IAEA TECDOC SERIES

IAEA-TECDOC-1834

Assessment of Vulnerabilities of Operating Nuclear Power Plants to Extreme External Events

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 on the IAEA Internet site

http://www-ns.iaea.org/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.

ASSESSMENT OF VULNERABILITIES OF OPERATING NUCLEAR POWER PLANTS TO EXTREME EXTERNAL EVENTS

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
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
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
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
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
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
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-1834

ASSESSMENT OF VULNERABILITIES OF OPERATING NUCLEAR POWER PLANTS TO EXTREME EXTERNAL EVENTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2017

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
December 2017

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Assessment of vulnerabilities of operating nuclear power plants to extreme external events / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2017. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1834 | Includes bibliographical references.
Identifiers: IAEAL 17-01131 | ISBN 978–92–0–108817–8 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Risk assessment. | Nuclear power plants — Natural disaster effects. | Nuclear power plants — Safety measures.

FOREWORD

The accident at the Fukushima Daiichi nuclear power plant, in March 2011, demonstrated the need to explore scenarios in which external hazards exceed the design basis events of a nuclear installation. Knowledge of plant behaviour during extreme event scenarios helps to improve plant safety, since potential vulnerabilities controlling the plant's capacity against such hazards can be identified and measures to limit the progression of potential accidents can be introduced.

Many Member States have already implemented actions targeted to identify quickly any weak links in the response to external hazards and to assess the plant's response if these links fail. Stress tests for EU nuclear power plants and the review by the Near-Term Task Force, established by the United States Nuclear Regulatory Commission, are salient examples. In November 2011, the IAEA released a methodology for the assessment of vulnerabilities of existing nuclear power plants to extreme natural hazards, thereby addressing one of the points in the Action Plan on Nuclear Safety, approved in September 2011 by the IAEA General Conference.

In response to the needs expressed by Member States, the IAEA decided in June 2013 to revise the methodology to generalize the method for a wider range of external hazards and to introduce the enhancements that could be identified from the research, developments and practical applications in recent years. This present publication is a result of that effort, and it provides an updated methodology for the vulnerability assessment of operating facilities to extreme external events.

The philosophy of the original methodology has been maintained; the purpose of which is to determine the strength of the hazards that could compromise safety, to identify weak points and cliff edge effects associated with each applicable hazard and to assess the time frame of the plant response once extreme events cause the more vulnerable items to fail. The methodology is designed to establish a consistent basis for the assessment, and it provides a possible harmonized approach, with results which are reproducible, consistent and based on internationally accepted good practices and processes.

This publication has been partially funded by the European Commission under the Peaceful Uses Initiative. The IAEA gratefully acknowledges this financial support. The IAEA officers responsible for this publication were F. Beltran and A. Duchac 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.

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

On 22 September 2011, the IAEA General Conference approved the Action Plan on Nuclear Safety that had been prepared by the Secretariat of the Agency after the accident at Fukushima Daiichi Nuclear Power Station [1]. The plan had been requested by a Ministerial Conference on Nuclear Safety held in June, 2011. The plan included twelve main actions, each of them with corresponding sub-actions, targeted to strengthening nuclear safety in light of the accident.

The first action in the plan was to 'undertake assessment of the safety vulnerabilities of nuclear power plants in light of lessons learned to date from the accident. Under this action, the IAEA Secretariat was asked to develop a methodology and make it available for Member States that may wish to use it in carrying out their national assessments into the safety vulnerabilities of nuclear power plants. The methodology was published in November, 2011. It addressed the assessment of vulnerabilities against two external hazards: earthquake and flooding.

The accident at Fukushima Daiichi Nuclear Power Station triggered a series of actions in many Member States, which were completed after the publication of the methodology or are still in progress. Particularly relevant are the following developments:

(1) The Stress Tests performed on European nuclear power plants during years 2011 and 2012 [2, 3];

(2) Activities in the United States of America derived from the Near-Term Task Force (NTTF) recommendations to the United State Nuclear Regulatory Commission (US-NRC) [4], with actions already implemented or planned [5];

(3) The safety assessments made during years 2011 and 2012 by the member countries of the Ibero-American Forum of Radiological and Nuclear Regulatory Agencies (FORO) having nuclear plants (Argentina, Brazil, Mexico and Spain);

(4) Comprehensive safety examinations for operating plants and plants under construction in China, carried out in 2011 [6];

(5) Activities in Canada derived from the regulatory integrated action plan on the lessons learned from the Fukushima Daiichi nuclear accident [7], with actions already implemented or planned.

Exchange of experiences during post-Fukushima safety assessments has taken place in a number of international meetings [8, 9], including an extraordinary meeting of the Convention on Nuclear Safety [10]. Those meetings have also contributed to disseminate new insights into the Fukushima Daiichi accident, and into the performance of other Japanese plants, which were also subjected to strong motion and tsunami and did not develop an accident (e.g. Fukushima Daini and Onagawa stations). In addition, international collaborative research programmes on severe external hazards and their effects on nuclear power plants were started by several organizations shortly after the accident and the outcome of them started to be available by the end of 2013.

In June 2013, based on the needs expressed by Member States, the IAEA Secretariat decided to revise the methodology published in 2011, in order to generalize the method for a wider range of external hazards and to introduce the enhancements that could be identified from the research, developments and practical applications in the recent years.

This publication expands the previous version by giving a more comprehensive approach, covering the selection of applicable hazards for a specific site; the selection of the components whose capacity is to be assessed for each applicable hazard and methods to assess plant performance after plant capacity

against a particular hazard is exceeded. In addition, guidelines for independent review and a self-assessment questionnaire are included in the revised publication.

The Fukushima Daiichi accident showed the need to explore scenarios where external hazards exceed the design basis. Knowledge of plant behaviour along those scenarios helps improve global safety, since the weak points can be identified, and measures to limit the progression of potential accidents or to mitigate their consequences can be introduced. This is the underlying philosophy of the present publication: the focus is to identify what can go wrong in an existing installation when external events exceed the design basis. The approach provides insights not readily obvious from the design process, where the main focus is on addressing the design basis. The Fukushima Daiichi accident was the result of an external hazard (tsunami), which significantly exceeded the design basis. The tsunami flooded the plant buildings up to a very high elevation and it rendered electrical safety systems inoperable. This scenario had not been considered and no provisions had been made for it. The basic resources that were necessary to maintain the fundamental safety functions were lost due to the unavailability of electrical power, resulting in an unmitigated accident progression. This eventually resulted in the loss of control over the installation and the associated radioactivity release.

The assessment of an operating nuclear power plant (NPP) against extreme external events needs therefore to review the response of the installation to the events, in order to identify how the loss of control over the installation, triggered by an extreme external event, could develop. As a result, the weaker structures, systems and components (SSCs) will be identified; and overall safety could be improved in an optimal way by the implementation of measures to address these weak links.

In addition to establishing the weaker SSCs against specific hazards, the assessment needs to consider the progression of the scenarios after the weaker SSCs fail. In this manner, it will be possible to estimate the evolution in time of the resulting accident, under the conditions of the extreme events defined in this publication. The assessment will then identify the plant components governing the times at which releases are to be expected, if any. This assessment will provide valuable insights, even if the accident scenarios are thought to be of a very low probability. This is, for example, the philosophy underlying the European Stress Tests, Refs [2 and 3].

An analysis, in which the strength of an external hazard is driven to a level which causes an accident, with independence of the annual frequency of exceeding this strength, will identify more vulnerable points of the NPP. However, such an assessment will give no indication about the actual risk posed by the installation. Obtaining a risk estimate requires, in addition, a determination of the frequency of exceedance of several levels of hazard strength at the site.

Hazard frequencies required for estimating risk could include a significant amount of uncertainty. However, it has to be recognized that more complete approach to decide on whether a safety margin for a particular hazard is large enough, and on how far plant improvements could go, is to compare the risk estimates with the safety goals set by the national authorities. Therefore, a methodology for vulnerability assessment (i.e. finding the weak links), such as the ones presented in this publication, will normally be supplemented by the estimation of the frequencies of exceedance of hazard strengths and the convolution of plant capacity with hazard frequencies in order to obtain, at least, point estimates of the risk metrics.

The methodology proposed in this publication does not aim at forming an exclusive basis for application in Member States. Given the uncertainties involved in certain extreme external events and the different strategies for risk mitigation utilized by the utilities, it is acknowledged that other approaches exist that may contribute to effective risk mitigation.

1.2. OBJECTIVE

The purpose of the methodology presented in this publication is threefold:

(1) Identify the plant more vulnerable aspects (‘weak links’) for the applicable extreme

external events, that is, the structures, systems and components (SSCs) more vulnerable to external events exceeding the plant design basis;

(2) Determine the severity of the external event below which there is a high confidence that the 'weak links' will not fail;

(3) Explore the plant response when those 'weak links' fail and estimate the time frame until reaching fuel damage, together with the SSCs governing the time frame.

In the present context, the 'weak links' can be designated as 'vulnerabilities', this term meaning an item which is 'less strong' against the external hazard. Hence, in the present context, every plant will have its 'vulnerabilities' or 'weak links', and 'vulnerability' does not necessarily mean non-compliance with a regulatory requirement.

The methodology is designed to establish a consistent basis for the vulnerability assessment against extreme events. It furnishes an approach intended to provide the utilities of the Member State and their Regulator with results which are reproducible, consistent and sound, based on accepted international practices and processes.

The methodology is particularly suitable when:

- Low capacity SSCs controlling overall plant's capacity need to be identified for the applicable hazards;
- Sufficient margin against potential cliff-edge[1] effects needs to be demonstrated;
- There is an interest in obtaining the progression in time for losing the fundamental safety functions and having fuel damage, once the more vulnerable SSCs have failed and taking into account the actual site conditions after the extreme event.

