
4	310	492	337	193	194	337	470
5	277	442	205	249	254	205	
6	271	322	488	263	263	488	
7	267	356	355	263	263	355	

Table A.1 gives the maximum accelerations recorded at the basemat of the reactor buildings. Maximum acceleration values of 0.32 *g* (Unit 6) to 0.68 *g* (Unit 1) in the horizontal E-W direction, and of 0.21 *g* (Unit 5) to 0.49 *g* (Unit 6) in vertical, were recorded. These values are to be compared with the dynamic

[28] For safety related SSCs, Japanese seismic design practice, as described in standard JEAG 4601-1987 (English translation in NUREG/CR-6241), considers three load cases and chooses the most conservative result. The three cases are: (1) Equivalent static analysis, with an equivalent horizontal acceleration (470 Gal in the case of Kashiwazaki-Kariwa NPP); (2) Dynamic seismic forces for design earthquake S1, maximum design earthquake, for which the response needs to be kept within the linear range; and (3) Dynamic seismic forces for design earthquake S2, extreme design earthquake, for which the response can exhibit small non-linearities (e.g. uplift of basemat, small non-recoverable deformation in shear walls).

S2 design values included in Table A.1, which are between 0.17 *g* (Unit 2) and 0.26 *g* (Units 6 and 7) in the horizontal direction. Comparison with the design basis response spectra at the basemats showed that there were significant exceedances of the S2 DBE for a very wide range of spectral frequencies [48], especially in the horizontal E-W direction.

The very thorough post-earthquake inspections, performed by the plant owner and confirmed by other independent organizations, concluded that despite the significant exceedance of seismic design parameters, the earthquake did not cause relevant damage to safety related SSCs in any of the seven units. The only effect with some radiological consequences was the sloshing of the spent fuel pool water into the reactor building operating floor of Unit 6 and subsequent leakage through cable penetrations into the radiological non-controlled area, where the drainage system discharged the water into the sea.

On the other hand, the earthquake caused widespread damage all over the site, affecting non-safety related items. Damage included generalized soil failures, which severely affected access roads, buried piping of the fire protection system, supports of exhaust ducts, and the anchorage of some equipment items. A minor fire broke out in a non-safety related transformer located outdoors.

Damage was also found in the shaft of the main turbine of Units 5 and 7, which experienced displacements that render the turbine inoperable. Damage concentrated in thrust bearings of the turbine rotor [12].

Even though the dynamic S2 DBE for the Kashiwazaki-Kariwa site was significantly exceeded, the static analysis for the equivalent static acceleration value specified for the plant (470 Gal, corresponding to 0.479 *g*) leads to story shear forces in the same order of magnitude, or even larger, than those derived from accelerations recorded at the different elevations, at least in Unit 7 [11]. Hence, caution has to be exercised when extrapolating this experience to other Member States: the loads induced by the earthquake on SSCs may not have exceeded the equivalent static loading conditions to the same degree as the dynamic S2 DBE was exceeded [12].

A.1.4. Hamaoka nuclear power plant (2009)

The Hamaoka nuclear power plant, on the East Coast of Japan, comprises five units. Units 1 and 2 are BWR Mark II reactors that started operation in the late 1970s and went into permanent shutdown in January 2009. Units 3 and 4 are BWR-5 advanced Mark II reactors, with 1100 and 1137 MWe, respectively. Unit 5 is an advanced BWR (ABWR) reactor, with 1380 MWe.

On 11 August 2009, an earthquake with a Japan Meteorological Agency (JMA) magnitude of 6.5 occurred, with epicentre at about 37 km off the site (Suruga Bay earthquake). At the time of the earthquake, Units 4 and 5 were at full power operation. Unit 3 was in outage, under scheduled maintenance. Automatic seismic reactor trip systems were activated in all units and the reactors in operation were immediately shut down.

The main shock lasted for about 3 seconds [49]. Maximum accelerations at the reactor building basemat ranged from 0.11 *g* (Unit 1, E-W horizontal) to 0.45 *g* (Unit 5, E-W horizontal). Vertical accelerations ranged from 0.03 *g* (Unit 2) to 0.084 *g* (Unit 5). These values were smaller than seismic design basis values (about 0.6 *g* for the Japanese S2 DBE). Motions induced by the earthquake in Unit 5 were far larger than in the other units, due to local site effects [49].

Inspection of Units 3 and 4 revealed no relevant damage. Those units were restarted within two months after the earthquake.

On the contrary, damage was found in the shaft of the main turbine of Unit 5, which experienced displacements that render the turbine inoperable. Damage concentrated in thrust bearings and thrust keys [12]. After the necessary repairs, Unit 5 was restarted in January 2011.

A.1.5. Fukushima Daiichi nuclear power plant (2011)

The Fukushima Daiichi nuclear power plant site, on the East Coast of Japan, included six BWR units. Unit 1 was a BWR-3 Mark I reactor (460 MWe), Units 2 to 5 were BWR-4 Mark I reactors (784 MWe) and Unit 6 was a BWR-5 Mark II reactor (1100 MWe). Unit 1 was connected to the grid in 1970, and all other units were built and put into operation in the 1970s.

On 11 March 2011, a moment magnitude 9.0 earthquake occurred along the Pacific Coast of Tohoku (Great East Japan earthquake or Off-the-Pacific-Coast-of-Tohoku earthquake), whose rupture zone had an extension of about 500 × 200 kilometres and a minimum distance of about 180 km off the site. At the site, the strong motion lasted for 70 seconds, with a total earthquake duration of about 120 seconds. The events after the earthquake, which eventually caused a major nuclear accident, have been extensively studied in the past decade by many organizations. The IAEA published a comprehensive report [50]. What follows is a brief summary of the points that are relevant in the framework of the present publication.

At the time of the earthquake, Units 1 and 3 were operating at full power, Unit 2 was in startup operation after scheduled outage, Unit 4 had its fuel off-loaded from the reactor vessel to the spent fuel pool, Units 5 and 6 were on outage. Automatic seismic reactor trip systems were triggered in all units and the reactors in operation were immediately shut down.

The earthquake caused damage to the on-site switchyard, leading to a loss of off-site power scenario and the startup of EDGs in all six units. Based on emergency power, RHR systems were started and, in line with procedures, post-earthquake inspections were initiated. All units responded to the earthquake as intended by the designers and as stipulated in the plant's procedures, with no signs of significant damage in safety related SSCs due to the earthquake motion.

Tsunami waves started reaching the site about 45 minutes after the earthquake. The wave reaching the site about 50 minutes after the earthquake overtopped the seawalls and inundated the site (see Section 3.2.1).

Table A.2 gives the maximum acceleration values observed at the basemat of all six units, together with the values derived from the dynamic seismic S2 DBE (1966) and from the earthquake used for seismic capacity assessment, denoted as Ss (2008)[29]. As mentioned before, Japanese seismic design practice, in addition to dynamic load cases S1 and S2, includes a static load case with a horizontal acceleration uniform along the height of the building. As already said for the Kashiwazaki-Kariwa nuclear power plant, caution has to be exercised when making a comparison of the recorded motions with the dynamic design basis (S2), since the equivalent static design level loading (470 Gal, corresponding to 0.479 *g*) might be the load case governing the design.

Horizontal acceleration values derived from the dynamic S2 DBE were exceeded in the basemat of basically all units, except for Unit 6. Exceedances were very significant in the east-west (E-W) direction.

[29] In 2008, after the Kashiwazaki-Kariwa event, a third earthquake Ss was introduced by the Japanese nuclear regulatory body, with the purpose of assessing safety against an earthquake larger than S2. As a result of this assessment, some plants introduced improvements, on a voluntary basis.

TABLE A.2. MAXIMUM ACCELERATION VALUES OBSERVED AT BASEMAT SLABS OF REACTOR BUILDINGS OF UNITS 1–6 OF THE FUKUSHIMA DAIICHI NPP – COMPARISON WITH VALUES DERIVED FROM DESIGN BASIS (1996) AND FROM 'BACK-CHECK' EARTHQUAKE (2008) [51]

Unit	Maximum recorded acceleration (Gal)			Maximum response acceleration (Gal)					Static horizontal acceleration (Gal)
				Derived from earthquake level used to assess plant safety (Ss)			Derived from design basis (S2)		
	N-S	E-W	U-D	N-S	E-W	U-D	N-S	E-W	
1	460	447	258	487	489	412	245		470
2	358	550	302	441	438	420	250		
3	322	507	231	449	441	429	291	275	
4	281	319	200	447	445	422	291	283	
5	311	548	256	452	452	427	294	255	
6	298	444	244	445	448	415	495	500	

On the other hand, if recorded accelerations are compared with the accelerations corresponding to the earthquake used for the 'back-check' or seismic safety assessment of the plant (Ss), it can be seen that 'back-check' accelerations were exceeded only in the basemat of Units 2, 3 and 5 in the east-west (E-W) direction. A similar exceedance is not observed in the north-south (N-S) and vertical (U-D) components, where a comfortable margin still remains between the reassessed motions and the observed accelerations. The owner reported that only minor upgrades had been introduced in the plant as a result of the 'back-check' assessment (e.g. piping supports) [51].

In any case, observed exceedances did not result in the loss of any safety function.

A.1.6. Fukushima Daini nuclear power plant (2011)

The Fukushima Daini nuclear power plant, in Japan, includes four units: one BWR-5 Mark II reactor (Unit 1) and three BWR-5 Mark II advanced reactors (Units 2, 3 and 4). All reactors have a power of 1100 MWe. The units started their commercial operation between 1982 (Unit 1) and 1987 (Unit 4).

The site is located on the shoreline, at about 12 km away from the Fukushima Daiichi site. Therefore, it was affected as well by the Great East Japan earthquake, or Off-the-Pacific-Coast-of-Tohoku earthquake, that occurred on 11 March 2011 (see Section A.1.5).

At the time of the earthquake, all four units were operating at full power. Automatic seismic reactor trip systems were triggered in all units and the reactors were immediately shut down. One off-site power source remained operable and RHR systems were started, as stipulated in plant's procedures. At the site, the strong motion lasted for 60 seconds, with a total earthquake duration of about 120 seconds.

Tsunami waves started reaching the site about 40 minutes after the earthquake. Tsunami waves overtopped the seawall and inundated seven of the eight seawater pump houses. Inundation surrounding the main buildings (reactor building and turbine building) was not significantly deep, with the exception of the south side of Unit 1 (see Section 3.2.1).

As can be seen in Table A.3, maximum accelerations recorded on the site were smaller than the seismic dynamic S2 design basis motions for Units 1 and 2, they slightly exceeded S2 motions in Unit 4, and exceedance was significant in Unit 3 in the horizontal north-south (N-S) direction [51]. On the other hand, values corresponding to the 'back-check' earthquake (Ss) were not exceeded. A static equivalent

acceleration of 0.479 *g* (470 Gal) was used for the design. The same considerations mentioned in Section A.1.5 about the need to be cautious when comparing recorded acceleration values with S2 design acceleration values to determine design basis exceedance apply here.

No damage to safety related SSCs due to the seismic motion was reported (see Refs [12] and [52]).

TABLE A.3. MAXIMUM ACCELERATION VALUES OBSERVED AT BASEMAT SLABS OF REACTOR BUILDINGS OF UNITS 1–4 OF THE FUKUSHIMA DAINI NPP – COMPARISON WITH VALUES DERIVED FROM DESIGN BASIS (1996) AND FROM 'BACK-CHECK' EARTHQUAKE (2008) [51]

Unit	Maximum recorded acceleration (Gal)			Maximum response acceleration (Gal)					Static horizontal acceleration (Gal)
				Derived from earthquake level used to assess plant safety (Ss)			Derived from design basis (S2)		
	N-S	E-W	U-D	N-S	E-W	U-D	N-S	E-W	
1	254	230	305	434	434	512	372	372	470
2	243	196	232	428	429	504	317	309	
3	277	216	208	428	430	504	196	192	
4	210	205	288	415	415	504	199	196	

A.1.7. Onagawa nuclear power plant (2011)

The Onagawa nuclear power plant, in Japan, has three BWR Mark I units, which started operation in 1984 (Unit 1, 524 MWe, BWR-4), 1995 (Unit 2, 825 MWe, BWR-5) and 2002 (Unit 3, 825 MWe, BWR-5), respectively.

Situated on the eastern coast of Japan, the Onagawa plant was the closest nuclear station to the epicentral area of the moment magnitude 9.0 earthquake that occurred along the Pacific Coast of Tohoku (Great East Japan earthquake or Off-the-Pacific-Coast-of-Tohoku earthquake) on 11 March 2011. The site is about 125 km away from the epicentral area. Due to its proximity to the earthquake source, the plant experienced the strongest shaking that any NPP has ever experienced from an earthquake. The IAEA carried out an expert mission to examine the performance of the plant during the earthquake [53]. What follows is a brief summary of the points that are relevant in the framework of the present publication.

At the time of the earthquake, Units 1 and 3 were operating at full power. Unit 2 was in startup operations, after a scheduled outage. Automatic seismic reactor trip systems were triggered in all units and the reactors were immediately shut down. One off-site power source remained operable and RHR systems were started, as stipulated in plant's procedures.

At the site, total earthquake duration was of about 160 seconds. There were two distinct strong motion periods. The first lasted for about 50 seconds. The second strong motion period, longer and stronger, lasted for about 80 seconds. Looking at the acceleration records, one would say that the plant was subjected to two consecutive strong earthquakes, separated by a time window of a few seconds [53].

No relevant damage to safety related SSCs was found during the inspections due to the earthquake motion. The three units achieved cold shutdown conditions, with all systems working as designed [53].

Minor cracking of concrete structures was identified during inspection walkdowns [53]. Small displacements were detected in the main steam turbine rotor at Units 2 and 3, which caused damage to the blades (see Refs [12] and [51]). In the turbine building of Unit 1, insulators in a medium voltage switchgear cabinet fractured and allowed contact of the bus bar with the cabinet enclosure. This led to a small fire in the cabinet.

Further studies revealed a loss of rigidity at the control and reactor buildings of Unit 2, with respect to the original values, that is, primary predominant frequencies were smaller than the ones previous to the earthquake. This fact was attributed to cracking or microcracking of the structural concrete (see Refs [54] and [55]). Those studies showed that the reinforcing bars remained in the elastic region during the earthquake. Hence, cracking posed no challenge to the structural safety of the buildings.

TABLE A.4. MAXIMUM ACCELERATION VALUES OBSERVED AT BASEMAT SLABS OF REACTOR BUILDINGS OF UNITS 1–3 OF THE ONAGAWA NPP – COMPARISON WITH VALUES DERIVED FROM DESIGN BASIS AND FROM 'BACK-CHECK' EARTHQUAKE (2008-2009) (see Refs [53] and [56])

Unit	Maximum recorded acceleration (Gal)			Maximum response acceleration (Gal)					Static horizontal acceleration (Gal)
				Derived from earthquake level used to assess safety (Ss)			Derived from design basis (S2)		
	N-S	E-W	U-D	N-S	E-W	U-D	N-S	E-W	
1	540	587	399	532	529	451	-[1]	-[1]	
2	607	461	389	594	572	490	363	363	470
3	573	458	321	512	497	476	375	375	

Note 1: Unit 1 was designed for an S1 earthquake with maximum acceleration of 250 Gal at the bedrock outcrop (278 Gal at the basemat) and for a static equivalent acceleration (470 Gal in the horizontal direction).

At the Onagawa site, the tsunami waves reached a height of 13.6 m, whereas the plant grade level had been chosen at elevation 14.8 m (13.8 m, after crustal subsidence caused by the earthquake). Therefore, only secondary floods took place, which could be addressed safely by the operators, with no safety consequences (see Section 3.2.1 below).

As can be seen in Table A.4, maximum accelerations recorded on the site exceeded design basis motions (S2) [53]. On the other hand, values corresponding to the 'back-check' earthquake (Ss) either were not exceeded or they were only barely exceeded. A static equivalent acceleration of 0.479 *g* (470 Gal) was used for the design. The same considerations mentioned in Section A.1.5 about the need to be cautious when comparing recorded acceleration values with S2 design acceleration values to determine design basis exceedance apply here.

Response spectra computed from acceleration signals recorded at the basemat of the reactor buildings showed small exceedances of the Ss earthquake spectra at frequency bands between 1 and 4 Hz and between 6 and 13 Hz [53]. Maximum exceedances were between 1.3 and 1.5 times the spectral ordinate for 5% damping.

The owner of the Onagawa plant voluntarily implemented the improvements derived from the 'back check' analysis performed for the new Ss earthquake. The improvement work was carried out in 2008–2009.

A.1.8. Tokai Daini nuclear power plant (2011)

The Tokai Daini site, in Japan, has a single BWR-5 1100 MWe reactor with a Mark II containment, which started commercial operation in 1978.

The moment magnitude 9.0 earthquake that occurred along the Pacific Coast of Tohoku (Great East Japan earthquake or Off-the-Pacific-Coast-of-Tohoku earthquake) on 11 March 2011 affected this plant, which is located at about 250 km from the epicentral area. At the time of the earthquake, Tokai Daini reactor was operating at full power. In response to the earthquake, the reactor automatically scrammed (rapid shutdown) [51]. At the site, the earthquake had a duration of about 30 seconds [12].

All three off-site power sources were lost and all three EDGs started automatically, providing power to the safety buses. About 30 minutes after the earthquake, tsunami waves started arriving at the site and eventually flooded the lower level of the site. One emergency diesel generator and one source of core cooling were lost, but the other sources remained operable, which eventually allowed the reactor to reach cold shutdown on 15 March.

The maximum acceleration of the earthquake was less than the design basis of the site [51]. Table A.5 provides the maximum accelerations recorded on the site. There was no relevant damage reported for safety related SSCs. A slight movement of the main steam turbine rotor was detected and a rod broke in an oil snubber connected to the turbine moisture separator [12].

TABLE A.5. MAXIMUM ACCELERATION VALUES OBSERVED AT BASEMAT SLAB OF REACTOR BUILDING OF THE TOKAI DAINI NPP – COMPARISON WITH VALUES DERIVED FROM DESIGN BASIS AND FROM 'BACK-CHECK' EARTHQUAKE [56]

Maximum recorded acceleration (Gal)			Maximum response acceleration (Gal)					Static horizontal acceleration (Gal)
			Derived from earthquake level used to assess safety (Ss)			Derived from design basis[1]		
N-S	E-W	U-D	N-S	E-W	U-D	N-S	E-W	
214	225	189	393	400	456	520	520	470

Note 1: Original dynamic design basis used real earthquake accelerograms (e.g. El Centro) scaled to a peak ground acceleration of 180 Gal.

A.1.9. North Anna nuclear power plant (2011)

The North Anna nuclear power plant, 65 km north-west of Richmond, Virginia (United States of America), has two three-loop pressurized water reactors (PWRs) of about 1000 MWe each. Unit 1 went on-line in 1978 and Unit 2 in 1980.

On 23 August 2011, an earthquake of magnitude 5.8 occurred at about 18 km west-southwest off the site, which generated relatively high accelerations (0.23 *g*) of short duration in the site [12]. The strong motion duration of the earthquake was 1 second with a total earthquake duration of about 2 seconds. It had a strong north-south directionality.

At the time of the earthquake, both units were operating at full power. The two reactors were automatically shut down by the reactor protection system (abnormal neutron flux rate) and the off-site power for the entire plant was lost upon the occurrence of the earthquake. The EDGs automatically started up, and both reactors reached cold shutdown conditions on 23 August (Unit 1) and 24 August (Unit 2), following plant procedures.

The PGA at the foundation of the Unit 1 reactor containment building was 0.23 *g* (north-south component), which was higher than the design value of 0.12 *g*. The response spectrum of the recorded acceleration signal in the north-south direction exceeded the design basis response spectrum at all frequencies greater than 1 Hz.

The CAV parameter for the north-south motion registered a value of 0.172 *g* sec, which is just above the value of 0.16 *g* sec, normally considered as a threshold for the potential onset of relevant damage in an NPP.

Seismic damage inspections started almost immediately after the occurrence of the earthquake. Very thorough inspections and analyses were performed in the following weeks, which led to the conclusion that no relevant damage had been induced by the earthquake in safety related SSCs. Commercial operation of the plant was resumed about three months after the earthquake.

A.2. SIGNIFICANT FLOOD EVENTS

This section provides details on lessons learned from existing nuclear installations that have experienced significant flooding events in the past.

A.2.1. Le Blayais nuclear power plant – Flood (1999)

The Le Blayais nuclear power plant, 50 km north-west of Bordeaux, on the banks of the Gironde estuary, in France, has four PWRs of 950 MWe each, which started operation between 1981 and 1983.

The plant grade level is at 4.5 m above the French national datum (NGF). The site is surrounded by a dike. The dike is an earthen structure and it is riveted along the Gironde estuary side by stone blocks (riprap). Alongside the Gironde estuary, the height of the dike was 5.2 m NGF, whereas it was 4.75 m NGF at the other sides. The design river flood level for the protection of the site was 5.02 m NGF. During the periodic safety review presented in 1998 to the regulatory body, the owner reassessed the design river flood level to be 5.46 m NGF and planned to increase the height of the dike up to 5.70 m NGF in year 2000 [57].

In the evening of 27 December 1999, Units 1, 2 and 4 were operating at full power. Reactor in Unit 3 was shut down, after a refuelling outage. Before the flooding event, Units 2 and 4 experienced a loss of off-site power event caused by damage in the 225 kV and 400 kV grids due to the strong windstorm. These two units shut down automatically and the EDGs started up and operated correctly. The 400 kV grid feeding Units 1 and 3 remained in operation [57].

During the night of 27–28 December 1999, high waves, caused by a combination of tides and exceptionally high winds, moved up the Gironde estuary and flooded the plant platform. In the initial stages of the flooding event, flood debris carried up the river by the high tide blocked the intake for circulating water pumps of Unit 1 and resulted in the automatic shutdown of the reactor in this unit. At 00:30 h on 28 December, all reactors were in a shutdown condition. During the flooding event, the waves moved the rock blocks protecting the earth structure of the dike and part of it was washed away down the river. The water reached a depth of around 30 cm in the northwest corner of the site (see Annex III of Technical Volume 2 of Ref. [50]). Investigations carried out on the site after the flood showed that the water had overtopped obstacles from 5.0 to 5.3 m NGF in height.

The water went into the underground gallery of the site mainly through the maintenance openings at the plant grade level [57]. This gallery is located outside the main buildings and almost surrounds them. Water flows developed from this gallery into the buildings due to hydrostatic pressure on the penetrations. Units 1 and 2 were affected by the incoming water. The following spaces were flooded in Units 1 and 2:

- Rooms containing the ESW pumps. In Unit 1, the ESW system pumps of train A were lost as a result of the immersion of their motors. The ESW system of each unit comprises four pumps on two independent trains, A and B. Each pump is capable of providing the entire throughput required. Train B remained operable.
- The bottom of the fuel building of Units 1 and 2 containing the cells of the two low head safety injection pumps and the two containment spray system pumps, which were rendered unavailable.
- Some utility galleries, particularly those running in the vicinity of the fuel building linking the pump house to the platform.
- Some rooms containing outgoing electrical feeders. The presence of water in these rooms led indirectly to the unavailability of some electrical switchboards.

Hence, even though the flood affected important safety related systems in Unit 1, redundancy of the ESW system allowed to cope with the emergency situation. Other systems which could have been used to cool down the reactor, such as the emergency feedwater system, remained operable.
Units 3 and 4 were basically not affected by the flooding event. Unit 3 was kept in cold shutdown by the shutdown cooling system. After recovery of the auxiliary 225 kV grid, Unit 4 was restarted and connected again to the grid on 30 December 1999.

The flooding event resulted from the concurrence of the following phenomena:

- Tide level: high but not an extreme tide amplitude (tide coefficient 77);
- Storm surge: extreme event, which was equivalent to the calculated 1000-year return period event (2.01 m). The maximum level measured prior to 27 December 1999 was 1.20 m, for a 40-year historical series of data;
- Wind speed: extreme event (maximum ten-minute average wind speed of about 100 km/h at 10 m height);
- Wind waves: extreme event (significant wave height estimated at 2.00 m at the site, no measurement of this parameter in the estuary).

A.2.2. Madras nuclear power plant – Flood (2004)

The Madras nuclear power plant, located at Kalpakkam, on the south-east coast of India, has two pressurized heavy water reactors (PHWRs) of 235 MWe each. Plant grade is about 4.5 m above mean sea level, but the pump house operating floor is located only about 2.5 m above mean sea level (Annex III of Technical Volume 2 of Ref. [50]).

The site was affected by the tsunami generated by the 26 December 2004, magnitude 9.1, earthquake that occurred off the western coast of Sumatra.

When the tsunami reached the plant, Unit 2 was operating at full power, whereas Unit 1 was under extended outage. Maximum runup of the tsunami at the site was 4.5 m above mean sea level [58]. When the tsunami struck, the circulating water pumps of Unit 2 were affected by flooding of the pump house and subsequent submerging of the seawater pumps. Following this, the reactor tripped automatically, and it was brought to cold shutdown using the emergency operating procedure.

The pump house is connected by a submarine tunnel about 500 m long to the intake well. The increase in water level in the pump house during the tsunami rendered all the seawater pumps located in this area inoperable except for one process seawater pump. This pump was used to cool the plant heat loads in the initial period following reactor shutdown. Later, this pump also became unserviceable due to clogging of the travelling water screen in the seawater pump house because of the ingress of large quantities of debris from the tsunami. Afterwards, cooling was achieved by using the firewater system.

Though the off-site power remained available throughout the event, EDGs were started and were kept running as a precautionary measure. The tsunami did not affect Unit 1.

The vital areas of the plant such as the reactor building, turbine building, service building, switchyard and ancillary systems were unaffected by the tsunami. The damage caused by the tsunami was limited to the peripheral areas.

After restoration of the affected areas, Unit 1 was restarted on 1 January 2005.

A.2.3. Fukushima Daiichi nuclear power plant (2011)

The Fukushima Daiichi nuclear power plant site included six BWR units. Unit 1 was a BWR-3 Mark I reactor (460 MWe), Units 2 to 5 were BWR-4 Mark I reactors (784 MWe) and Unit 6 was a BWR-5

Mark II reactor (1100 MWe). Unit 1 was connected to the grid in 1970 and all other units were built and set into operation in the 1970s.

In Units 1 to 4, the plant grade level around main buildings was set at elevation 10.0 m with respect to the datum elevation at Onahama Port (OP). In Units 5 and 6, the plant grade level around main buildings was set at elevation OP+13 m.

The design maximum tsunami height was specified as OP+3.12 m [50]. Corresponding to this value, OP+4.00 m was selected as the level for locating the safety related SSCs at the water intake area, corresponding to the location of the seawater cooling pumps (pump motors). The top of seawalls protecting the intakes was set at OP+5.5 m.

On 11 March 2011, a moment magnitude 9.0 earthquake occurred along the Pacific Coast of Tohoku (Great East Japan earthquake or Off-the-Pacific-Coast-of-Tohoku earthquake). The events after the earthquake, which eventually caused a major nuclear accident, have been extensively studied in the past decade, by many organizations. The IAEA published a comprehensive report [50]. What follows is a brief summary of the relevant points, in the framework of the present publication.

At the time of the earthquake, Units 1 and 3 were operating at full power, Unit 2 was in startup operation after scheduled outage, Unit 4 had its fuel off-loaded from the reactor vessel to the spent fuel pool, Units 5 and 6 were on outage. Automatic seismic reactor trip systems were triggered in all units and the reactors in operation were immediately shut down.

The earthquake led to a loss of off-site power scenario and the startup of EDGs in all six units. Based on emergency power, RHR systems were started. All units responded to the earthquake as intended by the design, with no signs of significant damage in safety related SSCs due to the earthquake motion.

Tsunami waves started reaching the site about 45 minutes after the earthquake. The wave reaching the site about 50 minutes after the earthquake, which had a runup height of 14–15 m, overtopped the seawalls and inundated the site [50]. It engulfed all structures and equipment located at the seafront, as well as the main buildings (including the reactor, turbine and service buildings) at higher elevations:

- The wave flooded and damaged the seawater pumps and motors of all six units at the seawater intake locations on the shoreline, resulting in a loss of UHS event for all units.
- Water entered and flooded the main buildings, including all the reactor and turbine buildings, the common spent fuel storage building and diesel generator building. It damaged the buildings and the electrical and mechanical equipment inside at ground level and on the lower floors. The damaged equipment included the EDGs or their associated power connections, power distribution panels and switchgear equipment, which resulted in the loss of emergency AC power in all units, except for Unit 6. This led to a station blackout scenario in Units 1 through 5.
- DC power sources in Units 1, 2 and 4, including batteries, power panels and connections, were inundated. As a consequence, DC power was also gradually lost in Units 1, 2 and 4, during the first 10–15 minutes of the flooding. After this time, operators were no longer able to monitor essential plant parameters.

Eventually, as described in detail by Ref. [50], the damage caused by this massive flooding of the site led to core damage in several of the units, and serious difficulties to cool some of the spent fuel pools.

A.2.4. Fukushima Daini nuclear power plant (2011)

The Fukushima Daini nuclear power plant, in Japan, includes four units: one BWR-5 Mark II reactor (Unit 1) and three BWR-5 Mark II advanced reactors (Units 2, 3 and 4). All reactors have a power of 1100 MWe. All units started commercial operation between 1982 (Unit 1) and 1987 (Unit 4).

The site is located on the shoreline, at about 12 km away from the Fukushima Daiichi site. Therefore, it was affected as well by the tsunami waves caused by the Great East Japan earthquake, or Off-the-Pacific-Coast-of-Tohoku earthquake, that occurred on 11 March 2011 (see previous section).

Plant grade level around main buildings was set at elevation OP+12 m [50]. Original design maximum tsunami height was specified as OP+3.7 m [50]. Corresponding to this value, OP+4.3 m was selected as the level for locating the safety related SSCs at the water intake area, which are housed by the heat exchanger buildings. These buildings house components of the RHR and emergency cooling water systems which, therefore, are not directly exposed to tsunami waves.

The design maximum tsunami height was reassessed to OP+5.2 in the 2000s, using the new Japan Society of Civil Engineers (JSCE) methodology [50]. As a result, heat exchanger buildings were made watertight.

At the time of the earthquake, all four units were operating at full power. Automatic seismic reactor trip systems were triggered in all units and the reactors were immediately shut down. One off-site power source remained operable and RHR systems were started, as stipulated in plant's procedures.

Tsunami waves started reaching the site about 40 minutes after the earthquake. Tsunami waves inundated the platform of the heat exchanger buildings. Maximum tsunami height was OP+9.1 m, less than the main plant grade level (OP+12 m), but maximum runup heights reaching about OP+14.5 m were observed. Inundation surrounding the main buildings (reactor building and turbine building) was caused only by the runup waves and it was therefore not significantly deep, with the exception of the south side of Unit 1.