In some contexts, the methodology can be used to determine in a systematic way which hazards could have a major contribution to risk and the SSCs more vulnerable to them. After this determination, depending on the Member State goals, many of the potential hazards could be eliminated from further evaluation; whereas the results regarding the hazards not eliminated could then be used as a first round for more sophisticated methods.

1.3. SCOPE

This methodology is intended to be used for existing nuclear power plants (NPPs) in their 'as-is' condition. The 'as-is' condition of an NPP refers to the present state and actual conditions of the NPP, considering the 'as-built', 'as-operated' and 'as-maintained' state of structures, systems and components [11]). As it is presented in this publication, the methodology takes into account the 'as-is' condition to find the capacities against events for which the NPP might not have been designed. Finding the 'as-is' condition normally implies that the methodology cannot be applied just based on document review, it requires the performance of plant walk downs.

The methodology covers the impact of all types of external events, both natural and human induced, except for wilful human induced events (i.e. not accidental), such as military action or industrial sabotage.

The methodology has been designed for plants operating 'at power', that is, with the reactor being critical and producing power. However, the approach would remain basically the same for other operating mode, the differences being only in the output from the activities related with systems analysis. Once the safety significant components for a particular operating mode have been selected, the methodology is the same as for the 'at power' mode. The methodology is able to accommodate

[1] In the context of this publication, a 'cliff-edge' effect refers to a situation in which a small increase in the hazard severity produces the widespread failure of plant structures, systems and components, corresponding to a sharp increase in risk.

longer grace periods during shutdown states or increased vulnerability to certain external hazards due to service or maintenance operations (e.g. additional flooding routes).

The intended users are the organizations operating the plants, supported by external experts if necessary.

Based on engineering judgement, the methodology could be adapted for use in other nuclear installations, such as research reactors and fuel cycle facilities, provided that the basic philosophy is maintained.

The methodology does not assess the accident management. It focuses on the performance of fundamental safety functions and on how and when these functions could be lost after an extreme event. If the impact of extreme external events propagates into a severe accident, guidance on severe accident management can be sought in the Ref [12].

It is to be noted that a vulnerability assessment as described in the present publication is not a safety assessment. A safety assessment is carried out to ensure that all relevant safety requirements are met [13]. In contrast, the vulnerability assessment described herein is targeted to explore the behaviour of the plant during extreme external events, which exceed the design basis, and to identify the more vulnerable points. The methodology does not check compliance with any safety requirement. Verification of compliance with whatever applicable safety requirement is out of the scope of the methodology.

1.4. OVERVIEW OF THE METHODOLOGY

This section provides the reader with an overall perspective of the methodology which is going to be developed in the following section.

The general workflow is given in Figure 1. The process starts from a comprehensive list of potential external hazards (ensemble of external hazards).

Using a given set of screening criteria and conservative bounding analyses, the list is screened in order to eliminate from the assessment those hazards that do not need to be analysed further. The screening criteria and bounding analyses are similar to those used in other contexts related with design or safety assessment [14-16].The only significant difference is that, except for extraordinarily rare events (e.g. large meteorite impact), the low frequency of occurrence cannot be used to screen-out a hazard at this stage. The approach is that, in general, the vulnerability assessment needs to be performed for events that are physically possible, even if they are thought to be of a very low probability. The intent here is to eliminate the possibility of screening-out a hazard from the very beginning on the basis of a frequency of occurrence which has been obtained with a large uncertainty, or (unknowingly) from incomplete or outdated information.

For a typical plant, it is expected that only a small number of hazards will need to be considered for a detailed vulnerability assessment.

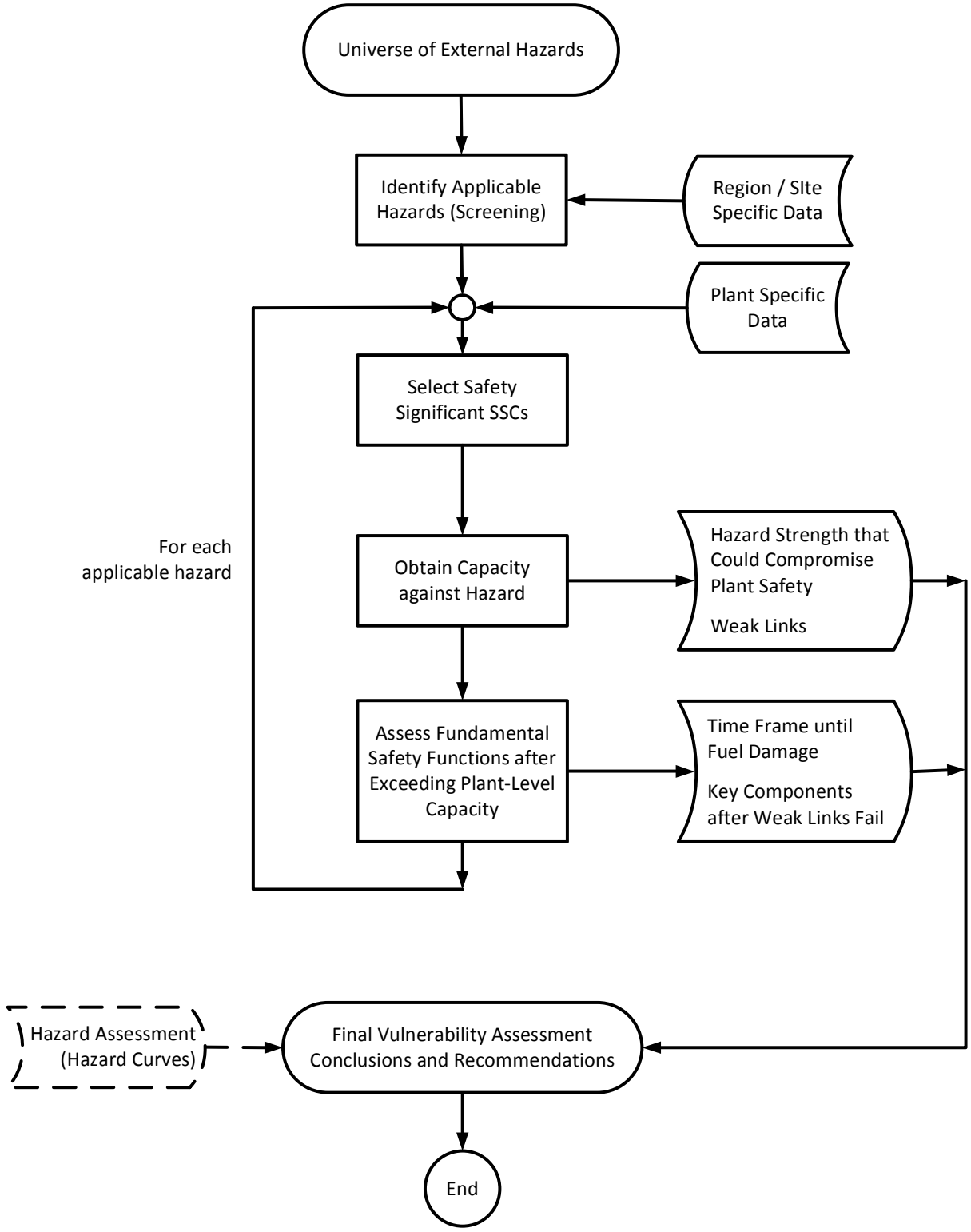


FIG. 1. Workflow of the vulnerability assessment.

For each of the applicable external hazards, the next step is to identify the SSCs required to maintain the fundamental safety functions in case of an event derived from the hazard. Following current international practice for assessment of beyond design basis external events, two approaches are given for this purpose: the so-called 'success path' approach [11, 17-19]; and the event tree–fault tree approach, which takes advantage of the plant logic models developed for Probabilistic Safety Assessment (PSA) studies [11, 18, 20].

From past experience in assessing beyond design basis external events (e.g. in the Individual Plant Examination of External Events (IPEEE) programme defined in Ref [21]), it is very likely that an envelope list of SSCs can be defined, covering all applicable hazards. For a typical plant, this list is expected to include in the order of several hundreds of items.

Once the required SSCs are identified, capacities are obtained from each of them. The targets here are the high confidence capacities; that is, for each item in the list of SSCs, the maximum strength of the hazard under which there is a high confidence that the item will maintain its intended safety functions. After ranking the SSCs on the basis of capacity, the SSCs with a lower capacity are the vulnerabilities or 'weak links' against the hazard. This constitutes the first output of the vulnerability assessment.

The capacity of the weaker SSCs can be used to compute the plant-level capacity; that is, the maximum strength of the hazard below which there is a high confidence that the plant will maintain the fundamental safety functions. This will be designated 'plant capacity' level and constitutes the second important output of the vulnerability assessment. In a deterministic sense, if the extreme external event has strength smaller than the capacity of the plant, then no safety significant consequences are to be expected.

Two methods are given to compute the plant-level capacity from the capacities of the individual components, depending on the approach used for selecting the SSCs. One is deterministic (Section 4.2) and the other, semi-probabilistic (Section 4.3).

Once the weaker SSCs against each applicable hazard have been identified, the next step of the assessment assumes failure of the weaker items and looks into the plant response to those failures, taking into account the likely conditions of the site after the extreme event (e.g. site devastation, access routes cut-off, etc.) and considering auxiliary or movable equipment included in the plant procedures that might remain available. This analysis is deterministic: after the failure of the weaker SSCs, a sequential and progressive loss of the remaining systems is postulated, once their operation is no longer possible (e.g. batteries depleted, tanks emptied, reservoirs depleted, etc.). The timing (time milestones) of the resulting sequence of events, until reaching fuel damage or a long term stable plant condition, is a key result of the exercise.

The methodology will then identify the vulnerabilities against the applicable extreme external events. However, unless the results of the corresponding probabilistic hazard assessments are available, the methodology will not be able to provide any indication about the actual risk posed for the installation. It is expected that the easy fixes of weaker SSCs will be implemented without further considerations. But, as mentioned above, the decision about whether a major fix has to be implemented normally needs to be based on the comparison between the actual risk and the safety goals established at each Member State.