The tsunami waves damaged the equipment hatch doors of seven of the eight heat exchanger buildings [52]. Entry of water into these buildings, which housed the seawater pumps and electric power centres, caused the loss of core cooling functions and pressure suppression functions in Units 1, 2 and 4 [50]. The runup wave that reached the reactor building of Unit 1 flooded its EDGs. Unit 3 was the least affected and, since it maintained the UHS, it was able to reach cold shutdown the day after the earthquake.

Because the extent of damage caused by the tsunami was not as great as at the Fukushima Daiichi site, the plant superintendent had more options for dealing with the effects of the tsunami. Most of the normal emergency core cooling systems were rendered out of service by the tsunami, either due to the loss of the UHS (at the heat exchanger buildings) or damage to electrical systems. However, plant operators were able to continue to provide water to the reactor cores with the reactor core isolation cooling (RCIC) system and the make-up water condensate (MUWC) system. The latter is usually considered a non-safety related system.

The plant superintendent called for mobile power trucks and mobilized the workers on the site to lay more than 9 km of temporary power cables in 16 hours, to restore power in the damaged heat exchanger buildings. In addition, replacement motors were procured for some of the flooded pumps in Units 1 and 4. This allowed the normal RHR systems to be returned to service three days following the tsunami, and Units 1, 2 and 4 were brought to cold shutdown either on the same day or the day after RHR had been restored.

A.2.5. Tokai Daini nuclear power plant (2011)

The Tokai Daini site, in Japan, has a single BWR-5 1100 MWe reactor with a Mark II containment, which started commercial operation in 1978.

For the original design (1971), a maximum tsunami height of HP+2.35 m was assessed (HP=Hitachi Port datum)[30] [59]. The plant grade level was set at HP+8.9 m. Emergency seawater pumps were mounted at a much lower elevation: the platform for accessing the motors was set at about HP+3.0 m. Nevertheless, this platform was protected by concrete side walls, with their top at HP+5.80 m.

The tsunami hazard was reassessed in 2002, using the JSCE method, which led to a new estimate of the maximum tsunami height at HP+5.75 m. This maximum height was smaller than the top of the walls protecting the emergency seawater pumps and no countermeasures were required.

The tsunami hazard was reassessed again in 2007 by the Ibaraki prefecture, who estimated the maximum tsunami height at HP+6.61 m. The owner of the plant voluntarily decided to increase the height of the walls protecting the seawater pumps up to HP+7.00 m. On 11 March 2011, this retrofit was essentially completed, except for the sealing work at one of the two bays housing the pumps [59].

The moment magnitude 9.0 earthquake that occurred along the Pacific Coast of Tohoku (Great East Japan earthquake or Off-the-Pacific-Coast-of-Tohoku earthquake) on 11 March 2011 affected this plant, which is located at about 250 km from the epicentral area. At the time of the earthquake, the Tokai Daini reactor was operating at full power. In response to the earthquake, the reactor automatically scrammed (rapid shutdown) [51]. All three off-site power sources were lost, and all three EDGs started automatically, providing power to the safety buses.

About 30 minutes after the earthquake, tsunami waves started arriving and flooded the lower level of the site. The maximum tsunami height at the site was HP+5.50 m, with maximum runups up to HP+6.20 m [59]. The tsunami inundated the seawater pump bay which had some pending sealing work and, therefore, was not watertight. This caused the loss of one of the EDGs and its associated electrical loads. The other seawater pump bay had been upgraded to be watertight and was not flooded by the tsunami. As a result, only one EDG and one source of core cooling were lost, but the other sources remained operable, which eventually allowed the reactor to reach cold shutdown on 15 March.

A.2.6. Onagawa nuclear power plant (2011)

The Onagawa nuclear power plant, in Japan, has three BWR Mark I units, which started operation in 1984 (Unit 1, 524 MWe, BWR-4), 1995 (Unit 2, 825 MWe, BWR-5) and 2002 (Unit 3, 825 MWe, BWR-5), respectively.

For the design of Unit 1 (1970), a maximum tsunami height of OP+2 m to OP+3 m was assessed [59]. For the design of Unit 2 (1987), the maximum tsunami height was assessed as OP+9.1 m [59]. In any case, the plant grade level was set at OP+14.8 m for all units.

The bottom of the pits for emergency seawater pumps was set at a much lower elevation: the platform for accessing the motors was set at OP+3.0 m [53]. However, the pits were surrounded at all sides by the plant platform at OP+14.8 m.

The tsunami hazard was reassessed in 2002, using the JSCE method, which led to a new estimate of the maximum tsunami height at OP+13.6 m. This maximum height was smaller than the selected plant grade and no countermeasures were required.

Situated on the eastern coast of Japan, the Onagawa plant was the closest nuclear station to the epicentral area of the moment magnitude 9.0 earthquake that occurred along the Pacific Coast of Tohoku (Great East Japan earthquake or Off-the-Pacific-Coast-of-Tohoku earthquake) on 11 March 2011. The site is about 125 km away from the epicentral area.

[30] Hitachi Port (HP) datum is 0.89 m below Tokyo Peil (TP) datum. Hence, '0.00 m HP' means '-0.89 m TP'. Hitachi Port (HP) datum is 0.15 m below Onahama Port (OP) datum. Hence, '0.00 m HP' means '-0.15 m OP'.

At the time of the earthquake, Units 1 and 3 were operating at full power. Unit 2 was in startup operations, after a scheduled outage. Automatic seismic reactor trip systems were triggered in all units and the reactors were immediately shut down. One off-site power source remained operable and RHR systems were started, as stipulated in the plant's procedures.

After the earthquake, the elevation OP+14.8 m of plant grade was reduced to about OP+13.8 m, due to crustal subsidence caused by the earthquake in the area.

The first tsunami wave arrived at the site approximately 45 minutes after the earthquake [50]. The maximum observed tsunami height (tide gage) was about OP+13 m [59]. Even though the plant platform elevation 'dropped' from 14.8 m to 13.8 m as a result of the earthquake, the elevation was still adequate to prevent the site from being inundated [50].

However, a secondary tsunami induced flooding at Unit 2 took place. Hydrostatic pressure differences between the seawater pump pit (OP+3.0 m) and the tsunami wave (OP+13 m) caused seawater to flow through penetrations in the seawater pump pit floor. Once in the pit, the water flowed through a pipe and/or cable tray trench into the reactor auxiliary building area basement, and flooded train B of the reactor building closed cooling water system heat exchanger and pump room, and the high pressure heat exchanger and pump room used for cooling high pressure core spray auxiliary components. The flood ultimately caused the shutdown of train B of the EDGs and train B high pressure core spray diesel generator. Trains A of these safety systems were not affected by the flooding. Therefore, this secondary flood eventually had no safety consequences.

A.2.7. Fort Calhoun nuclear power plant – Flood (2011)

The Fort Calhoun nuclear power plant, in Nebraska, United States of America, had a PWR of 512 MWe. The plant site is adjacent to the Missouri River, at Blair, about 30 km north of Omaha. The plant started operation in 1973 and it was permanently shut down for decommissioning in 2016. The following data about flood design levels and reassessment of these levels is taken from Ref. [60].

The plant grade was set at 306 m MSL, which is not substantially higher than normal river levels. The design flood elevation was 306.6 m MSL. Without any special provision, safety related components in the plant were protected by hardened features up to a flood height of 307 m MSL. The intake structure was located at an elevation of 307.1 m MSL.

River flood levels were reassessed in 1993 by the U.S. Army Corps of Engineers, using the 'probable maximum flood' concept, to be 307.6 m MSL, with no upstream dam failures. Consequently, floodgates were permanently mounted adjacent to openings, which could be quickly set into position to provide further flood protection of most components up to an elevation of 307.7 m MSL. Protection of the intake structure to an elevation of 307.7 m MSL was accomplished through a combination of floodgates and sandbags. In the 2010 updated safety analysis report, the plant owner indicated that it would use sandbags, temporary earth levees and other methods to allow safe shutdown up to a water elevation of 308.8 m MSL [60].

In June 2011, the Missouri river underwent an extraordinary flood, which developed along several weeks. The owner sent a first notification ('unusual event') to the regulatory body on 6 June 2011, stating that the river was above a warning level stage and expected to rise further. The plant was in a refuelling outage since April. The reactor was shut down.

The river reached its peak stage at the nearby hydrologic station at Blair (about 4 km upstream of the plant) on 29 June 2011. The recorded peak stage at this station was 308.1 m MSL (1010.20 ft above NAVD88[31]). From this peak onwards, the river stage descended very slowly and with occasional new smaller peaks during July and August. River stage returned to values below the flood stage defined by the U.S. National Weather Service in mid-September.

[31] See https://water.weather.gov/ahps2/hydrograph.php?wfo=oax&gage=blan1

Apart from the floodgates and sandbags considered in the safety assessments, during the flood event the operators installed a long rubber water filled berm surrounding the main plant buildings. It was a 2.40 m (8 ft) high berm, which offered protection up to 308.4 m MSL stage of the river. However, this berm was punctured by a 'BobCat' vehicle during plant operations and deflated on 26 June 2011, when the river at the site was reported at the 306.7 m MSL elevation [61]. The collapse of the berm allowed floodwaters to surround the main electrical transformers and operators transferred power from off-site sources to the EDGs as a precautionary measure [61]. After rupture of the berm, protection was provided only with sandbags and the pumping out of water that seeped in.

Maximum river stage at the site was in the order of 307 m MSL. Fundamental safety functions were kept during the flood event, even though access to the plant was severely impaired during weeks.

A.3. SIGNIFICANT EXTREME WEATHER EVENTS

This section provides details on lessons learned from existing nuclear installations that have experienced significant extreme weather events in the past.

A.3.1. Saint Laurent des Eaux nuclear power plant – Ice blockage (1987)

The Saint-Laurent nuclear power plant is located on the Loire river, in France, upstream of the city of Blois and downstream of Orleans. The site has two PWRs of 915 MWe each, Units B1 and B2, both of which started operation in 1981. In addition, it used to have two natural uranium graphite-gas cooled reactors, which were brought into service in 1969 (Unit A1, 500 MWe) and 1971 (Unit A2, 530 MWe). The gas cooled reactors were permanently shut down in 1990 and 1992, respectively.

On 12 January 1987, due to exceptionally low temperatures, ice blocks in the Loire river clogged the cooling water intake for Unit A1, resulting in the loss of the UHS for this unit. The loss caused the automatic shutdown of the reactor in Unit A1 and the unavailability of all the auxiliary turbo blowers of the unit used for RHR (see Refs [47] and [62]). Off-site power from the grid was used to directly power the blowers and start residual heat removal. After an hour, one of the boilers supplying steam to the turbo blowers could be started. The other three followed during the morning. The availability of all four turbo blowers was restored just before the collapse of the electrical power grid in West France due to a failure of the Cordemais thermal power plant, which occurred at about noon. The failure of the thermal power plant was also traced back to the cold weather conditions. The collapse of the grid produced the automatic shutdown of Unit A2.

Fundamental safety functions in the plant were kept during the event.

A.3.2. Davis-Besse nuclear power plant – Tornado (1998)

The Davis-Besse nuclear power plant is located on the shoreline of Lake Erie, in Ohio, close to the city of Toledo, in the United States of America. The plant has a PWR of 925 MWe that started operation in 1978.

On 24 June 1998, the plant was directly hit by a tornado classified as F-2 in the Fujita scale, with wind speeds in the range from 54 to 75 m/s (195 to 270 km/h). These speeds are within the wind design basis of the plant for safety related SSCs [47].

The tornado damaged the plant's switchyard and the reactor automatically shut down due to loss of off-site power. EDGs were started, which provided power to the plant's safety systems (see Refs [63] and [64]). The RHR from the reactor core developed as intended by the design. Fundamental safety functions in the plant were kept during the event.

On the other hand, significant damage was recorded at the switchyard and to non-safety related buildings and roofs. The three lines connecting the plant to the grid were cut off. The emergency response communication system was highly challenged by the damage of two of the three available telephone systems (only the microwave remained operational). Plant computer systems failed because of loss of power. Rain entered the turbine hall through the damaged roof (due to large holes) [47].

A.3.3. Turkey Point nuclear power plant – Hurricane (1992)

The Turkey Point nuclear power plant is located close to Homestead, in Florida, about 40 km south of Miami, in the United States of America. The site has two operating nuclear units, Units 3 and 4, with PWRs of 837 and 829 MWe, respectively. These reactors started commercial operation in 1972 and 1973. In addition, the site has three gas fired units.

On 24 August 1992, the site was directly hit by Hurricane Andrew, which produced wind speeds of 233 km/h and gusts at 282 km/h. These speeds are within the wind design basis of the plant for safety related SSCs [47].

Operators received early warnings from the weather forecast services. On this basis, equipment was removed from outside areas or tied down, drains plugged to prevent water coming into buildings, removable goods were secured and operators requested to stay into the diesel building as displacements of people between buildings was expected to be impaired by the storm. Units 3 and 4 started shutdown 10 and 9 hours, respectively, before the expected hurricane impact. Emergency core cooling systems performed well throughout the event [47].

Seismic class 1 structures did not suffer any damage during the passage of the hurricane. A total loss of off-site power was experienced for five days, but emergency diesels provided the required power to the plant during this period. One diesel unit had to be stopped because of high temperature, incompatible with operating procedures [47].

During the storm, many false alarms from the spent fuel storage caused concern because storage was not accessible during the storm. Off-site communications were lost, and access roads blocked for some time: helicopters had to be used for fuel and consumables. Families were hosted at the plant and fed, to allow operators to work with peace of mind regarding the status of their families [47].

A water tower collapsed with major damage to fire protection system piping, water supply system, electrical services and instrumentation. Some non-safety related buildings (warehouse, administrative) were destroyed [47].

A.3.4. Maanshan nuclear power plant – Salty sea smog (2001)

The Maanshan nuclear power plant is located on the coast, at the very south end of the Island of Taiwan. It has two PWRs of 950 MWe each, which started operation in 1984 and 1985, respectively.

On 18 March 2001, a seasonal sea smog, rich in salt content, caused the malfunction of power transmission lines in Southern Taiwan, resulting in a total loss of off-site power in the Maanshan nuclear power plant [65]. A buildup of salt crystals transported by heavy sea winds on the insulators on power lines leading to the plant was the root cause of the event.

On the previous day, 17 March 2001, the 345 kV off-site power was lost, which had motivated the automatic shutdown of both units. Although the 345 kV grid was restored later on during the day, it remained in an unstable condition and both reactors had been kept in a hot standby since they tripped off [65].

On 18 March 2001, at 00:41 h, the plant lost all trains of 345 kV off-site power. Supply of essential 4.16 kV buses was transferred automatically to the 161 kV off-site grid. A few minutes later, one 345 kV line

was restored, and an attempt was made to change back to the 345 kV grid, but a ground fault at the essential 4.16 kV bus A of Unit 1 happened and a fire broke out, which rendered this bus inoperable. The emergency diesel generator of train A started but tripped off because of failure signal in essential bus A. The emergency diesels of train B could not be started due to difficulties in manual activation since the building was full of smoke and lighting was insufficient (see Refs [47] and [65]). Inability to start the diesels in train B resulted in a loss of power in essential 4.16 kV buses of Unit 1, that is, in a station blackout scenario (effectively, since 00:45 h) (see Refs [65] and [66]).

Power to essential bus of train B was restored using a swing emergency diesel generator (shared between Units 1 and 2) at 02:54 h, which ended the emergency condition declared in Unit 1 [65].

When the incident happened, both reactors had already been shut down for 21 hours. They were in a hot shutdown condition, with reactor pressure at 157 kg/cm^2 and temperature at 291°C. During the event, the turbine driven auxiliary feedwater pump functioned normally as designed, and with the proper operation of pilot operated relief valves at the steam generators, the core temperature and pressure continued to reduce throughout the event.