When the results of probabilistic hazard assessments are available (hazard curves), the plant level capacity obtained for each applicable hazard as described above could be used to obtain a point estimate for the annual frequency of the hazard causing safety significant damage. For each hazard, the approach involves the computation of a plant-level fragility curve from the high confidence plant-level capacity and the convolution of this fragility curve with the mean hazard curve (Section 10-B-9 of Ref [16]). This approach has already been followed by regulators in some Member States to obtain quick risk estimates [22].

Throughout this process of risk identification and mitigation, the operating organization needs to maintain an approach of maintaining risks as low as reasonably practicable. This is particularly important in the assessment of extreme external events, where significant investments of resources are possible.

1.5. STRUCTURE

The rest of the publication is organized into eight additional sections, two appendices and three annexes.

Section 2 is devoted to the process of selection of the hazards relevant to a particular site. The section includes a comprehensive list of potential external hazards, possible hazard combinations and the rules for screening this list in order to identify the hazards that could be significant for a particular site.

Section 3 describes the approaches for selection of the SSCs to be considered during the capacity assessment.

Section 4 gives the general methodology for capacity assessment, whereas Section 5 particularizes the methodology for five specific hazards: earthquake, high winds, flood, aircraft impact and explosion/hazardous releases.

Section 6 provides the approach for assessment of the performance of safety functions once the more vulnerable components for a particular hazard have failed.

Section 7 gives guidance on how to obtain estimates of risk from the plant level capacities obtained as described in Sections 4 and 5. Firstly, the section gives an overview on probabilistic hazard assessments, corresponding to hazards that commonly result to be significant in existing nuclear plants. Guidance on hazard assessment is given by reference to the relevant IAEA safety standards and other technical documentation. The second part of the section describes the development of a plant-level fragility curve from the results of the vulnerability assessment and how it can be used to obtain an estimate of risk.

Section 8 provides a summary of the results expected from the overall vulnerability assessment.

Finally, Section 9 is devoted to the composition and personnel qualification for the team responsible for the assessment.

Appendix A includes guidelines for an independent review of the work performed according to the previous sections. It gives the main points of the process to check the application of the methodology.

Appendix B provides a self-assessment questionnaire, intended to be a tool for an internal review of the work performed to assess the vulnerability against external hazards, previous to an external independent review.

Annex 1 includes the definition of the external hazards considered in Section 2 and Annex 2 gives examples of preliminary screening of hazards for typical sites. Annex 3 provides further insights in the form of a commentary about particular aspects of the overall methodology. Annex 4 illustrates the process of SSC selection (Section 3) by means of an example.

Finally, the references cited along the publication and a Glossary of terms is given at the end of the publication.

1.6. USE OF THIS PUBLICATION

The main body of this publication is intended as guidance for the engineering team implementing the methodology. It describes the different steps, the expected outcome at each step and the requirements for the team performing the study. The publication is not completely self-contained. Due to space limitations, Section 5 (capacity assessment for a selection of hazards) and Section 7 (hazard assessment) make reference to other publications for a detailed guidance.

Appendix A provides guidance to the team performing an independent review of the vulnerability assessment. This appendix highlights the key points that have to be checked during the review in order to have a reasonable assurance that the vulnerability assessment has been carried out according to the present publication.

Appendix B is intended as a check list for self-assessment of compliance with methodology and the intended output. It can be used as guidance for an internal review or as self-test before the independent review.

The methodology for plant capacity assessment presented in this publication is, in many aspects, a generalization of methods that have been in use for seismic assessment since the 1980s. Experience in the application to hazards other than seismic is more limited. The commentary in Annex 3 provides insights about key issues regarding this generalization to other hazards.

2. SELECTION OF APPLICABLE HAZARDS

2.1. UNIVERSE OF EXTERNAL HAZARDS

A comprehensive list of external hazards (universe of hazards) is given in Table 1. For compiling the list, a large number of references have been considered (Refs [14-17, 21, 23-39].

Hazards are given in order of decreasing number of references citing them. Note that only the hazards are listed, not the consequences of the hazards. For instance, the blockage of a reservoir or of a cooling tower is not a hazard by itself, but the consequence of other hazards such as a ship impact, the formation of ice (frazil ice), bio-fouling at the screens or the accumulation of debris during a flood.

Wilful human induced hazards (i.e. not accidental), such as military action or industrial sabotage, have been excluded, since they are out of the scope of the methodology. A more detailed description of the hazards that appear in Table 1, and of the associated phenomena, can be found in Annex 1.

2.2. HAZARD COMBINATIONS

Hazard combinations are to be considered in the assessment when the two following conditions are met:

(1) The combination is credible for the site. Credibility could be judged based on the knowledge of the phenomena and on the operating experience in Member States;

(2) The combination has a damage potential significantly larger than any of the combined hazards considered separately.

Note that credibility in the present context is always associated to a common physical phenomenon at the origin of the hazards. For example, seismic ground motion hazard at a site and tsunami hazard at the same site is a credible hazard combination, since both hazards would have a common origin, a fault rupture at the seabed. Simultaneous occurrence of extreme events not linked by causality needs to be considered in the assessment only when a high degree of correlation exists between those extreme events.

As a matter of example, the combinations given in the following are considered to be credible [31-32, 34, 39-40]:

- Earthquake and flood. This is a situation in which the site is affected by an earthquake, which at the same time triggers a flood mechanism. The flood may be produced by a tsunami (coastal sites), a seiche (lake sites) or by a dam break or landslide caused by the earthquake (river sites). The time is different for the earthquake and for the flood. That is, both events will not take place at the same time. The flooding of the site will develop some time after the earthquake has affected the NPP and potentially damaged structures, systems and components. The time difference will depend on the distance to the natural or man-made structure causing the flood (e.g. subduction fault, failed dam). It can vary from a few minutes to several hours.
- Earthquake and depletion of reservoir. This possibility applies to river sites. In this situation the site is affected by an earthquake, which at the same time damages a water retaining structure located downstream of the site or produces a blockage upstream of the river used as ultimate heat sink. The depletion of the reservoir will take place after the earthquake has affected the plant and potentially damaged SSCs. The time difference will depend on the volume of the reservoir and the degree of damage at downstream or upstream structures.

TABLE 1. LIST OF EXTERNAL HAZARDS (CONT.)

Hazard	Class*	Phenomena associated with the hazard
Earthquake	N	Ground shaking. Liquefaction or other gross soil failures Surface faulting at the site
High winds ('straight' winds or tropical cyclones)	N	Wind pressures/suction on exposed SSC Windborne missiles
Flood due to meteorological causes	N	Local extreme precipitation. Run-off from precipitation or snow melt. Storm surge / High tide / Wind waves.
Tornado	N	Wind pressures/suction on exposed SSC Windborne missiles Atmospheric pressure change
Flood due to long period water waves	N	Tsunami / Meteotsunami Seiche / Tidal bore Landslide onto water body.
Flood due to failure of water control structures	N, H	Dam failure Levee or dike failure Failure of external onsite water impoundment
Explosion	H	Accident on-site or in nearby facilities Accident on nearby road / railroad / navigation channel Accident in a nearby pipeline
Release of hazardous substances (toxic, asphyxiant, corrosive or radioactive)	H	Accident on-site or in nearby facilities Accident on nearby road / railroad / navigation channel Accident in a nearby pipeline.
Extreme temperatures	N	High summer temperature Low winter temperature
Aircraft crash	H	Direct impact of aircraft. Fire and explosion
External fire (forest, hydrocarbon storage, nearby factories)	N, H	Smoke and ash generation Propagation and possible entrance to site

(*) N = Natural; H = Human Induced

TABLE 1. LIST OF EXTERNAL HAZARDS (CONT.)

Hazard	Class*	Phenomena associated with the hazard
Volcanic tephra fallout	N	Fall and deposition of pyroclastic material such as ash, pumice and scoria, which may take place at a long distance from the volcano.
Volcanic activity	N	Opening of new vents
		Ground deformation
		Volcano generated missiles/gases/aerosol
		Pyroclastic density currents. Lava flows.
Lightning	N	Lightning strike
Slope instability	N	Landslides
		Rock slides
		Snow avalanches
		Landslide downstream that blocks river and causes backwater effect to the site
Hail	N	Direct impact
		Accumulation in roofs
Extra-terrestrial activity	N, H	Meteorite strikes
		Satellite falls
Abrasive windstorms (dust storms and sandstorms)	N	Reduced visibility
		Accumulation of sand or dust. / Abrasion
		Malfunction of sensitive equipment outdoors
Ship/barge impact	H	Direct impact of ship/barge
		Release of hazardous substances
		Contamination of cooling water
Collision of floating bodies	N	Impact of floating debris or ice
Foundation ground instability	N, H	Collapse due to karst / caverns
		Subsidence due to water or oil wells
		Expansive soils. / Consolidation
Electromagnetic interference	N, H	Malfunction of electrical/electronic devices due to on-site or off-site electromagnetic emission.
		Note that the source of the electromagnetic disturbance can be extra-terrestrial (solar storms).

(*) N = Natural; H = Human Induced

TABLE 1. LIST OF EXTERNAL HAZARDS (cont.)