A.4. OTHER SEVERE EVENTS

This section provides details of other severe events from existing nuclear installations.

A.4.1. Cadarache laboratories – Forest fire (1989)

The French Alternative Energies and Atomic Energy Commission (CEA) has a large research site in Cadarache, near Aix-en-Provence, in the south of France. This area houses, among other facilities, the Jules Horowitz fission research reactor and the International Thermonuclear Experimental Reactor (ITER fusion reactor).

On 1 August 1989, at 13:40 h, a forest fire broke out in the woods surrounding the site, at only 3 km distance from the outer fence of the site (see Refs [47] and [27]). The fire moved very quickly towards the site due to the strong wind and reached the site limits in less than one hour. Fire brigades from municipalities around the site and firefighter teams from the Departmental level (Bouches-du-Rhone), up to 130 firefighters, came to help the on-site fire brigade. Air support was provided by Canadair waterbombers based in Marseille. The planes flew continuously over the site, often in dangerous routes, as close as possible to the main fire sources. Despite these efforts, the fire penetrated into the site and affected 5 ha inside its boundary [27].

The fire was considered to be extinguished on 6 August 1989, that is, the total duration of the event was about five days. During the event, all the facilities remained protected and no relevant incidents were reported. On the other hand, access to the site was very difficult, which sometimes challenged the arrival of specialized personnel and support firefighters.

Being surrounded by dense woods, the forest fire hazard had been assessed by CEA/Cadarache and measures had been implemented to assure confinement of buildings, to avoid the risk of fire propagation through the ventilation systems (airborne incandescent particles) and to assure availability of water for the external fire protection system. In addition, within the site boundary, an effort had been made to eliminate vegetation which could fuel a fire [27].

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).

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

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Safety Standards Series No. SSR-3, IAEA, Vienna (2016).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Fuel Cycle Facilities, IAEA Safety Standards Series No. SSR-4, IAEA, Vienna (2017).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Aspects of Nuclear Power Plants in Human Induced External Events: Margin Assessment, Safety Reports Series No. 88, IAEA, Vienna (2017).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Methodologies for Seismic Safety Evaluation of Existing Nuclear Installations, Safety Reports Series No. 103, IAEA, Vienna (2020).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Vulnerabilities of Operating Nuclear Power Plants to Extreme External Events, IAEA-TECDOC-1834, IAEA, Vienna (2017).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Approaches to Safety Evaluation of New and Existing Research Reactor Facilities in Relation to External Events, Safety Reports Series No. 94, IAEA, Vienna (2019).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA-TECDOC-1791, IAEA, Vienna (2016).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Non-linear Response to a Type of Seismic Input Motion, IAEA-TECDOC-1655, IAEA, Vienna (2011).

[11] JOHNSON, J.J., GODOY, A., GURPINAR, A. and KENNEALLY, R., "Impact of the Niigataken Chuetsu-Oki Earthquake (NCOE) to the Kashiwaza-Kariwa Nuclear Power Plant, Post-Earthquake Response, and Lessons Learned: U.S. Perspective for Design Basis Earthquakes and Beyond Design Basis Earthquakes," in *U.S. DoE Natural Phenomena Hazards Meeting*, Germantown, MD (October 18-19, 2016).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Instrumentation System and its Use in Post-Earthquake Decision Making at Nuclear Power Plants, IAEA-TECDOC-1956, IAEA, Vienna (2021).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Safety for Nuclear Installations, IAEA Safety Standards Series No. SSG-89, IAEA, Vienna (2024).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design for Nuclear Installations, IAEA Safety Standards Series No. SSG-67, IAEA, Vienna (2021).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Nuclear Installations against External Events Excluding Earthquakes, IAEA Safety Standards Series No. SSG-68, IAEA, Vienna (2022).

[16] U.S. NUCLEAR REGULATORY COMMISSION, "An Approach to the Quantification of Seismic Margins in Nuclear Power Plants," NUREG/CR-4334, Washington D.C. (1985).

[17] AMERICAN SOCIETY OF CIVIL ENGINEERS, "Seismic Design Criteria for Structures, Systems, and Components in Nuclear Facilities," ASCE 43-19, Reston, VA (2019).

[18] AMERICAN SOCIETY OF CIVIL ENGINEERS, "Seismic Analysis of Safety-Related Nuclear Structures," ASCE 4-16, Reston, VA (2016).

[19] U.S. NUCLEAR REGULATORY COMMISSION, "Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,"

SECY-93-087 (Response to: U.S. NRC, “Staff Requirements Memorandum to SECY-93-087,” July 21, 1993), Washington D.C. (1993).

[20] U.S. NUCLEAR REGULATORY COMMISSION, “Seismic Design Standards and Calculational Methods in the United States and Japan,” NUREG/CR-7230, Washington D.C. (2017).

[21] SMiRT-23, “Considerations for Beyond Design Basis External Hazards in NPP Safety Analysis,” SMiRT-23,Division IV, Paper ID 424, Manchester, United Kindom (August 10-14, 2015).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Aspects of Nuclear Power Plants in Human Induced External Events: Assessment of Structures, Safety Reports Series No. 87, IAEA, Vienna (2018).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Hazards Associated with Human Induced External Events in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-79, IAEA, Vienna (2023).

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Aspects of Nuclear Power Plants in Human Induced External Events: General Considerations, Safety Reports Series No. 86, IAEA, Vienna (2017).

[25] HENKEL, F.O. and KOSTOV, M., “Risk Assessment and Development of Protection Capacity for Critical Infrastructures due to Aircraft Attack,” RISK PROTEC CI – Results of a European R&D Project, Sofia (2014).

[26] OECD NUCLEAR ENERGY AGENCY, “Improving Robustness Assessment Methodologies for Structures Impacted by Missiles (IRIS_2012) – Final Report,” Report NEA/CSNI/R(2014)5, Paris (August 2014).

[27] ANDREANI, A.M. and ANDRE, S., “Exemples d'Agressions Externes Vecues sur le Site de Cadarache,” *Controle,* no. 142, pp. 83-84 (2001).

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-18, IAEA, Vienna (2011).

[29] SCHNEIDER, J. and VROUWENVELDER, T., “Introduction to Safety and Reliability of Structures,” 3rd edition, International Association for Bridge and Structural Engineering, Zurich (1997).

[30] EUROPEAN COMMITTEE FOR STANDARDIZATION, “Eurocode – Basis of Structural Design,” European Standard EN 1990:2002+A1, Brussels (2005).

[31] ELLINGWOOD, B., GALAMBOS, T.V., MacGREGOR, J.G. and CORNELL, C.A., “Development of a Probability Based Load Criterion for American Standard A58 – Building Code Requirements for Minimum Desing Loads in Building and Other Structures,” U.S. Department of Commerce, NBS Special Publication 577, Washington D.C. (1980).

[32] U.S. NUCLEAR REGULATORY COMMISSION, “Individual Plant Examination for Severe Accident Vulnerabilities-10CFR50.54(f),” Generic Letter 88-20, Washington D.C. (1988).

[33] U.S. NUCLEAR REGULATORY COMMISSION, “Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities,” NUREG-1407, Washington D.C. (1991).

[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-9 (Rev. 1), IAEA, Vienna (2022).

[35] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment for Seismic Events, IAEA-TECDOC-1937, IAEA, Vienna (2020).

[36] KENNEDY, R.P., “Overview of Methods for Seismic PRA and Margin Analysis Including Recent Innovations,” in *Proceedings of the OECD-NEA Workshop on Seismic Risk*, Tokyo (10-12 August 1999).

[37] ELECTRIC POWER RESEARCH INSTITUTE, “Updated Plant Level Fragility Estimates: Reassessment of IPEEE Data and Seismic Probabilistic Risk Assessment Data,” White Paper EPRI 3002018215, Palo Alto, CA (June 2020).

[38] ELECTRIC POWER RESEARCH INSTITUTE, “Seismic Fragility and Seismic Margin Guidance for Seismic Probabilistic Risk Assessments,” Technical Report EPRI 3002012994, Palo Alto, CA (2018).

[39] ELECTRIC POWER RESEARCH INSTITUTE, “Fleet Risk Assessment for the Next Generation Attenuation East Ground Motion Model,” White Paper EPRI 3002018217, Palo Alto, CA (2020).

[40] KENNEDY, R.P. and SHORT, S.A., “Basis for Seismic Provisions of DOE-STD-1020,” UCRL-CR-111478 / BNL-52418, Washington, D.C. (1994).

[41] U.S. NUCLEAR REGULATORY COMMISSION, “Tornado Climatology of the Contiguous United States,” NUREG/CR-4461, Rev. 2, Washington D.C. (2007).

[42] U.S. NUCLEAR REGULATORY COMMISSION, “Technical Basis for Regulatory Guidance on Design-Basis Hurricane-Borne Missile Speeds for Nuclear Power Plants,” NUREG/CR-7004, Washington D.C. (2011).

[43] WORLD METEOROLOGICAL ORGANIZATION, “Manual on Estimation of Probable Maximum Precipitation (PMP),” WMO-No. 1045, Geneva (2009).

[44] INTERNATIONAL ATOMIC ENERGY AGENCY, Multi-Unit Probabilistic Safety Assessment, Safety Reports Series No. 110, IAEA, Vienna (2022).

[45] HERRING, K.S., ROONEY, V. and CHOKSHI, N.C., “Effects of November 8, 1980 earthquake on Humboldt Bay Power Plant and Eureka, California area Reconnaissance report 13 Nov-14 Nov 80,” NUREG-0766, Washington D.C. (1981).

[46] NICHOLSON, C., ROELOFFS, E. and WESSON, R.L., “The northeastern Ohio earthquake of 31 January 1986: Was it induced?,” *Bulletin of the Seismological Society of America,* vol. 78, no. 1, pp. 188-217 (1988).

[47] INTERNATIONAL ATOMIC ENERGY AGENCY, Extreme External Events in the Design and Assessment of Nuclear Power Plants, IAEA-TECDOC-1341, IAEA, Vienna (2003).

[48] INTERNATIONAL ATOMIC ENERGY AGENCY, Review of Seismic Evaluation Methodologies for Nuclear Power Plants based on a Benchmark Exercise, IAEA-TECDOC-1722, IAEA, Vienna (2013).

[49] KAMAGATA, S. and TAKEWAKI, I., “New insights into seismic behavior of building and surrounding soil at Hamaoka nuclear power station during Suruga Bay earthquake in 2009,” *Soil Dynamics and Earthquake Engineering,* vol. 53, pp. 73-91 (2013).

[50] INTERNATIONAL ATOMIC ENERGY AGENCY, “The Fukushima Daiichi Accident,” Technical Volumes 1 to 5, IAEA, Vienna (2015).

[51] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA International Fact Finding Expert Mission of the Fukushima Dai-Ichi NPP Accident following the Great East Japan Earthquake and Tsunami, IAEA, Vienna (2011).

[52] ELECTRIC POWER RESEARCH INSTITUTE, “EPRI Fukushima Daini Independent Review and Walkdown,” Report 1023422, Palo Alto, CA (August 2011).

[53] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Mission to Onagawa Nuclear Power Station to Examine the Performance of Systems, Structures and Components following the Great East Japanese Earthquake and Tsunami, IAEA, Vienna (2012).

[54] KUMAGAI, T., OGATA, Y., HIROTANI, K., MORIKAWA, H. and SUGAWARA, O., “Simulation Analysis using 3-D Nonlinear FEM model for Onagawa Unit 2 Control

Building at the time of the 2011 off the Pacific coast of Tohoku Earthquake," in *Division V, SMiRT 23*, Manchester, (2015).

[55] HIROTANI, K., OGATA, Y., OHASHI, Y., BABA, Y. and SUGAWARA, O., "Response Characteristics of Operating Floor of Reactor Building in Onagawa Nuclear Power Plant Unit 2 during Tohoku Earthquake 2011," in *16th World Conference on Eartquake Engineering*, Santiago de Chile, (2017).

[56] GOVERNMENT OF JAPAN, "The Accident at TEPCO's Fukushima Nuclear Power Stations," Report to the IAEA Conference on Nuclear Safety (June 2011).

[57] INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE, "Raport sur l'Inondation du Site du Blayais Survenue le 27 Decembre 1999," IRSN, Fontenay-aux-Roses (January 2000).

[58] JIN, S., HONG, S. and IMAMURA, F., "2004 Indian Ocean Tsunami on the Madras Nuclear Power Plant, India," in *Proceedings of the Korean Nuclear Society spring meeting*, Tajeon, Republic of Korea (2006).

[59] ATOMIC ENERGY SOCIETY OF JAPAN, The Fukushima Daiichi Nuclear Accident: Final Report of the AESJ Investigation Committee, Springer (2015).

[60] U.S. NUCLEAR REGULATORY COMMISSION, "Screening Analysis Report for the Proposed Generic Issue on Flooding of Nuclear Power Plant Sites Following Upstream Dam Failures," Office of Nuclear Regulatory Research, Washington, D.C. (July 2011).

[61] U.S. NUCLEAR REGULATORY COMMISSION, "NRC Activates Incident Response Center for Tracking Events at the Fort Calhoun Nuclear Power Plant," NRC News No. IV-11-031, Arlington, TX (26 June 2011).

[62] PHARABOD, J.P., Les Jeux de l'Atome et du Hasard, Editions Calmann-Levy (1988).

[63] U.S. NUCLEAR REGULATORY COMMISSION, "NRC Team Dispatched to Davis-Besse Nuclear Plant," NRC News No. RIII-98-40, Lisle, IL (25 June 1998).

[64] U.S. NUCLEAR REGULATORY COMMISSION, "NRC Inspection Team Monitoring Davis-Besse Plant Response to Tornado Damage and Loss of Offsite Power," NRC News No. RIII-98-40a, Lisle, IL (25 June 1998).

[65] ATOMIC ENERGY COUNCIL, "The Station Blackout Incident of the Maanshan NPP Unit 1," Taiwan, Republic of China (2001).

[66] ATOMIC ENERGY COUNCIL, "Report for the Convention on Nuclear Safety," Republic of China (2004).

ANNEX I. DEVELOPMENT OF ANNUAL PERFORMANCE FREQUENCY PREDICTION BASED ON SEISMIC MARGIN

Quantification of annual frequency based performance involves combining the mean seismic hazard curve and mean fragility curves for the installation (one fragility curve for each safety function in the evaluation). The hazard and fragility curves are convolved, that is, integrated to compute the mean annual frequency of installation unacceptable performance. The convolution integral subdivides the ground motion hazard space into bins characterized by the hazard parameter (e.g. PGA), multiplies the conditional probability of failure representative of each PGA bin by the annual rate of occurrence of corresponding PGAs[32], and sums up these products over all the PGA bins, as follows:

$$\lambda_f = \int_0^\infty \frac{-dH(a)}{da} F(a)\, da \qquad \text{(I–1)}$$

where:

λ_f = mean annual frequency of installation failure (e.g. CDF for an NPP);
$F(a)$ = installation-level mean fragility curve;
$H(a)$ = hazard curve.

Discretization of fragility and hazard curves is illustrated in Fig. I–1, which shows a schematic representation of the convolution integral. The PGA range of interest corresponds to PGAs in which the conditional probability of failure is not practically zero or one. For typical applications, this range corresponds to a one-decade span in the mean annual frequency of hazard exceedance.

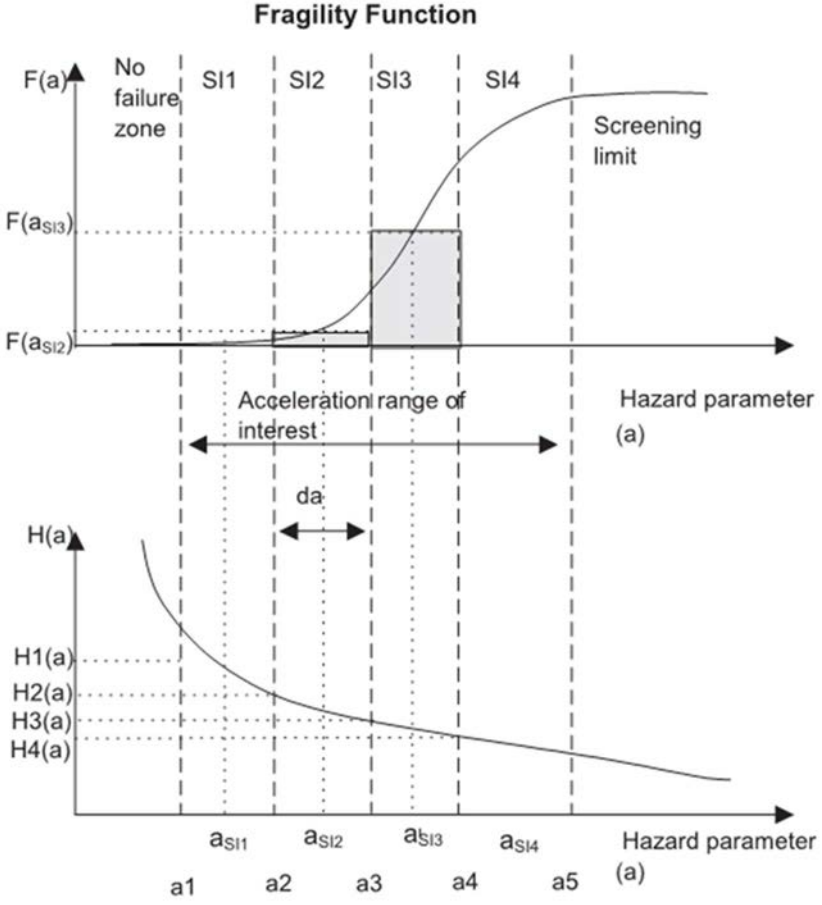

FIG. I–1. Example convolution of seismic fragility and hazard curves [I-1].

[32] Equal to the difference in annual exceedance frequencies of the lowest and highest PGAs in each bin.

When the installation-level seismic fragility curve is available, for instance, from a SPSA of the design, it can be used in the convolution integral, either directly or simplified using a log-normal function fit. However, it is more common in Member States that only a SMA or a PSA based SMA assessment of the design is performed. When only the HCLPF capacity is known from a margin assessment, it can be used to generate an estimate of the corresponding installation-level fragility as discussed in Section 5.2.1.

When plotted on a log-log scale, hazard curves typically have a slightly concave shape that can be adequately approximated as piecewise linear segments over each one-decade span of the annual exceedance frequency. A closed form solution of the convolution integral was proposed in Ref. [I–2] based on this simplification, which is considered appropriate for the purposes of this publication. In Ref. [I–2], *H(a)*, the mean annual frequency of exceedance (MAFE) of PGA > *a* within the PGA range of interest, is defined by the following equation:

$$H(a) = K_1 \, a^{-K_H} \tag{I–2}$$

where:

a = value of the hazard parameter (e.g. PGA);
K_H = piecewise linear slope of the hazard curve over one MAFE decade in log-log space;
K_1 = constant that anchors the hazard curve.

The parameters K_H and K_1 are determined such that $H(a)$ produces a close match to the mean hazard curve in the ground motion range of interest. This range of interest typically starts slightly below the HCLPF capacity and spans about one MAFE decade.

$$K_H = 1 / log10(A_R)$$
$$K_1 = H(A_{HCLPF}) \times (A_{HCLPF})^{KH} \tag{I–3}$$

where:

A_R = increase in PGA value across one MAFE decade anchored close to A_{HCLPF}
$H(A_{HCLPF})$ = MAFE of the HCLPF PGA

Since the slope A_R is typically considered valid for the hazard levels including the DBE ground motion, and the mean hazard curve intercepts the DBE ground motion, A_{DBE}, at the mean DBE return period, T_{DBE}, the parameter K_1 is often calculated as follows:

$$K_1 = H(A_{DBE}) \times (A_{DBE})^{KH} = (A_{DBE})^{KH} / T_{DBE}$$

Using this piecewise linear representation of the mean hazard curve in the risk convolution integral and using the A_m and β_c parameters to represent the mean fragility curve yields:

$$\lambda_f = K_1 \, (A_m)^{-K_H} \, e^{0.5 \, (K_H \, \beta_c)^2} \tag{I–4}$$

Since the mean hazard curves are typically slightly concave rather than straight in log-log space, the estimate of annual frequencies using this simplified closed form equation is conservatively biased. Experience from practical application typically shows this bias to be adequately limited for the purpose of this publication.

Finally, the achieved annual frequency performance metric can be estimated based on seismic margin results by substituting the HCLPF capacity in the previous equation. If only the HCLPF capacity is available from the margin assessment, A_m and β_c can be replaced by 2 × A_{HCLPF} and 0.3, respectively (see Section 5.2.1):

$$\lambda_f = K_1 \ (2\,A_{HCLPF})^{-K_H} \ e^{0.045\,(K_H)^2} \qquad \text{for } \beta_c = 0.3 \qquad \text{(I–5)}$$

which can be simplified in terms of $H(A_{HCLPF})$ and A_R that can be directly extracted from the hazard curve to be:

$$\lambda_f = \frac{H(A_{HCLPF})}{2^{K_H}} \ e^{0.045\,(K_H)^2} \qquad \text{for } \beta_c = 0.3 \qquad \text{(I–6)}$$

This results in λ_f being equal to:

= 0.164 $H(A_{HCLPF})$ for $A_R = 2.0$
= 0.285 $H(A_{HCLPF})$ for $A_R = 3.0$
= 0.358 $H(A_{HCLPF})$ for $A_R = 4.0$

Equation (I–6) concludes that the annual frequency based performance metric for typical installations can be estimated from the seismic margin when only the hazard severity at the corresponding HCLPF capacity and the change in hazard severity over a one-decade MAFE span are known. Certain simplifications are involved in this estimate and are based on experience with typical outcomes of seismic fragility evaluations and seismic hazard analyses.

Equation (I–6) also shows the significance of the sensitivity to the slope of the hazard curve. For the same hazard severity at the HCLPF ground motion capacity, that is, the same scenario based performance, the achieved annual frequency based performance corresponds to higher annual rates of failure as the hazard curve slope parameter A_R increases. In other words, for the same seismic margin, the annual frequency of installation failure is higher when the hazard curve slope is relatively flat than when it is relatively steep. For context, mean hazard curves from PSHAs typically have slopes that correspond to A_R values between 2 and 4 in the MAFE range from 10^{-3} yr^{-1} to 10^{-5} yr^{-1}. The achieved performance can therefore be rewritten as the product of two independent functions of the margin and hazard slope:

$$\lambda_f = H(A_{HCLPF}) \ F(A_R) \qquad \text{(I–7)}$$

The A_R-dependent term in the estimated annual frequency is given by:

$$F(A_R) = \frac{e^{0.5\,(K_H\,\beta_C)^2}}{e^{2.33\,\beta_C\,K_H}} \qquad \text{(I–8)}$$

And for $\beta_c = 0.3$:

$$F(A_R) = \frac{1}{2^{K_H}} \ e^{0.045\,(K_H)^2} = \frac{1}{2^{\frac{1}{log10(A_R)}}} \ e^{0.045\left(\frac{1}{log10(A_R)}\right)^2} \approx \left[\frac{1.05}{2^{log10(A_R)}}\right]^{\left(\frac{1}{log10(A_R)}\right)^2} \qquad \text{(I–9)}$$

Figure I–2 plots this relationship for a wide range of A_R values that span practical applications. The term $F(A_R)$ is more sensitive to the hazard curve slope at relatively low values of A_R. It seems to approach an asymptote at higher A_R valuers. Figure I–2 also shows the relationship between $F(A_R)$ and A_R for higher values of the composite variability β_c that controls the slope of the installation-level fragility curve. The illustration demonstrates that the increase in variability β_c results in lower mean annual probabilities of failure (i.e. improved performance metric) for installations that have the same HCLPF capacity based seismic margin and are subject to the same seismic hazard. This comparison does not mean that having higher uncertainty helps achieves better seismic performance. Section 5.3.2 discusses the implications of this comparison.

The factors that influence the hazard curve slope parameter A_R are the following:

- State of knowledge about seismic hazard characterization in the region, namely, epistemic uncertainty. A_R decreases when uncertainty decreases.
- Uncertainty in local site geomaterial properties and seismic response characterizations.
- Installation DBE hazard level. A_R decreases for the same site as the DBE hazard level increases.
- Installation annual frequency based performance goal for the affected safety function. A_R decreases for the same site and installation as $\lambda_{f,T}$ decreases (since the ground motion range of interest shifts to higher PGA values at the site).

In theory, installations with lower variability than β_c = 0.3, which correspond to significantly steep fragility curves, may have higher (i.e. worse) mean annual frequency of failure if they have the same HCLPF capacity that characterizes the seismic margin and are subject to the same seismic hazard. Practically, this possibility is eliminated by ensuring adequate seismic margin against cliff edge effects.

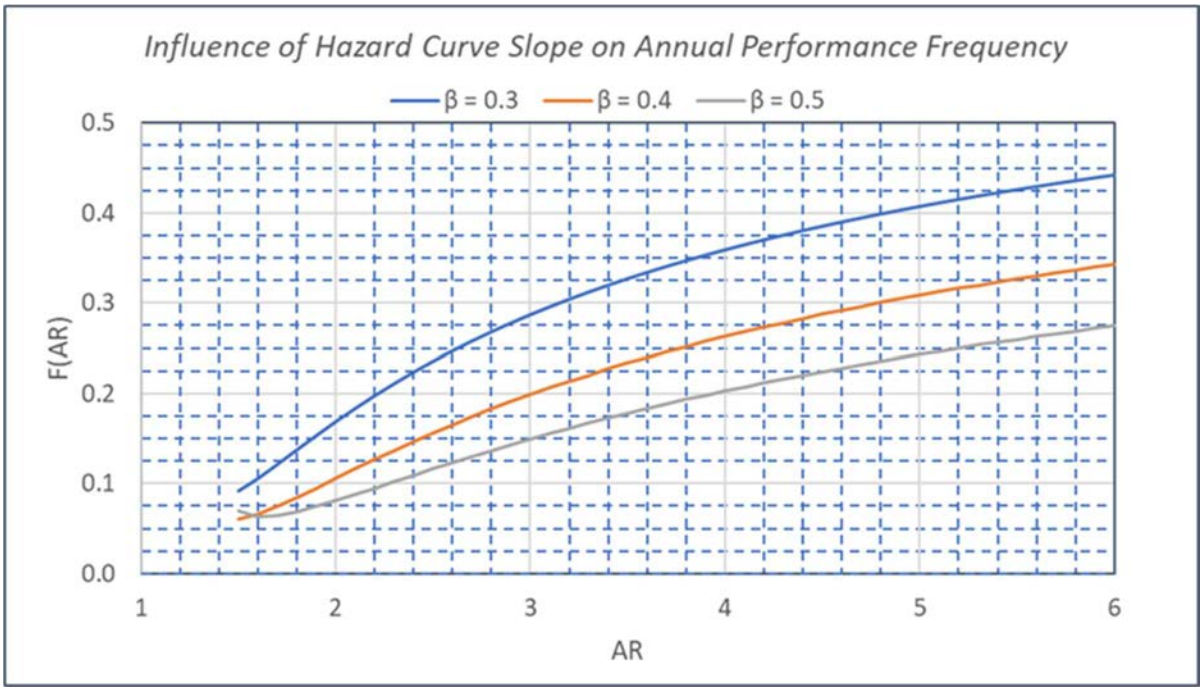

FIG. I–2. Relationship between risk integral term $F(A_R)$ and hazard curve slope A_R.

References to Annex I

[I–1] INTERNATIONAL AOMIC ENERGY AGENCY, Methodologies for Seismic Safety Evaluation of Existing Nuclear Installations, Safety Report Series No. 103, IAEA, Vienna (2020).

[I–2] KENNEDY, R.P. and SHORT, S.A., Basis for Seismic Provisions of DOE-STD-1020, UCRL-CR-111478 / BNL-52418, Washington, DC (1994).

ANNEX II. DEVELOPMENT OF SEISMIC MARGIN REQUIRED TO ACHIEVE TARGET ANNUAL PERFORMANCE FREQUENCY

In this Annex, 'adequate margin' is discussed strictly in reference to achieving the annual frequency based performance goal. Other margin adequacy considerations are applicable and discussed elsewhere in the body of this publication.

Seismic margin is typically defined relative to the DBE using the ratio $R = A_{HCLPF} / A_{DBE}$.

Therefore, in order to achieve an annual frequency based performance goal, the adequate margin, R, depends on the relationship between the seismic hazard level at the DBE and the target annual frequency of unacceptable performance. Specifically, it depends on the ratio of the MAFE at the DBE, $H(A_{DBE})$, and the target annual frequency for the performance goal, $\lambda_{f,T}$. This ratio is expressed by the parameter $R_{DP} = H(A_{DBE}) / \lambda_{f,T}$.

As this ratio increases, the margin required to achieve the ratio increases[33]. In current practice prevalent in Member States, this ratio is typically on the order of 10. A range of 5 to 20 is used herein as a practical range of interest for this ratio.

The annual frequency based performance metric derived from the HCLPF capacity (Annex I) can be expressed in terms of the DBE and the seismic margin, as follows:

$$H(A_{HCLPF}) = H(R \times A_{DBE}) = K_1 \, (R \times A_{DBE})^{-K_H} = R^{-K_H} \left(K_1 \, {A_{DBE}}^{-K_H}\right) = R^{-K_H} \, H(A_{DBE}) \tag{II–1}$$

And, from the equations in Annex I:

$$\lambda_f = R^{-K_H} \, H(A_{DBE}) \; F(A_R) \tag{II–2}$$

$$F(A_R) = \frac{e^{0.5 \, (K_H \, \beta_C)^2}}{e^{2.33 \, \beta_C \, K_H}} \tag{II–3}$$

The adequate margin R to achieve a certain annual frequency $\lambda_{f,T}$ is therefore:

$$R^{K_H} = \frac{H(A_{DBE}) \; F(A_R)}{\lambda_{fT}} = R_{DP} \, F(A_R) \tag{II–4}$$

$$R = [R_{DP} \, F(A_R)]^{\frac{1}{K_H}} \tag{II–5}$$

Figure II–1 plots this relationship for $\beta_c = 0.3$, a wide range of A_R values, and three cases bounding the practical range of R_{DP}. As expected, the adequate margin increases with the ratio R_{DP}, especially for relatively flat hazard curves (i.e. as A_R increases). At some combinations of low A_R and R_{DP} values, the adequate margin is equal to or less than 1.0. This means that having the HCLPF capacity be the DBE is sufficient to achieve the annual frequency based performance goal for these cases. These unlikely combinations correspond to cases in which the target annual frequency is set too low relative to the DBE or the design was originally performed to a DBE that automatically achieves the current annual frequency performance goal.

[33] For example, to achieve the same annual performance, the adequate margin above a DBE set at the 10^{-4} MAFE level is higher than the adequate margin over a DBE set at the 4×10^{-4} MAFE level.