Hazard	Class*	Phenomena associated with the hazard
Blockage or diversion of river	N, H	Obstruction upstream of river channel by landslides or by jams caused by ice, logs, debris or volcanic materials.
Biological phenomena	N	Growth of algae/mussels/clams at intake Clogging of intake by fish or jellyfish Clogging of air filters by leaves/insects.
Depletion of a reservoir	N, H	Loss of the water body used as Ultimate Heat Sink due to natural (drought) or human induced (dam break) causes
Freezing precipitation, ice and frost related phenomena	N	Formation of layers of ice at exposed surfaces Formation of frazil ice and pack ice (blockage of water intakes or damage to intake structures).
Extreme snow-fall and snowpack	N	Accumulation of snow in roofs and at grade level Blockage of air intakes
Variation of groundwater level	N	Change in water pore pressures which may affect soil stability, increase forces on embedded structures or it may favour seepage through walls and foundation slabs.
Saltspray/Saltstorm	N	Salty winds blowing from the sea during severe storms, resulting in electrical arches or grounding, leading to short circuits, fires and loss of power.
Waterspouts	N	Same as tornadoes Transfer of large amounts of water to land from nearby water bodies

(*) N = Natural; H = Human Induced

- Earthquake and damage to nearby hazardous facilities. This possibility corresponds to an earthquake affecting the site and the nearby facilities. Damage in the nearby facilities may induce the release of hazardous substances, explosions and fires at those facilities. Note that another nuclear unit in a multi-unit nuclear site can be considered a nearby hazardous facility. In most cases, the effects of the releases, explosions and fires on the NPP will not be simultaneous with the ground shaking. That is, they will occur, at most, shortly after the earthquake.
- High winds and flood. Operating experience shows that, especially at coastal sites, high winds and flood due to meteorological causes tend to occur simultaneously, since both phenomena have a common origin. Typically, a tropical or extra-tropical cyclone produces strong winds, together with high wind waves and a storm surge that increases the average sea water level. Accumulation of debris and organic material (algae) at the water intakes also occur as a result of the high water level.
- High winds and damage to nearby hazardous facilities. This combination corresponds to strong winds affecting the site and the nearby facilities. Damage in the nearby facilities induces the release of hazardous substances, explosions and fires at those facilities which could affect the nuclear site. A nuclear unit in a multi-unit nuclear site can be considered a nearby hazardous facility.
- High winds and lightning. The simultaneous occurrence of strong winds and lightning is very common and it has been reported at many nuclear sites. It can be argued that lightning does not make damage potential significantly larger than the damage potential

of strong winds alone. However, lightning causes malfunction of electrical systems and increases likelihood of loss of off-site power and fires. The combination of high winds and salt-spray has also been reported at some coastal nuclear sites. However, the effects of this combination can be considered to be similar to the ones resulting from the combination of high winds and lightning.

- High winds and snow fall. The simultaneous occurrence of strong winds and heavy snow fall (blizzard) is also part of operating experience for plants located in cold areas.
- High winds and biological phenomena. Operating experience in coastal sites shows that high winds can be associated with anomalous accumulation of aquatic organisms, such as algae, or seaweed.
- External fire and aircraft crash. Operating experience shows that for sites with nearby forests, the use of airborne extinguishing media during forest fires could reasonably lead to an aircraft impacting the NPP. On the other hand, the reverse is also true, a crash of a large aircraft will cause in all probability an external fire.
- Extreme temperature (hot) and high wind. Hot weather can cause deeper sag of conductors and wind induced loads and swinging could then cause short circuits, large mechanical stresses in towers, etc. NPP and offsite power grids 'tired' by several days of hot weather can be affected by a fault caused by high winds.

This list of combinations reflects current operating experience but it cannot be considered as exhaustive. Potential hazard combinations can be very site specific. Identifying credible combinations for a particular site will normally be carried out after the site specific screening of hazards described in Section 2.3. Each screened-in hazard will then be checked with respect to all other screened-in hazards to see if there could be a common physical origin at that site. If a common physical origin is found for extreme events derived from the two hazards, then the vulnerability to the combination of hazards will need to be assessed.

2.3. SITE SPECIFIC SCREENING OF HAZARDS

2.3.1. Purpose of screening

The purpose of the screening is to eliminate from further assessment the external hazards or combination of hazards that cannot have safety consequences in a particular site.

Following the general practice, screening can be performed in two steps:

(1) Preliminary screening, based on qualitative criteria, which eliminates from the assessment those hazards that clearly will not have safety consequences or whose consequences are enveloped by other hazards (Section 2.3.2);

(2) Bounding analyses, which use simple conservative calculations to show that the worst case possibility of a particular hazard or a combination will not have safety consequences (Section 2.3.4).

The significance of a hazard is site specific, even though there are some hazards that are significant in the vast majority of sites. Consequently, the screening is installation-specific. It depends on the particular site and on the particular installation layout.

It is to be noted that even if an individual hazard is screened out, it may still contribute to a combined event scenario. This needs to be evaluated. Even if a hazard has a negligible individual effect, it may produce a significant effect when combined in a credible way with other hazards. Such hazards are not to be screened out from the credible combinations.

It is emphasized that screening of hazards needs to be based on updated site and regional data. Updated data can be very different from the data used during the design of the NPP, especially for human induced hazards or meteorological hazards for which only a limited number of site specific records were available in the design phase.

Updated hazard data may always be looked at with a 'critical eye'. The analyst may look for instances where the currently available evidence might be in contradiction with the hazard level considered in the design basis external events. It could happen, for example, that existing facilities have accumulated additional data since construction and first operation that indicates an increase in the frequency of events and/or an increase in the potential severity of an extreme event.

2.3.2. Preliminary screening criteria

A set of screening criteria is defined to minimize the possibility of omitting significant hazards while, at the same time, reduce the amount of required vulnerability analyses to manageable proportions.

For screening out an external hazard from the vulnerability assessment, any one of the following qualitative criteria provides an acceptable basis:

Criterion 1: The hazard is of equal or lesser damage potential than the events for which the installation has been designed. This criterion is purely deterministic and requires an evaluation of plant design basis in order to estimate the resistance of plant structures and systems to a particular external hazard.

Criterion 2: The hazard could not result in worse consequences than the consequences of other hazard which has not been screened out.

Criterion 3: The events associated with the hazard cannot take place close enough to the installation to affect it. Either the events are physically impossible at the site or they cannot be strong enough to affect the NPP.

Criterion 4: The hazard is included in the definition of another hazard which has not been screened out.

Criterion 5: The hazard corresponds to events that are slow in developing and it can be demonstrated that there is sufficient time to eliminate the source of the threat or to provide an adequate response.

Note that, based on Criterion 1, any hazard not able to challenge plant normal operation will be automatically screened out.

These criteria are the same that are used for preliminary screening in probabilistic safety assessments against external events [16], except for Criterion 2. In the Criterion 2 stated here, no consideration is given to the comparison with the probability of occurrence associated to other hazards[2].

Note that the criteria above do not depend on the probabilities of occurrence associated to the hazards. This fact makes the results of the preliminary screening more robust, since the estimation of probabilities at the level of the screening thresholds commonly used in practice[3] is subject to a large degree of uncertainty.

These preliminary screening criteria apply to a single reactor as well as to multi-unit sites, since the criteria are applied at the external hazard level.

Annex 2 provides examples of application of the preliminary screening criteria to typical sites.

[2] Criterion 2 in Ref [16] states that the hazard can be screened out if it has a significantly lower mean frequency of occurrence than another hazard, taking into account the uncertainties in the estimates of both frequencies, and the hazard could not result in worse consequences than the consequences from the other hazard.

[3] In some Member States, a commonly used threshold screening criteria is an annual probability of exceedance of 10^{-7}. Events shown to be less frequent than this threshold are screened out from further consideration.

2.3.3. Plant and site review

The application of the screening criteria for a given external hazard needs to be based on the review of updated information about the site, the installation and its design basis.

Certain level of judgement may be exercised in the application of the screening criteria, in order not to defeat the purpose of this stage of the assessment. For exercising this judgement, the hazard analyst has to be aware of the recent experiences regarding external hazards not only at the site and its surroundings, but also worldwide. The independent review is expected to verify and endorse this screening based on regional information, plant specific and site specific information (Appendix A).

The preliminary screening according to the criteria of section 2.3.2 could be validated by a walk down of the site and its surroundings. The walk down needs to confirm the basis for the screening-out of the hazards that have been eliminated from further study, especially when the screening-out has been based on the specific plant layout.

The walk down is commonly used also for collecting additional data for further analysis of external hazards not screened out.

2.3.4. Bounding analyses

For external hazards that are not screened out using the screening criteria of section 2.3.2, a second level of screening could be introduced using bounding analysis. This second level of screening is not qualitative anymore: it is based on simple conservative calculations. Again, the purpose is to efficiently use resources to screen out some external hazards, so that more attention could be paid to the remaining (not screened-out) hazards.

In the context of the present vulnerability assessment, a bounding analysis is a simple upper bound calculation intended to show that the worst case possibility of a particular hazard will not have safety consequences (i.e. damage to safety significant components). Hence, the key point is that the analysis may demonstrably use assumptions such that the computed outcome is conservative with respect to the expected worst case outcome.

For example, if one site is close to a chemical plant in which solid explosive substances are stored, the analyst could assume that the maximum mass of explosive material stored at the facility is kept together at the same position and that this position is at the point closest to the nuclear installation. Then, if the analyst computes under this assumption the amplitude of the explosion pressure wave, reaching the safety buildings and it is below the threshold of damage to the components (Table II-2 of Ref [30]), then the hazard of explosion at the nearby chemical plant could be screened out based on this bounding analysis.

Note that bounding analyses here needs to only consider physical phenomena, with independence of the probability of the events. The intent here is to eliminate the possibility of screening-out a hazard on the basis of a frequency of occurrence which can only be estimated with a very large uncertainty or which has been obtained (unknowingly) from incomplete or outdated information.

An exception to this general criterion could be taken for very rare events, for which there is wide consensus worldwide that consideration is not needed within nuclear safety analyses. This is the case, for example, of hazards derived from extra-terrestrial activity (meteorite strikes or satellite falls). In the context of the present publication, an event can be considered to be ‘very rare’ at a particular site when it can be shown that the frequency of occurrence is less than about 10^{-9} per year.

2.3.5. Results

As a result of the screening process described in the previous sections, a list of hazards and hazard combinations will be kept for further analysis. Screened-out hazards and screened-out combinations will not be given further consideration. Screened-out hazards will be considered hazards with no potential safety consequences at the site.

As pointed out in Section 8, the site specific screening of hazards and especially the bases for screening out hazards and hazard combinations need to be published with sufficient detail and quality to allow independent assessment.