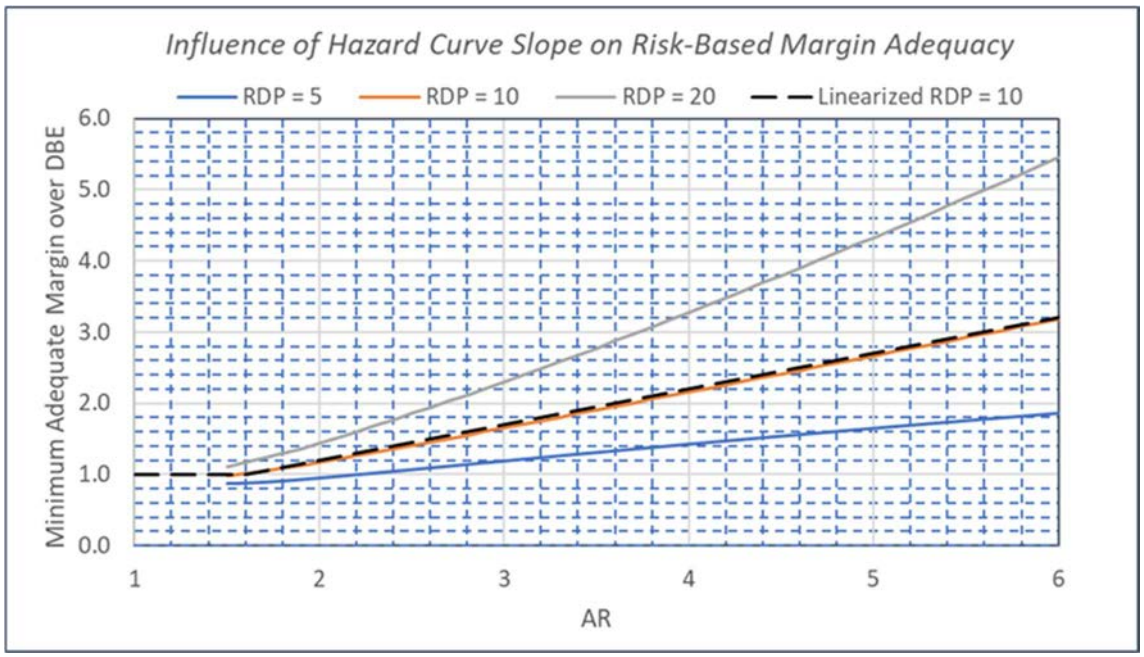

FIG. II–1. Relationship between seismic margin to achieve target frequency and hazard curve slope.

For values of R_{DP} equal to 10, which is the order of practical applications, the adequate margin can be reasonably specified using the following straight line[34]:

$$R(R_{DP}=10) = 1.0 \quad \text{at } A_R \leq 1.6 \qquad \text{(II–6)}$$
$$= 3.0 \quad \text{at } A_R = 5.6$$
$$\text{with linear interpolation in between}$$

At other values of R_{DP}, the adequate margin can be simply scaled up and down according to:

$$R(R_{DP}\neq 10) = R(R_{DP}=10) \times (R_{DP} / 10)^{1/KH} \geq 1.0 \qquad \text{(II–7)}$$

where the limit of 1.0 is imposed to maintain the meaning of seismic margin.

The equations given for R above consider that the slope of the seismic hazard curve between the acceleration amplitudes A_{DBE} and A_{HCLPF} is reasonably close to the slope represented by the parameter A_R in the PGA range of interest, which is typical. If this slope is significantly different[35], the equation for R can be easily generalized as follows:

$$R = [R_{|AR'=AR}]^{\log(AR')/\log(AR)} \qquad \text{(II–8)}$$

where:

$R_{|AR'=AR}$ is the adequate margin calculated assuming that the hazard curve slopes are equal, and

$A_{R'}$ is calculated similar to A_R using the hazard curve slope between A_{DBE} and A_{HCLPF}

Figure II–2 plots the relationship in Eq. (II–5) for $R_{DP} = 10$ and a range of β_c values from 0.3 to 0.5, where $R \geq 1.0$ is imposed. Figure II–2 indicates that sensitivity of the adequate margin to the installation-level variability parameter is lower than that to the mean hazard curve slope. The comparison with Fig.

[34] A slightly better linear fit can be achieved by setting $R = 3$ at $A_R = 5.7$ instead of 5.6. $A_R = 5.6$ was preferred as an anchor point for the convenience of using a line slope of 1:2 in calculating the adequate margin. The resulting conservatism is insignificant.

[35] A practical check is to compare the current A_R to that based on the hazard curve between $H(A_{DBE})$ and $H = \lambda_{f,T}$.

II–1 indicates that this sensitivity is significantly lower than that to the ratio of the DBE hazard level to the target annual performance.

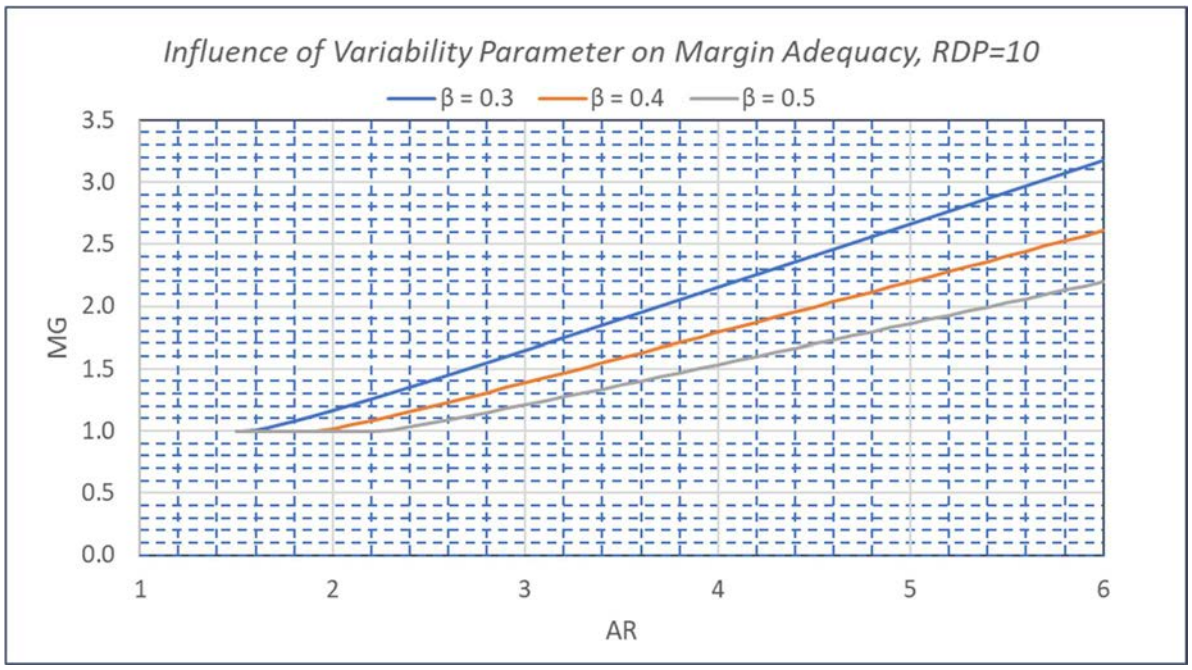

FIG. II–2. Relationship between seismic margin to achieve target frequency and hazard curve slope for R_{DP}=10 and variable β_c.

ANNEX III. EXAMPLE IMPLEMENTATIONS OF CLIFF EDGE SEISMIC MARGIN ASSESSMENT

This Annex presents stylized examples to demonstrate practical implementation of the cliff edge seismic margin adequacy criteria developed in Section 7.2.3. Example implementations are developed for the following cases:

1. An installation that performed an SMA performance evaluation;
2. An installation that performed an SPSA performance evaluation.

These two examples represent two cases in which the performance evaluation methodologies used in the safety assessment of the design (i.e. SMA and SPSA) provide the least and the most amount of detail among the three safety assessment methodologies recommended in IAEA Safety Standards Series No. SSG-89, Evaluation of Seismic Safety for Nuclear Installations [III–1]. For an installation that performed safety assessment using the hybrid PSA based SMA methodology, elements of the cliff edge seismic margin assessment implementations used in both examples can be combined as applicable depending on the information available from the installation design safety assessment.

III-1. USING SMA OUTPUT

Input data:

$\lambda_{f,T}$	$= 10^{-5}$ yr^{-1}	Annual performance goal
A_{DBE}	$= 0.3\ g$	DBE ground motion (PGA)
T_{DBE}	= 10 000 yr	Mean return period for the DBE
A_{HCLPF}	$= 0.5\ g$	Installation-level HCLPF capacity (PGA)
β_c	= 0.3	Estimated composite variability (see Section 5.2.1)
A_R	= 2.8	Increase in value of A in a 10-fold reduction in MAFE

Note:

The installation-level HCLPF capacity margin is $1.67 \times A_{DBE}$. This HCLPF capacity satisfies the recommended seismic margin to achieve the target annual frequency based performance objective (see Section 5.2.3.1). Following Eq. (6) (see Section 5.2.3.1), the minimum margin to achieve this objective at this installation is $1.6 \times A_{DBE}$. The recommendations in Eq. (6) are based on a β_c value equal to 0.3 or higher, as typically observed in recent SPSA studies. Review of the ratio $A_{10\%} / A_{HCLPF}$ to confirm this assumption and identify potential non-classic cliff edge failure events is not possible given the available information, since only the HCLPF capacity is provided by the SMA. This is a limitation on the utility of SMA methodology for design robustness (an alternative qualitative review is proposed in Section 7.2.3.4).

Objective 1:

Geotechnical investigations indicated that the site may be susceptible to seismic induced slope failure hazard. This failure mode was not modelled in the SMA success paths. Review of the consequences of potential slope failure indicated that concurrent damage to affected SSCs can result in a cliff edge failure event for all success paths. The HCLPF capacity for slope failure was deterministically estimated using conservative analysis methods to be at least 0.8 g. Assess its adequacy to achieve a robust design.

Criteria:

Follow the criteria in Section 7.2.3.1, with the idealizations recommended in Section 7.2.3.4.

Solution:

Using Eqs (1) and (3):

A_m= 1.01 g
K_H = 2.24
K_I = 6.77×10^{-6} yr^{-1}
λ_f= 8.33×10^{-6} yr^{-1} using Eq. (3) (see Section 5.2)
λ_f= 8.38×10^{-6} yr^{-1} using discrete convolution integral (Fig. III–1, blue and grey curves)

Numerical calculation of λ_f using discrete convolution integration (Fig. III–1) produces essentially the same value as the approximate closed form solution of Eq. (3) (see Section 5.2), which confirms the process implementation. For the remainder of this example, use the value of λ_f from the numerical integration.

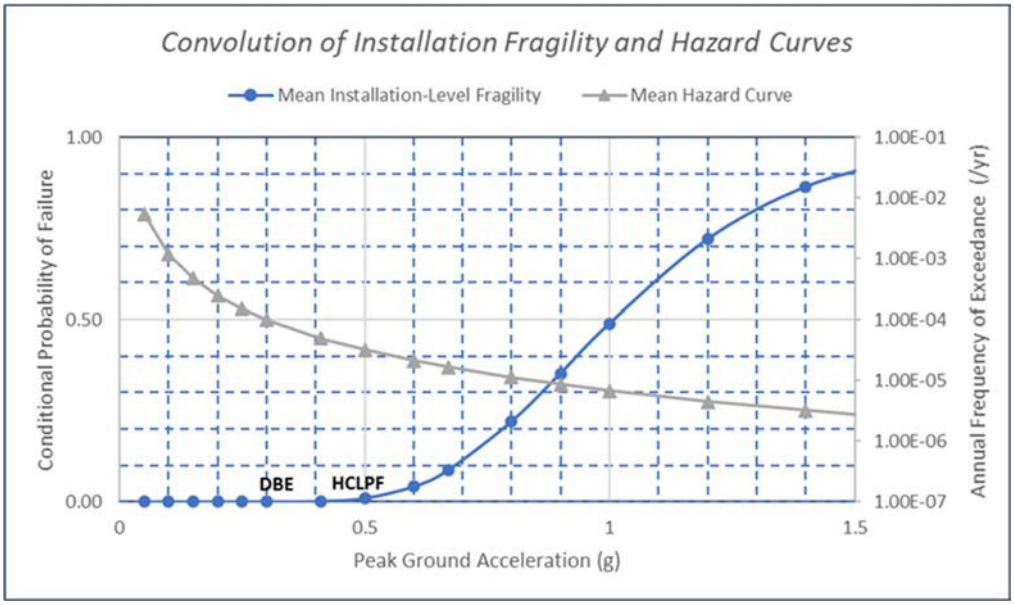

FIG. III–1. SMA installation-level mean fragility convolution with seismic hazard curves.

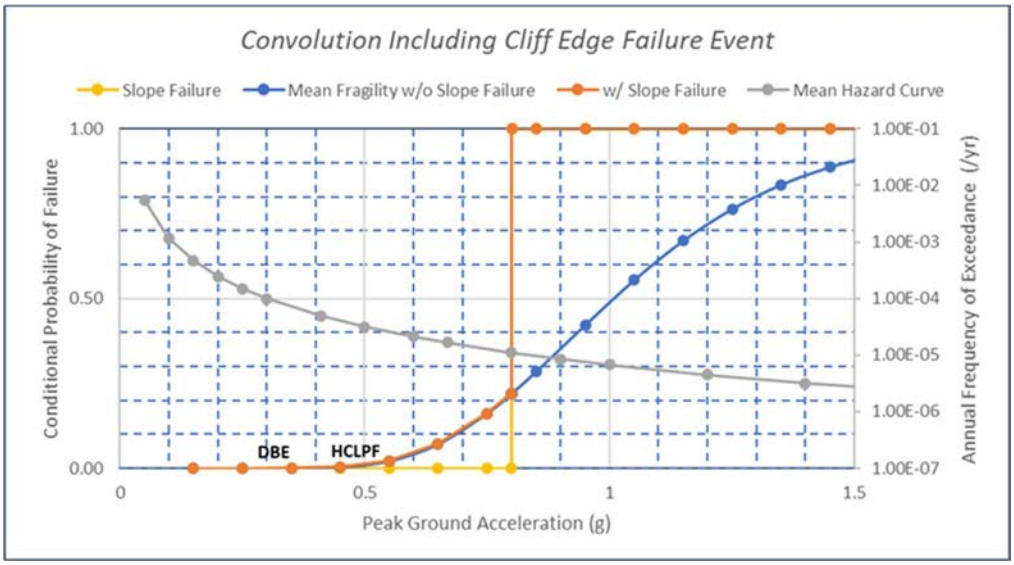

FIG. III–2. SMA installation-level fragility convolution with and without cliff edge effect.

For the slope failure event, only the HCLPF capacity is available, i.e. the complete fragility function was not developed. Following Section 7.2.3.4, the slope failure event with a HCLPF capacity of 0.8 *g* is idealized as a step function going from a conditional failure probability of 0 to 1.0 at PGA = 0.8 *g* (Fig. III–2). This somewhat conservative idealization (see Section 7.2.3.4) is suitable for a demonstration example. This idealized fragility is combined with the installation-level fragility curve and convolved with the mean hazard curve in Fig. III–2 (dark orange and grey curves). The resulting total value and increase in annual frequency of an unacceptable end state are found to be the following:

$$\lambda_{f^*} = 1.26 \times 10^{-5}\ \text{yr}^{-1}$$

$$\Delta\lambda_f = 4.22 \times 10^{-6}\ \text{yr}^{-1}$$

The computed annual frequency of unacceptable performance is higher than the target of 10^{-5} yr^{-1}, which does not satisfy the second adequacy criterion in Section 7.2.3.1. The increase in annual frequency due to the cliff edge failure event is about 33% of the total, which is higher than the 10% proposed for the first criterion in Section 7.2.3.1. Having not satisfied either criterion, the cliff edge HCLPF capacity of 0.8 *g* is not demonstrated to be adequate to achieve the robust design performance objectives in this idealized example.

This conclusion does not necessarily mean that a revision of the design is required. A less conservative idealization than a step function for the cliff edge fragility will result in smaller estimates of annual frequency metrics, and this may change the conclusion. A more realistic fragility idealization can be used if an explicit fragility evaluation was performed or where justified by sufficient knowledge about the failure mode and site conditions to inform the estimation of minimum variability associated with the cliff edge failure event[36]. This minimum variability and the HCLPF capacity of the failure event can be used to construct a log-normal fragility curve to replace the step function used in this example.

Objective 2:

Considering the same site and installation, determine the minimum HCLPF capacity for a potential cliff edge failure event to be acceptable for design robustness.

Criteria:

Follow the criteria in Section 7.2.3.1 with the idealizations recommended in Section 7.2.3.4.

Solution:

From before:

$$\lambda_f = 8.38 \times 10^{-6}\ \text{yr}^{-1} \text{ using discrete integration}$$

The minimum adequate HCLPF for a cliff edge failure event is found by iteration. The cliff edge failure fragility shown in Fig. III–2 is shifted to the right by increasing its HCLPF capacity in increments of 0.01 *g*. It is found that at a HCLPF capacity of 0.96 *g* for this failure mode, the total mean annual frequency λ_{f^*} computed by convolving the resulting trial of the installation-level fragility with the mean hazard curve (orange and grey curves in Fig. III–2) becomes equal to the target of 10^{-5} yr^{-1}. This satisfies the second criterion in Section 7.2.3.4. By inspection, the HCLPF capacity needed to satisfy the first criterion (for a 10% annual frequency contribution) is higher and is therefore not governing since satisfying one criterion is sufficient for this margin adequacy assessment.

Accordingly, potential cliff edge failure events with HCLPF capacities higher than 0.96 *g* can be found by default to be adequate for a robust design that achieves the annual frequency based performance goal.

[36] In the absence of explicit fragility evaluation, a lower bound estimate of the variability parameter has to be used in conjunction with the HCLPF capacity to achieve high confidence in the cliff edge seismic margin adequacy assessment.

An installation specific screening criterion for cliff edge failure events can be established at or above 0.96 *g*. A precise determination of HCLPF capacities for potential cliff edge failures does not need to be performed if they can be shown with high confidence to exceed this screening criterion.

III-2. USING SPSA OUTPUT

This example uses the installation presented in Section III–1. SPSA was used for safety assessment of the design. The fragility curves for individual cutsets produced by the PSA model logic tree are generated. The installation-level mean fragility curve is computed by union of the cutset mean fragility curves and is provided as conditional probabilities of an unacceptable end state at discrete PGAs. This installation-level mean fragility curve is shown in Fig. III–3. The shape of this explicitly quantified installation-level fragility curve does not typically follow a log-normal distribution or another functional form. The installation-level HCLPF capacity is determined by piecewise interpolation as the PGA corresponding to 0.01 probability on the installation-level mean fragility curve. This HCLPF capacity is found to be 0.5 *g*, i.e. equal to the HCLPF capacity from the SMA in Section III–1.

For reference, the SMA based installation-level fragility estimated using a generic β_c equal to 0.3 (see Section III–1) is shown in Fig. III–3. For this idealized example, the mean fragility curve from the SPSA output, though non-log-normal, has a shape that generally resembles the fragility estimated from the SMA output in the previous example. This similarity is intended for this example to allow developing insights from comparing the outputs for the cliff edge seismic margin assessment for the two examples using comparable input conditions. Typically, SMA and SPSA outputs show larger differences.

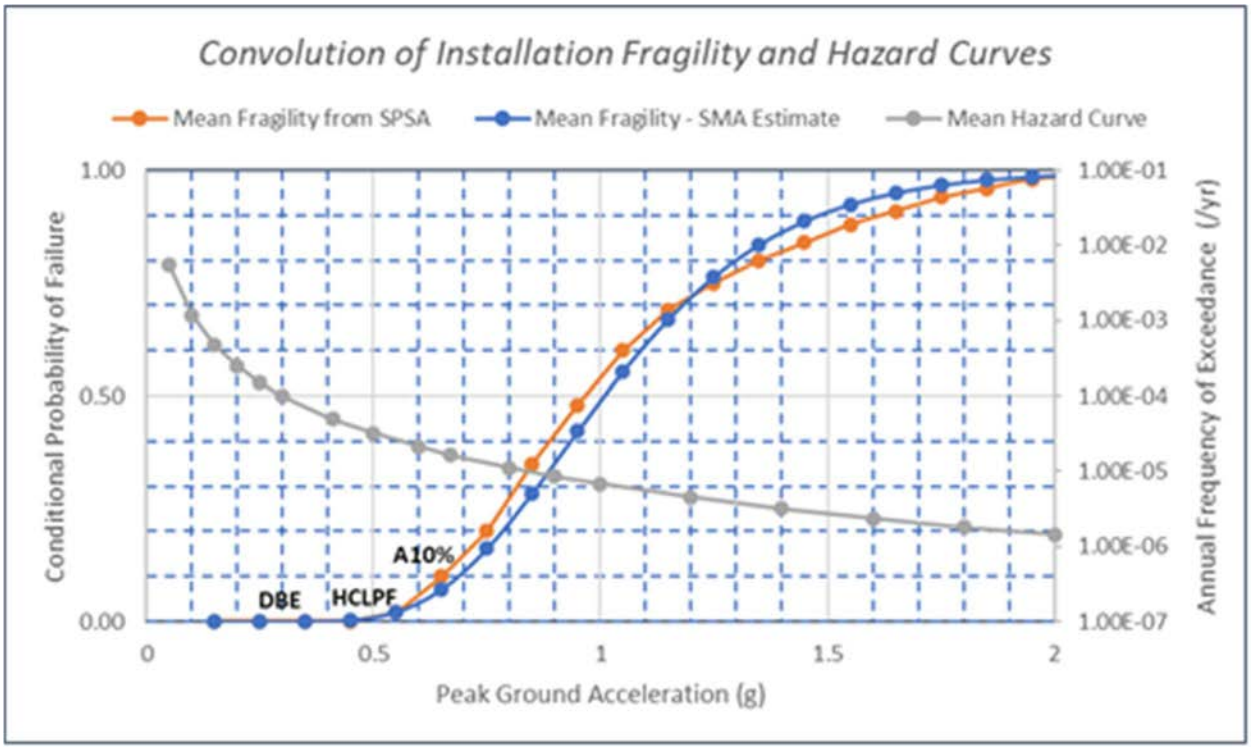

FIG. III–3. SPSA and SMA installation-level fragilities and mean hazard curve.

Input data:

$\lambda_{f,T}$	$= 10^{-5}$ yr^{-1}	Annual performance goal
A_{DBE}	$= 0.3\ g$	DBE ground motion (PGA)

T_{DBE}	= 10 000 yr	Mean return period for the DBE
A_{HCLPF}	= 0.5 g	Installation-level HCLPF capacity (PGA)
$A_{10\%}$	= 0.65 g	Installation-level capacity at 10% mean probability of failure (PGA)
β_c		N/A (Discretized fragility curve, Fig. III–3)
A_R	= 2.8	Increase in value of A in a 10-fold reduction in MAFE

Objective 1:

Similar to the previous example, the installation-level HCLPF capacity satisfies the recommended seismic margin to achieve the target annual frequency based performance objective. However, the installation-level fragility curve shows a steeper shape at low conditional probabilities (i.e. the lower left tail in Fig. III–3) than that corresponding to β_c of 0.3. This would violate the assumptions of Eq. (6). Reassess the adequacy of the seismic margin.

Criteria:

Follow the criteria in Section 7.2.3.2, implemented according to Section 7.2.3.3.

Solution:

The ratio $A_{10\%} / A_{HCLPF}$ is equal to 1.3, which is lower than 1.4 and, thus, confirms that the mean fragility curve at the left tail is effectively steeper than used in developing the seismic margin adequacy recommendations in Section 5.2.3.1.

The first seismic margin adequacy acceptance condition in Section 7.2.3.2 considers the additional margin in the installation-level HCLPF capacity, which is equal to 1.67 × A_{DBE}, above the minimum of 1.6 × A_{DBE} recommended by Eq. (6). The minimum recommended $A_{10\%}$ corresponding to Eq. (6) is equal to:

$$A_{10\%,min} = 1.4 \times 1.6 \times 0.3\ g = 0.67\ g$$

The installation-level $A_{10\%}$ is 0.65 g, i.e. less than 0.67 g. This condition, strictly speaking, is therefore not met, though this exceedance is likely to not be considered to be practically significant.

The second acceptance condition in Section 7.2.3.2 quantifies the annual frequency of installation unacceptable performance using the fragility curve which includes $A_{10\%} / A_{HCLPF} < 1.4$. By discrete numerical integration of the convolution integral (Fig. III–3, orange and grey curves), the achieved annual frequency of unacceptable performance is found to be:

$$\lambda_f = 8.88 \times 10^{-6}\ \text{yr}^{-1}$$

This achieved performance meets the target of less than 10^{-5} yr^{-1}. The installation-level fragility therefore meets the second acceptance condition and is shown to be consistent with the performance goal. It also only slightly exceeds the threshold for the first acceptance condition. Meeting either acceptance condition is sufficient for this margin adequacy assessment.

This somewhat steep installation-level fragility curve indicates the potential presence of several SSC failures of comparable seismic fragilities on one or more branches of the SPSA cutsets. Review of the individual cutset fragilities with significant risk contributions should enable identifying these SSCs. If the installation-level fragility did not meet the performance objective, or if achieving a less steep fragility curve is desired for other reasons, the SSCs represented by these fragilities may be suitable candidates for seismic capacity enhancements and/or refinement of their fragility evaluations.

Objective 2:

Considering the same site and installation, determine the minimum HCLPF capacity for a potential classic cliff edge failure event to be acceptable for design robustness.

Criteria:

Follow the criteria in Section 7.1.3.1, with the idealizations recommended in Section 7.2.3.4.

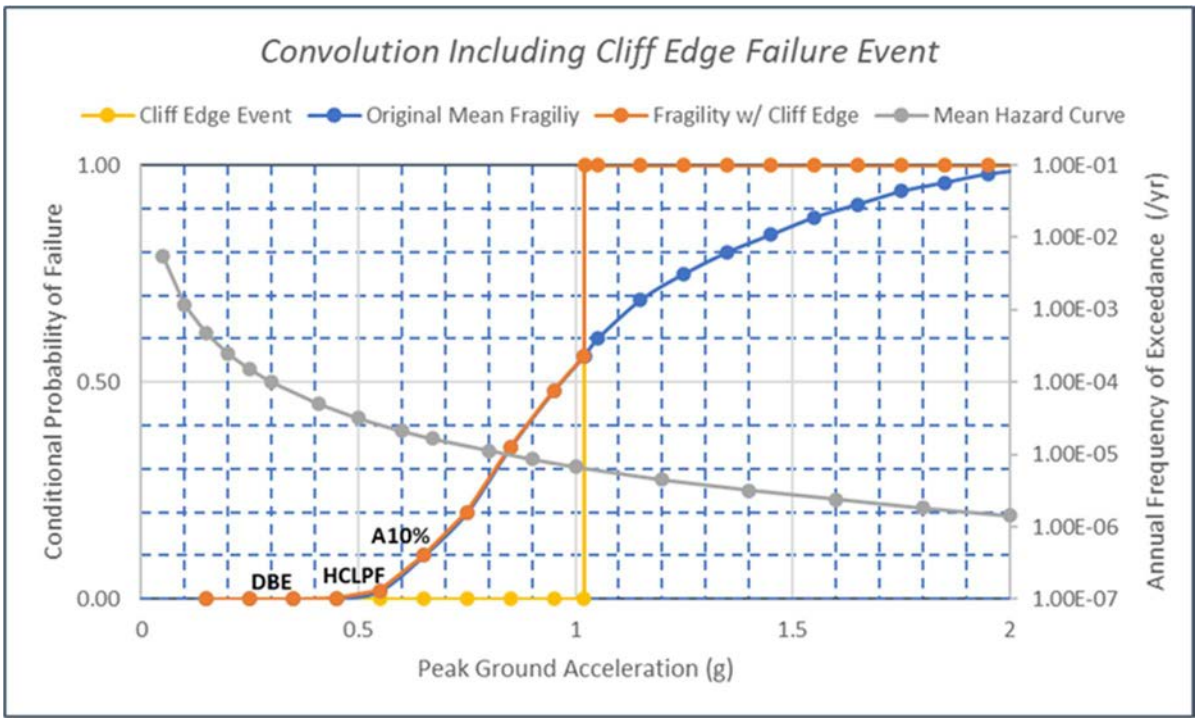

FIG. III–4. SPSA installation-level fragilities with and without generic cliff edge event.

Solution:

From before:

$$\lambda_f = 8.88 \times 10^{-6}\ \text{yr}^{-1} \text{ using discrete integration}$$

The minimum HCLPF capacity being determined is for a generic potential cliff edge event. With no knowledge of the specifics of the failure mode, the fragility function of this generic event is conservatively represented by a step function from 0 to 1 at the PGA corresponding to its HCLPF capacity. Figure III–4 shows this representation. The HCLPF capacity for this generic failure mode is determined by iteration. The corresponding PGA value is incremented by 0.01 *g* until the annual frequency of unacceptable performance, λ_{f^*} , computed by convolving the resulting trial of the installation-level fragility with the mean hazard curve (orange and grey curves in Fig. III–4), becomes equal to the target of 10^{-5} yr^{-1}. It is found that a HCLPF capacity of 1.02 *g* for a generic cliff edge failure mode is sufficient to screen out this failure mode by satisfying the second criterion in Section 7.2.3.4. By inspection, the HCLPF capacity needed to satisfy the first criterion (for a 10% annual frequency contribution) is higher and is therefore not governing since satisfying one criterion is sufficient for this margin adequacy assessment.

Accordingly, potential cliff edge failure events with HCLPF capacities higher than 1.02 *g* can be found by default to be adequate for a robust design that achieves the annual frequency based performance goal. An installation specific screening criterion for cliff edge failure events can be established at or above 1.02 *g*. Precise determination of HCLPF capacities for potential cliff edge failures need not be performed if they can be shown with high confidence to exceed this screening criterion. The difference between this screening criterion for generic cliff edge failure events and the corresponding 0.96 *g* found in the previous example reflects the influence of the relatively steeper lower tail of the installation-level fragility determined using the SPSA methodology compared to the generic log-normal shape anchored to the HCLPF capacity from the SMA methodology (Fig. III–3).

Objective 3:

Geotechnical investigations indicated that the site may be susceptible to seismic induced slope failure hazard. This failure mode was not modelled in the original SPSA of the design and is therefore absent from the installation-level fragility in Fig. III–3. Analysis of the consequences of potential slope failure indicates that concurrent damage to affected SSCs leads directly to an unacceptable end state. A fragility evaluation was performed for slope failure. The resulting mean fragility curve is shown in Fig. III–5 and does not have a log-normal shape. This is not uncommon when fragilities for failure modes that include severe non-linearities such as geotechnical failures are explicitly evaluated. The HCLPF capacity for slope failure is taken equal to the 1% conditional failure probability on this mean fragility curve. It is found to be equal to the 0.8 *g* HCLPF capacity estimated using deterministic methods in the previous example.