3. SELECTION OF COMPONENTS

3.1. GENERAL

The first step in the assessment of plant vulnerabilities against an applicable hazard is the selection of structures, systems and components (SSCs) to be considered with regard to the hazard.

The SSCs which are included in the initial scope setting are those SSCs required to maintain the fundamental safety functions during a specified period of time, for a set of plant initial conditions induced by each applicable hazard. The period of time, sometimes called 'mission time', depends on the time required to reach a stable or controlled plant state and on the time assumed to be necessary for the external assistance to reach the NPP.

The fundamental safety functions are defined in Ref [41]:

(1) Control of reactivity;
(2) Removal of heat from the reactor and from the fuel store;
(3) Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

In addition to SSCs required for the fundamental safety functions, the scope setting has to also include other SSCs which failure could lead to the failure of SSCs performing these functions.

Hence, the starting activity for the selection of SSCs is the identification of the initial conditions which may be induced from each of the applicable external hazards and could challenge the plant's ability to perform the fundamental safety functions. The selection of SSCs depends on a hazard magnitude, SSC design, plant grade, plant layout, etc. For example, the external hazard could be an aircraft crash and the initial condition caused by the aircraft crash could be a loss of off-site power, if the aircraft strikes on the station switchyard, or a loss of the primary heat sink, if it strikes on the intake structure. A strike on the spent fuel storage building may result in a spent fuel pool failure.

Note that induced initial conditions can be different from one external hazard to the other. Table 2 provides a suggested list of induced initial conditions normally associated to each hazard, which can be used for the purpose of selecting the SSCs. These conditions correspond to low-medium severity scenarios typically already taken into account in the design or in later safety assessments. Within the present methodology, they are considered just as plant initial conditions. As described in the following sections, the methodology will find out how, when the hazard strength exceeds a threshold, the initial conditions can evolve into a more severe scenario. For instance, the loss of off-site power (LOOP) that appears in Table 2 can evolve into a station black-out (SBO) scenario if power back-up sources (e.g. diesel generators) fail at a certain level of external flood.

Once the induced initial conditions are identified for a particular hazard, two approaches can be used for the selection of SSCs required for the hazard: the 'success path' approach and the 'event tree/fault tree' approach, as described in the following sections. These approaches have been extensively used in the context of seismic margin assessments [11, 19, 20, 42].

The list of selected SSCs for each hazard gives the scope of the work for the capacity evaluation corresponding to the hazard. The required effort strongly depends on how large this list is (i.e., the number of SSCs that have to be evaluated).

The following components are examples of items which will normally need to be selected:

- Items whose failure could directly or indirectly cause accident conditions after the postulated initiating event;

- Items required for shutting down the reactor, maintaining the reactor in a shutdown condition, removing residual heat over the required period of time and monitoring parameters essential to these functions;
- Items not related with the operation of the reactor, but which can pose a radiological hazard (e.g. spent fuel);
- Items required to prevent or to mitigate non-permissible radioactive releases.

TABLE 2. INITIAL PLANT CONDITIONS ASSOCIATED TO EXTERNAL EVENTS WITH LOW-TO-MEDIUM SEVERITY (TO BE USED ONLY FOR THE PURPOSE OF SELECTION OF SAFETY SIGNIFICANT COMPONENTS)

Plant initial conditions	External hazards for which plant initial conditions apply
Loss of off-site power AND Small loss of coolant accident	Earthquake
Loss of off-site power AND Loss of 'soft' exposed systems and components	High winds Tornado Abrasive windstorms (dust storms and sandstorms)
Loss of off-site power AND Loss of primary ultimate heat sink	Flood due to long period water waves Flood due to failure of water control structures Volcanic tephra fallout
Loss of off-site power AND Loss of function of uninsulated exterior equipment Loss of ultimate heat sink	Extreme temperatures
Loss of off-site power	Flood due to meteorological causes Aircraft crash External fire (forest, hydrocarbon storage, nearby facilities) Lightning Hail Saltspray/Saltstorm Freezing precipitation and frost related phenomena Electromagnetic interference (solar storms)
Loss of primary ultimate heat sink	Aircraft crash Volcanic tephra fallout Ship/barge impact Collision of floating bodies Blockage or diversion of river / Frazil ice Biological phenomena Depletion of a reservoir
Loss of unshielded systems and components (several possibilities will likely need to be considered, including loss of off-site power)	Explosion
Loss of required operator actions	Release of hazardous substances (toxic, asphyxiant, corrosive or radioactive)
Loss of structures, systems and components within the area of influence	Slope instability Foundation ground instability
Loss of sensitive instrumentation and control components	Electromagnetic interference
Loss of systems and components affected by the collapse of roofs	Extreme snowpack

Note: Site or design specific conditions may require adaptation of this table.

3.2. A SUCCESS PATH APPROACH

The success path approach relies on defining 'success paths' for the accomplishment of the fundamental safety functions, given the induced initial conditions defined in the previous section. A 'success path' is a set of systems and associated components that can be used to bring the plant to a controlled or safety state and maintain it for a specified period of time. A complementary definition is that a 'success path' is comprised by SSCs whose successful performance will put the NPP in a safe state.

Figure 2 shows an example of a success path diagram for the safe shutdown of a Pressurized Water Reactor (PWR), after a loss of off-site power. The diagram serves the purpose of identifying the front-line systems required to accomplish the safety functions. In the example, the path considers the functions of reactivity control, reactor coolant pressure and inventory control and the decay heat removal. Similar diagrams can be built for spent fuel or containment-related safety functions.

The support systems and structures, required for the operation of the front-line systems, need to be identified as well. Commonly, there are support systems that are required to support more than one front-line system. In addition, there are support systems that are required for the long-term operation of other support systems, with an indirect support to the front-line system. Careful consideration needs to be given to these support dependencies. Typical support systems that are included in the success paths are:

- Electric power systems;
- Safeguard actuation systems;
- Service water systems;
- Component cooling water systems;
- Essential air;
- Heating, ventilation and air conditioning systems;
- Structures supporting or shielding required equipment (e.g. buildings).

Sometimes the 'safety division' concept can help the analyst identify the success path, since each safety division provides, by definition, all required fundamental safety functions and also ensures functional integrity in terms of frontline, control and support systems.

Success paths are normally defined including all redundancies of each required system; this helps ensuring that component random failure or unavailability is somehow taken into account. As a result, for each system, all redundant SSCs are normally included in the success path.

Within a success path, operator action can be credited for restoring the functions of certain SSCs that could be temporary affected by the external event. In order to credit operator actions, the following conditions have to be met:

- Procedures and training are in place;
- Procedures take into account the environment in which actions have to be taken (e.g. internal fire and flood, smothering);
- Operator actions utilize instrumentation and components (I&C) included in the success path;
- Egress routes are included in the success path for assessment (including opening of doors and emergency lighting). At least two alternate egress routes must be included in operator action procedures. Note that access routes for the operator to activate alarms may be required.

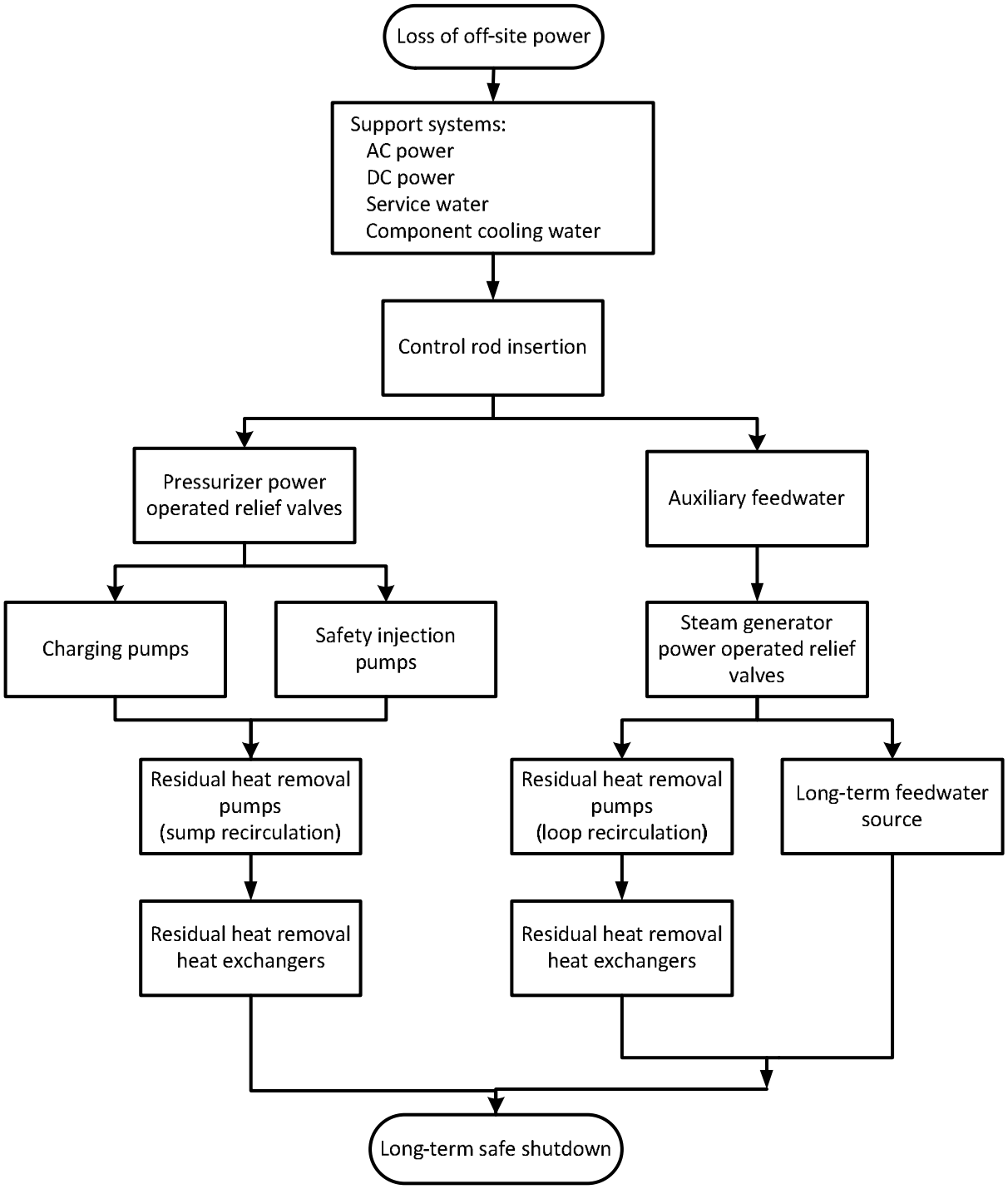


FIG. 2. Example of a success path logic diagram for a PWR. Each branch represents an alternative path (adapted from Ref. [19]).

Once the front-line and support systems are identified, the required equipment, distribution systems, and structures to develop the success path are itemized. These required SSCs will be listed on a Selected SSC List, which will be augmented by required structures. Note that the list will include both active and passive components. Active components are those which need to change state in order to perform their intended function (e.g. a pump). On the contrary, passive components perform their functions without changing state (e.g. a tank). Along with identification of the SSCs, their required performance within the success path needs to be identified. For example, active valves may be not required to be actuated in order to develop the success path.
For a given set of induced initial plant conditions, the Selected SSC List may be based on one or more

success paths. For less severe events, multiple success paths based on full redundancy of systems, and engineering capacity based on design criteria may be required; on the other hand for the more extreme events, a single safe shutdown path may be deemed to be adequate. In the context of the present methodology, the focus is on the more extreme events and, consequently, the single success path approach for each set of initial conditions is considered adequate.

Hence, several paths may exist and the most favourable path (largest capacity) is to be selected. However, since the plant level capacity against the hazard is to be computed only in the following activities, the selection of the success path may be revisited after the capacity assessment is started. This is fairly common in practice; an iterative process takes place in order to maximize the computed plant capacity.

As mentioned before, multiple SSC lists could be defined, as a function of the different hazards or the different events corresponding to each hazard. Note that different sets of SSCs will be required for different events, based on the location and extent of effects of the event.

The success path approach was developed for 'hand' implementation, as opposed to 'computerized' implementation, [43]. In summary, the updated plant documents describing the 'as-is' configuration of the plant (P&ID, electrical and I&C diagrams, plant layout schemes, etc.) are reviewed in order to:

- Identify minimum scope setting of SSCs which are comprised in the success path to achieve the safety functions (i.e., identify the 'design and operational limits' of required SSC in the system drawings);
- Identify any dependences associated with SSCs in the success path;
- Identify interactions with other SSCs not directly performing safety functions, but whose failure could compromise the SSC performance in the success path (e.g. any item collapsing and falling on a component which is part of the success path; or loss of ventilation in a room where heat generating success path equipment is located);
- Verify that, to the extent possible, adequate independence exists among SSCs performing different safety functions. Dependences have to be identified and documented;
- Verify that selected SSCs do not include low reliability equipment (e.g. operating experience with a large probability of failure on demand);
- Verify timing during which the SSCs in the success path have to perform their intended functions; this need to include an assessment of the stock of consumables, its availability and accessibility, given the impact of the extreme external event.

During the capacity assessment, most SSC failure modes corresponding to external hazards can be analysed after grouping together the different sub-components of the same equipment item into a single item. This is sometimes called the 'rule-of-the-box' [43]. Following this rule, for example, the body, the actuator and the limit switches of a motor operated valve will appear as a single equipment item in the Selected SSC List; or all the subcomponents of a diesel generator mounted on the same skid will appear as a single item in the Selected SSC List.

The rule-of-the-box cannot be applied for failure modes where the capacity assessment cannot be done for the combined items as a whole. A typical example is the chatter (change of state) of electromechanical relays during earthquake shaking. The good performance of the relay panel (structural stability, electrical continuity, etc.) cannot be used to demonstrate that no chatter will occur during the shaking. Hence, the relays require an assessment in addition to that of the panel they are mounted on.

In a typical plant, it is expected that the number of items on a Selected SSC List defined for a particular set of initial conditions will be in the order of several hundreds, after applying the rule-of-the-box.

3.3. EVENT TREE / FAULT TREE APPROACH

When a validated internal event Level 1 PSA within the plant design basis is available (IAEA Safety Standards SSG-3 [44]), the associated event tree/fault tree models can be used to identify the safety significant components corresponding to each set of plant initial conditions. In many cases, conditions given in Table 2 will already have been considered in the Level 1 PSA as initiating events and the corresponding event trees will be available. If conditions not taken into account in the Level 1 PSA need now to be considered, the Level 1 PSA model will need first to be adapted according to the guidance in Ref [44].

The SSCs modelled in the internal events Level 1 PSA, for the induced initial conditions corresponding to the applicable external hazards (Section 3.1), are used to compile the safety significant components. The systems, both front line and supporting that are required to perform the plant safety functions, are identified in the accident sequence analysis. Performance of these systems is analysed by means of fault trees. The top event of the fault tree is the system failure state(s) identified in the accident sequence analysis (event tree). The fault tree extends the analysis to the level of individual basic events, which typically includes failure of components.

The individual component of a system appearing in an accident sequence is identified as a basic event in a fault tree. The collection of such components in the fault trees is the initial Selected SSC List. For each item of the list, the functional requirements to achieve the system performance are taken from the fault tree.

Note that, when this approach is followed, the system analysis takes place in the ‘failure space’ (as opposed to the ‘success space’); that is, the selection of safety significant components is made based on the identification of components whose failure could prevent the accomplishment of the safety functions (‘failure paths’). This includes the front-line systems, their support systems and other systems that may interact with the former or are credited to prevent the loss of safety functions.

When using the systems models developed for a Level 1 PSA for developing the Selected SSC List, the following points have to be taken into account:

- Internal events PSA models usually include only active components, since the probability of random failure of passive components is negligible. For the capacity assessment against external events, both active and passive components have to be considered, since the external events typically could lead to failure of both types of components.
- Therefore, passive components needed to perform the required safety functions or that may interact or produce failure of the internal PSA components (e.g. building structures) have to be added to the Selected SSC List. This activity usually involves consultation of general lay-out drawings, piping and instrumentation diagrams and electrical one-line drawings.
- Internal events PSA models can be very detailed. They can have a separate representation of several items that are different components of the same item of equipment (e.g. the limit switches and the motor of a motor operated valve). For the vast majority of failure modes caused by external events, the different components of the same equipment item can be grouped together in a single item for capacity assessment purposes (rule-of-the-box).
- Internal events PSA models usually consider a mission time of 24 h, which would normally be too short for the kind of extreme external events considered in this publication.

Therefore, the analyst will normally need to either include additional equipment or to exclude certain equipment which is credited in the analysis, but cannot operate beyond 24 h in order to extend the mission time as much as possible.

Annex 4 gives an example to illustrate this process. Note that within this event tree/fault tree approach, event trees and fault trees are used just as a tool to identify components required to perform the fundamental safety functions for each postulated set of plant initial conditions. This is the first step of the present methodology. Only the functional and system dependencies are taken into account. At this step, no consideration is given to the effects of the external events on the components or on the overall site conditions.

3.4. RESULTS

The output of the activity of selection of the safety significant components, following one of the approaches described in the previous sections, is a list of SSC items for each of the applicable hazards. For each item, the required functionality consistent with the intended functions within the success path or the fault tree needs to be given. Typically, the list includes the following for each item:

- Identification (e.g. plant tag);
- Description of item (e.g. horizontal pump, Heating, Ventilation and Air Conditioning (HVAC) duct, auxiliary building);
- Location in plant (e.g. room, building, area);
- Required functionality or intended function.

In some instances, different lists could be produced for the same hazard. This is the case when different initiating events are considered for the same hazard. A typical example is the aircraft crash, which could result in different initiating events depending on the buildings or areas of the plant which are impacted.

4. GENERAL METHODOLOGY FOR PLANT CAPACITY ASSESSMENT

4.1. GENERAL

In the context of the present guidelines, the plant-level capacity for a particular hazard is defined by the strength of the hazard that could start compromising the safety of the plant. Here, the compromising of safety means that the plant is rendered incapable of achieving safety objectives under the impact of an event having such a level of strength or higher. In other words, when the hazard remains below the plant-level capacity, it is very unlikely that the fundamental safety functions are jeopardized.

Two approaches are given here for plant capacity assessment: deterministic and semi-probabilistic. They are explained in the following sections. In Section 5 the general methodology presented in this section will be particularized for specific hazards.

It is important to note that the capacity assessment is made on the 'as-is' condition of the plant. The intent is not to perform just a paper review, but to base the assessment on the actual configuration and condition of the plant, as described in 'as-built' documents and as found during plant walk downs. Hence, in both approaches, the 'in-plant' evaluation plays a key role, which is explained also in this section.

4.2. DETERMINISTIC PROCEDURE

In a general case, the steps for assessing the plant capacity for a particular hazard using the deterministic approach are those in Figure 3. These steps are described in the following sections.

4.2.1. Define reference strength for the hazard

Following a deterministic approach, the assessment of plant capacity is carried out using an event defined at a selected level of hazard strength (severity level). For example, for earthquake hazard, the event may be defined by a ground motion response spectrum in the free field. For aircraft impact hazard, the event may be defined by a category of aircraft and an impact velocity.

This event is a working tool and may be either selected by the analyst or prescribed by the Regulator of the Member State. In the context of seismic assessments, this event is sometimes called the 'Review Level Earthquake' (RLE) [11].