Criteria:

Follow the criteria in Section 7.2.3.2, implemented according to Section 7.2.3.3.

Solution:

Following Section 7.2.3.3, the installation-level mean fragility curve including the slope failure event is computed using the union of the original installation-level mean fragility and the slope failure fragility, as shown in Fig. III–5. This updated fragility is convolved with the mean hazard curve shown in Fig. III–5 (dark orange and grey curves). The resulting total value and increase in annual frequency of unacceptable performance are found to be the following:

$$\lambda_{f^*} = 1.02 \times 10^{-5}\ \text{yr}^{-1}$$

$$\Delta\lambda_f = 1.32 \times 10^{-6}\ \text{yr}^{-1}$$

The computed annual frequency of unacceptable performance is slightly higher than the target of 10^{-5} yr^{-1}, the second adequacy criterion in Section 7.2.3.1. The increase in annual frequency due to the cliff edge failure event is about 13% of the total, which is higher than the 10% proposed for the first adequacy criterion in Section 7.2.3.1. Strictly speaking, having not satisfied either acceptance criterion, the cliff edge failure mode would not be demonstrated to have an adequate seismic margin for a robust design. However, the extent by which the first criterion is exceeded in this example is relatively small. In a safety evaluation, it is expected to be considered of little practical significance given the uncertainty and achievable precision in the underlying calculations.

The increase in annual frequency due to the slope failure event is significantly smaller than computed under the previous example (i.e. 4.17×10^{-6} yr^{-1}) using only HCLPF capacities from the SMA output and conservatively biased fragility idealizations. This comparison demonstrates the advantage of SPSA to provide more realistic decision making input.

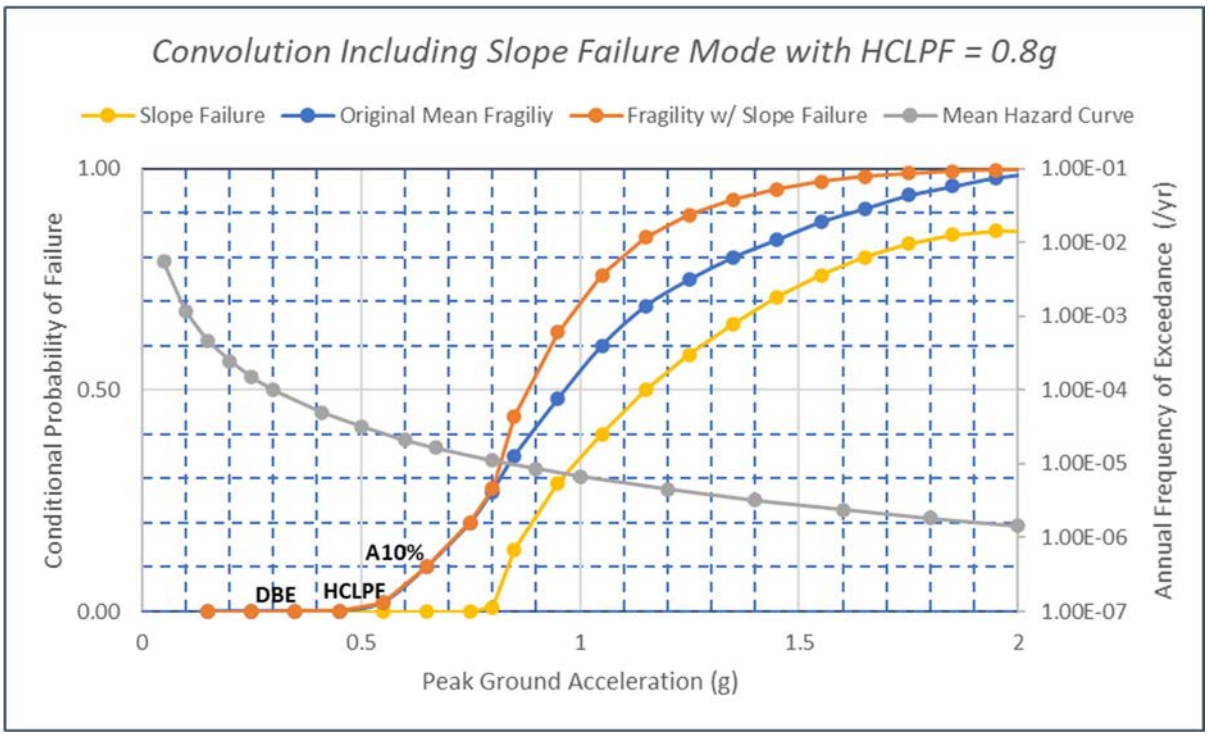

FIG. III–5. SPSA installation-level fragilities with and without slope failure fragility with 0.8 g HCLPF.

Objective 4:

Refined fragility evaluation was performed for the slope stability failure mode. As a result, the seismic fragility curve for this failure event was revised. The revised seismic fragility is shown in Fig. III–6. It was found to have a HCLPF capacity of 0.9 *g*, which is improved from the HCLPF capacity estimated using deterministic methods in the previous example. However, it is less than the 1.02 *g* HCLPF capacity determined for screening out generic cliff edge failure events earlier in this example. Reassess the seismic margin adequacy of this failure mode.

Criteria:

Follow the criteria in Section 7.2.3.2, implemented according to Section 7.2.3.3.

Solution:

Following Section 7.2.3.3, the installation-level mean fragility curve including the slope failure event is computed using the union of the original installation-level mean fragility and the slope failure fragility, as shown in Fig. III–6. This updated fragility is convolved with the mean hazard curve in Fig. III–6 (dark orange and grey curves). The resulting total value and increase in annual frequency of unacceptable performance are found to be the following:

$$\lambda_{f^*} = 9.63 \times 10^{-6}\ \text{yr}^{-1}$$

$$\Delta\lambda_f = 7.50 \times 10^{-7}\ \text{yr}^{-1}$$

The computed annual frequency of unacceptable performance is lower than the target of 10^{-5} yr^{-1}, which satisfies the second adequacy criterion in Section 7.2.3.1. The increase in annual frequency due to the cliff edge failure event is less than the 10% of the total proposed for the first adequacy criterion in Section 7.2.3.1. Satisfying either acceptance criterion is considered sufficient to demonstrate that the

slope failure has adequate seismic margin for a robust de design[37]. Comparison of this conclusion to that from Objective 2 demonstrates the advantage of performing explicit fragility evaluation vs. deterministic HCLPF capacity evaluation.

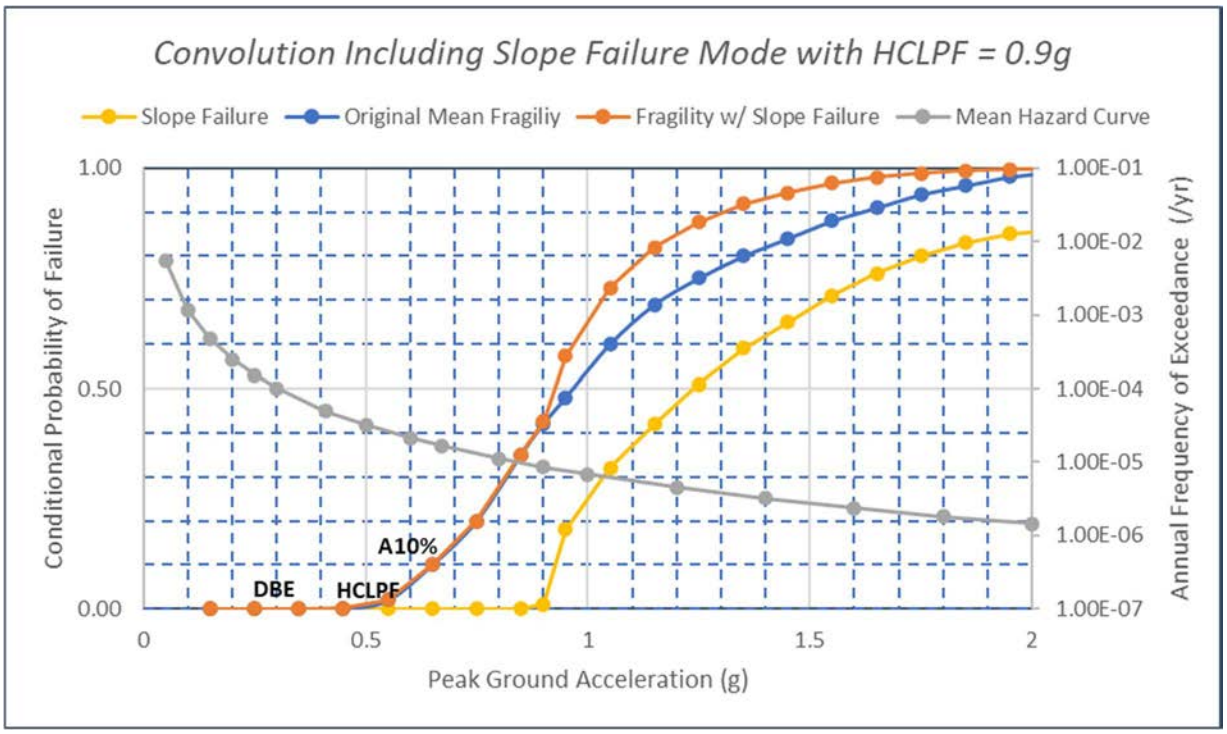

FIG. III–6. SPSA installation-level fragilities with and without slope failure fragility with 0.9 g HCLPF.

References to Annex III

[III–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Safety for Nuclear Installations, IAEA Safety Standards Series No. SSG-89, IAEA, Vienna (in preparation).

[37] In this idealized example, the significance of decreasing the mean annual frequency of unacceptable performance from 1.02×10^{-5} to 9.63×10^{-6} yr^{-1} is emphasized for illustration. In a real-life safety assessment, this difference may not be considered sufficiently significant to change qualitative conclusions, given the typical uncertainties and achievable precision in SPSA.

GLOSSARY

Cliff edge effect: An instance of severely abnormal conditions caused by an abrupt transition from one status of a facility to another following a small deviation in a parameter or a small variation in an input value.

Design: The process and the result of developing a concept, detailed plans, supporting calculations and specifications for a facility and its parts.

Design basis: The range of conditions and events taken explicitly into account in the design of SSCs and equipment of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits.

Design basis external events: The external event(s) or combination(s) of external events considered in the design basis of all or any part of a facility.

Design extension conditions: Postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits.

Design margin: For a particular external hazard, the difference between the severity of the design basis external event and the severity of an event that could reasonably start compromising the performance of the intended safety functions[38].

Diversity: The presence of two or more independent (redundant) systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of CCF, including common mode failure.

Performance goal: The performance goal for a facility in relation to a specific external event is defined as the maximum acceptable probability of failure of the facility to meet the safety requirements (shutdown, containment, cooling) in case of that external event[39]. (IAEA Safety Reports Series No. 94)

Redundancy: Provision of alternative (identical or diverse) SSCs, so that any single structure, system or component can perform the required function regardless of the state of operation or failure of any other.

*Safety assessmen*t: The process, and the result, of systematically analysing and evaluating the hazards associated with sources and practices, and associated protection and safety measures.

Scenario based external hazard: External hazard whose severity cannot be defined using a single parameter; therefore, it needs the definition of a set of parameters which, all together, define the severity. For instance, the severity of an external explosion is defined by the nature of the explosive substance, the mass of the substance, the distance to the safety buildings, the degree of confinement, etc.

Segregation: An activity where types of waste or material (radioactive or exempt) are separated or are kept separate on the basis of radiological, chemical and/or physical properties, to facilitate waste handling and/or processing.

[38] Sometimes, the *design margin* is identified with the severity of the event that could reasonably start compromising the performance of the intended safety functions.

[39] The performance goal metrics relevant to NPPs most often quoted in IAEA publications are core damage frequency (CDF) and large early release frequency (LERF). Equivalent goals can be constructed for other types of nuclear installations.

ABBREVIATIONS

ABWR	Advanced Boiling Water Reactor
AC	Alternate Current
AFE	Annual Frequency of Exceedance
BDBE	Beyond Design Basis Earthquake
BWR	Boiling Water Reactor
CAV	Cumulative Absolute Velocity
CCF	Common Cause Failure
CDF	Core Damage Frequency
CDFM	Conservative Deterministic Failure Margin
CEA	Alternative Energies and Atomic Energy Commission
DBE	Design Basis Earthquake
DC	Direct Current
DiD	Defence in Depth
EDG	Emergency Diesel Generator
ESW	Essential Service Water
HCLPF	High Confidence of Low Probability of Failure
HP	Hitachi Port (datum for heights)
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
JMA	Japan Meteorological Agency
JSCE	Japan Society of Civil Engineers
LERF	Large Early Release Frequency
MAFE	Mean Annual Frequency of Exceedance
MSL	Mean Sea Level
MUPSA	Multi Unit Probabilistic Safety Assessment
NAVD88	North America Vertical Datum (since 1988)
NGF	Nivellement General de la France (French national datum for heights)
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
OP	Onahama Peil (datum for heights, Onahama Port Construction Standard Surface)
PSA	Probabilistic Safety Assessment
PSHA	Probabilistic Seismic Hazard Assessment
PHWR	Pressurized Heavy Water Reactor
PWR	Pressurized Water Reactor
RDS	Redundancy, Diversity, and Segregation
RHR	Residual Heat Removal
SMA	Seismic Margin Assessment
SPSA	Seismic Probabilistic Safety Assessment
SSC	Structures, Systems and Components
TP	Tokyo Peil (datum for heights, average sea level in Tokyo Bay)
UHS	Ultimate Heat Sink
WMO	World Meteorological Organization

CONTRIBUTORS TO DRAFTING AND REVIEW

AZUMA, K.	Nuclear Regulation Authority of Japan, Japan
BELTRAN, F.	Belgar Engineering Consultants, Spain
COMAN, O.	International Atomic Energy Agency
CONTRI, P.	International Atomic Energy Agency
FORD, P.	Consultant, United Kingdom
GROMEK, K.	Ontario Power Generation, Canada
GÜRPINAR, A.	Consultant, Turkey
HIBINO, K.	Nuclear Regulation Authority of Japan, Japan
KOSTAREV, V.	CKTI-Vibroseism, Russian Federation
KIM, J.	Korea Hydro and Nuclear Power, Republic of Korea
LEE, H.	International Atomic Energy Agency
LEI, S.	Canadian Nuclear Safety Commission, Canada
LOPEZ, J.	U.S. Nuclear Regulatory Commission, United States of America
MAHMOOD, M.	International Atomic Energy Agency
MOOK, L.	Korea Hydro and Nuclear Power, Republic of Korea
ORBOVIC, N.	Canadian Nuclear Safety Commission, Canada
PINO, G.	ITER-Consult, Italy
REGA, J.	Tractebel, Belgium
SAMMADAR, S.	U.S. Nuclear Regulatory Commission, United States of America
STOEVA, N.	International Atomic Energy Agency
STOYANOV, G.	Canadian Nuclear Safety Commission, Canada
TALAAT, M.	Simpson, Gumpertz & Heger, United States of America
VIALLET, E.	Électricité de France, France
WU, C.	Nuclear Regulation Authority of Japan, Japan
YAMAZAKI, T.	Japan Nuclear Safety Institute, Japan

Consultancy Meetings

Vienna, Austria: 20–22 May 2020, 7–9 June 2021, 7–9 March 2022

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550

Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group

Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:

www.eurospanbookstore.com/iaea

For further information:

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

International Atomic Energy Agency
Vienna