The plant-level capacity and the weaker SSCs against the hazard (vulnerabilities) do not depend on the selected reference event. The reference event is introduced to make the assessment more efficient. Instead of computing the capacity of each selected SSCs, it is usually easier to decide if the capacity of a component is smaller or larger than the strength corresponding to the reference event. For example, bounding conservative computations can be used to show that the high confidence capacity of a component is larger than the reference event and, afterwards, eliminate the component from further consideration. As a result, only the components for which the high confidence capacity cannot be easily shown to be larger than the reference event are kept for detailed capacity analyses.

Some amount of judgement is needed to define the reference event and, sometimes, it might imply an iterative approach. Ideally, the reference hazard severity could be set at a slightly higher level than the expected plant level capacity. If it is set too low, the weaker SSCs will not be identified (all SSCs will be screened out before preforming detailed capacity calculations). On the contrary, if it is set too high, the assessment will require a large number of detailed capacity calculations. Note that, in the context of the present methodology, the reference event is just a screening level to make the analysis more efficient. Instead of computing capacities for all SSCs, it is usually easier to decide if capacity is larger or smaller than the reference event.

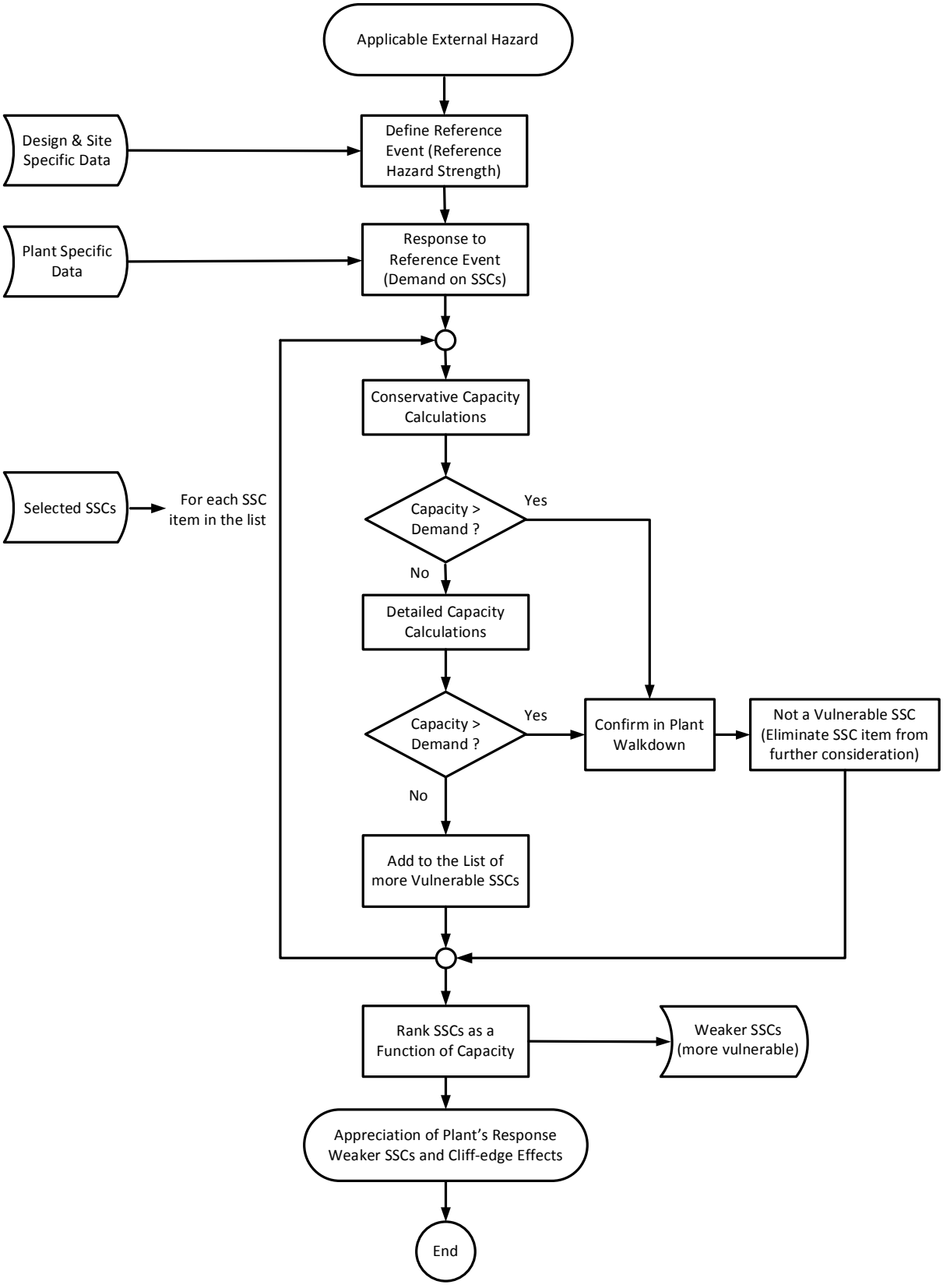


FIG. 3. General workflow of the deterministic procedure for plant capacity assessment.

The deterministic method assumes that the responses (force, stress, flood level, acceleration, heat flux, etc.) are scalable with respect to the hazard strength in the vicinity of the selected level of hazard. Consequently, if the final capacity is significantly different from the strength of the hazard corresponding to the reference event, and the responses to the hazard are significantly non-linear or non-scalable, then the analysis has to be repeated for an event closer to the expected plant capacity.

4.2.2. Plant response to the reference event

In this step, the response of the NPP to the reference event is obtained, that is, the effects of the reference event on the plant are computed. The computed response will provide the reference demand on the Selected SSCs (Section 3).

Examples of demand are the maximum level of flood in a particular building, the level of seismic shaking at a particular elevation (in-structure response spectra), the wind pressure at an external wall, the side-on overpressure caused by the reference explosion, the concentration of a toxic substance at an air intake, etc..

The methods used to compute the plant response can be very different from one hazard to the other. Section 5 provides examples for specific hazards. The general condition is that the demand is to be computed using best estimate parameters and procedures, that is, with no conservative bias (Table 3). Methods can include anything between simple hand calculations to very sophisticated finite element simulation or experimental methods. Normally, the more sophisticated the method, the less conservative the computed response. However, engineering judgment may be exercised in order to select an accurate enough approach without defeating the purpose of performing a cost effective assessment.

4.2.3. Capacity of the selected components

In this step, the capacity of the Selected SSCs is computed, to be compared with the reference demand obtained in the previous step.

Capacity depends on the functionality required for the SSCs and it is obtained according to conservative rules, but not as conservative as those used in the design. The goal is obtaining a capacity with a relatively large probability of being exceeded (e.g. between 95 and 99%). The specific rules to compute capacity vary from one hazard to the other and depend on the functionality requirements. As an example, the general approach given in Table 3 for mechanical or structural assessments Conservative Deterministic Failure Margin (CDFM method) is considered to be appropriate in the present context. Examples for specific hazards are given in Section 5.

TABLE 3. SUMMARY OF CONSERVATIVE DETERMINISTIC FAILURE MARGIN (CDFM) APPROACH FOR STRUCTURAL/MECHANICAL CAPACITY CALCULATIONS (ADAPTED FROM OECD-NEA, REF [45])

Load Combination	Normal + Extreme external event	
Load from extreme external event	84% Non-exceedance probability, given that the event occurs	
Structural model	Best estimate (median)	
Material strength	Code specified minimum strength	OR
	95% exceedance if test data are available	
Strength equations	Code ultimate strength or functional limits	OR
	84% exceedance if test data are available	
Inelastic energy absorption	Only for non-brittle failure modes	
	Go to 95% exceedance ductility levels	

The plant response computed in the previous step relates the parameter defining the strength of the reference event to the effects ('demand') at the location of the SSCs. Consequently, the capacity of each SSCs can be obtained in the same terms used to specify the reference event (e.g. in terms of peak ground acceleration, or gust wind speed at 10 m height in the free field, or mass of explosive material at the specified distance). This is possible, as far as the reference response is scalable with respect to the hazard strength.

To make the assessment more efficient, the capacities are computed in two stages. In a first stage, engineering judgement based on previous experience (e.g. previous studies, seismic experience, available test results, etc.) and simple conservative calculations are given credit to exclude from detailed capacity calculations ('screen out') those SSCs whose high confidence capacity clearly exceeds the demand in the reference event. When the capacity of a selected SSC can be conservatively shown to be above the reference demand, then the item is considered not to be vulnerable and screened out from any further study. This elimination could be confirmed by a plant walk down, which has to confirm the conditions under which the capacity has been obtained (Section 4.4.3).

In a second stage, detailed capacity calculations are carried out for the SSCs not screened out in the previous stage. Computed capacities can be above or below the reference demand. As a result, the SSCs not screened out in the first stage can be ranked from lower to higher capacity. The low capacity SSCs are the more vulnerable items (weak links) against the hazard.

When assessing capacity of the selected SSCs, it is to be noted that capacity of SSCs with functionality requirements cannot be obtained just by analysis, unless functionality depends only on keeping structural integrity. Functionality during or after the extreme event, normally requires to be demonstrated via testing.

4.2.4. Plant-level capacity

The deterministic procedure for plant capacity assessment is normally used in combination with the success path approach for selection of components (Section 3.2). In this case, the plant-level capacity is given by the item with the smallest capacity. In general terms, if C is the capacity computed for this item and D is the demand caused by the reference event, the plant-level capacity is given by C/D times the selected level of hazard strength in the reference event. Hence, within a deterministic approach, the plant level capacity is assumed to be given by the high confidence capacity of the weakest component needed to accomplish the fundamental safety functions.

On the other hand, when the event tree/fault tree approach has been used for selection of components, once the high confidence capacities of the selected SSCs have been computed, those capacities can be propagated using the Boolean equations to obtain the plant level high confidence capacity. This is described in Section 4.3.5, within the semi-probabilistic procedure.

4.2.5. Discussion

There are several fundamental results coming out of this capacity assessment:

- Appreciation of the plant's response to the external hazard;
- Identification of the plant's weak links and any potential cliff-edge[4] effect related to the hazard;
- Identification of the threshold of hazard strength beyond which the fundamental safety functions could be jeopardized.

A well-designed and maintained plant will normally have a plant-level capacity well above the design basis hazard strength.

[4] A 'cliff-edge' effect refers to a situation in which a small increase in the hazard severity produces a simultaneous and widespread failure of plant structures, systems and components, corresponding to a sharp increase in risk..

The deterministic approach has the advantage that, once the rules for computing demand and capacity are established, engineers without training in probabilistic methods can perform the evaluations. On the other hand, more conservative assumptions are normally made and less insight about available margins are obtained.

4.3. SEMI-PROBABILISTIC PROCEDURE

In a general case, the steps for assessing the plant capacity for a particular hazard using the semi-probabilistic approach are those in Figure 4. These steps are described in the following sections.

4.3.1. Define reference strength for the hazard

As for the deterministic approach, the first step is defining a reference event (hazard strength), which will be used for computing the plant response.

Since the purpose of this methodology is to find a high-confidence plant-level capacity, the reference event could be defined as close as possible to the expected high confidence plant-level capacity.

Similarly to the deterministic approach, calculations will assume that the responses (force, stress, flood level, acceleration, heat flux, etc.) are scalable with respect to the hazard strength in the vicinity of the reference event. Consequently, if the final plant-level capacity is significantly different from the strength of the hazard corresponding to the reference event, and the responses to the hazard are significantly non-linear or non-scalable, then the analysis has to be repeated for an event closer to the expected plant-level capacity.

4.3.2. Plant response to the reference event

As in the deterministic approach, the component capacity assessment requires the analysis of the plant response to the reference event. The effects of the postulated reference event at the position of the SSCs within the plant are required in order to obtain the capacities with reference to the parameters defining the event.

4.3.3. Screening of robust structures, systems and components

In a probabilistic framework, a probabilistic definition of capacity is used. Capacity is defined as the conditional probability of failure of a SSC for a given value of the hazard parameter (e.g. maximum ground acceleration, blast peak pressure, etc.). The concept has been extensively used within seismic assessments, where this conditional probability of failure is called ‘fragility curve’ [46]. This concept of ‘fragility’ has been generalized from seismic hazard to other hazards as well.

In many cases, a log-normal model is used to approximate fragility curves [46]. The capacity is then expressed in terms of median value and logarithmic standard deviations β_R and β_U reflecting the randomness in capacity and uncertainty in the median capacity, respectively. For simplicity, the logarithmic standard deviation β_c, defined as the composite variability, is often used. Using the lognormal model for the fragility, the two parameters – median capacity and β_c - are sufficient to develop a best estimate or mean fragility as a function of the hazard parameter. A ‘high confidence’ capacity is conventionally defined by the hazard strength that corresponds to 1% failure probability in the mean fragility curve of the component[5].

[5] This ‘high confidence’ value is known as the ‘High Confidence of Low Probability of Failure’ (HCLPF) capacity in the Literature dealing with seismic safety assessment.

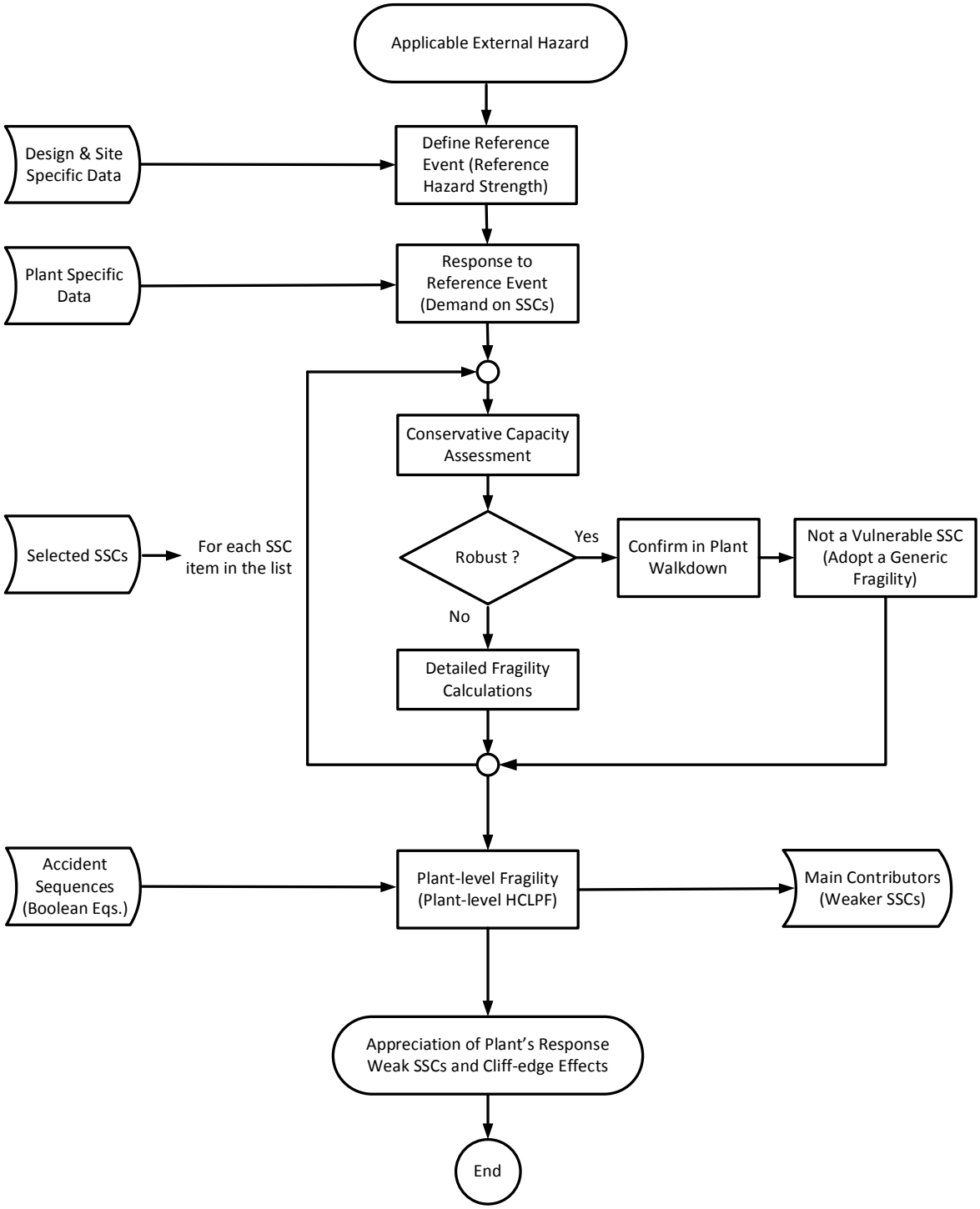


FIG. 4. General workflow of the semi-probabilistic procedure for plant capacity assessment.

Once the plant response to the reference event has been obtained, engineering judgement based on previous experience (e.g. previous studies, seismic experience, available test results, etc.) and simple conservative calculations are given credit to exclude from detailed fragility calculations ('screen out') those SSCs so robust that are clearly not the weak links against the hazard.

When the high confidence capacity of a selected SSC can be conservatively shown to be above the reference demand, then the item is considered not to be a weak link and it is given a simplified treatment. The simplified treatment normally involves grouping similar SSCs and defining for them generic fragility curves based on simple calculations, previous studies or documented experience.

As in the deterministic approach, the screening could be confirmed by a plant walk down (Section 4.4.3), which has to confirm the conditions under which the capacity estimate has been obtained.

4.3.4. Fragility calculations

For the SSCs not screened out as rugged SSCs, more detailed capacity calculations will need to be performed in order to develop fragility curves or, at least, high confidence capacity values. As already mentioned, capacity depends on the functionality required for the SSCs. Hence, the fragility curves are linked to the failure modes that lead to the loss of the intended functionality.

There are several possibilities for computing fragilities and, as shown in Section 5, each hazard has its own specificities. In the context of this publication, the philosophy of the so-called 'Hybrid Method' used in seismic assessments is considered adequate [45]. Following this approach, a 'high confidence' capacity is computed using the same procedures and rules described in Section 4.2.3 for the deterministic approach. Then, the computed capacity is assumed to correspond to 1% failure probability in the mean fragility curve of the component. Then, variability is conservatively estimated. When using a log-normal model, this can be achieved by an estimate of the composite variability coefficient, β_c. With these two parameters, $C_{1\%}$ and β_c , a log-normal mean fragility curve can be defined. Since the fragility curve is anchored to the 'high confidence' capacity $C_{1\%}$, note that the lower β_c is estimated, the more penalizing the composite fragility curve for the component will be.

4.3.5. Plant-level capacity

The event tree/fault tree analysis carried out for selection of safety significant SSCs (Section 3.3) is based on a number of accident sequences. The progression of each accident sequence is traced through the success or failure of system functions. The top event of each such system failure is modelled by a fault tree; the basic events on this fault tree are component failures, random equipment failures and operator failures. By solving the fault trees, the Boolean equation (Boolean sum of 'minimal cut sets'), for each accident sequence (plant damage state) can be obtained[6]. Each minimal cut-set in the Boolean equation represents a combination of failures leading to core damage.

Using the semi-probabilistic approach, the conditional probability of ending in a particular plant damage condition, for given hazard strength levels, is quantified by combining the component fragilities using the Boolean expression for the accident sequence [20]. This provides the plant-level fragility curves for the plant damage state (Figure 5).

Plant-level fragility curves for different damage states can be added to have an overall plant-level fragility. Plant-level capacity against the hazard is conventionally defined by the hazard strength that corresponds to 1% failure probability in the mean plant-level fragility curve. The more vulnerable SSCs are identified as the major contributors to this 1% conditional probability of failure.

[6] A 'minimal cut-set' is a combination of events that causes the accident sequence to occur. All events in the cut-set need to occur for the accident to take place.

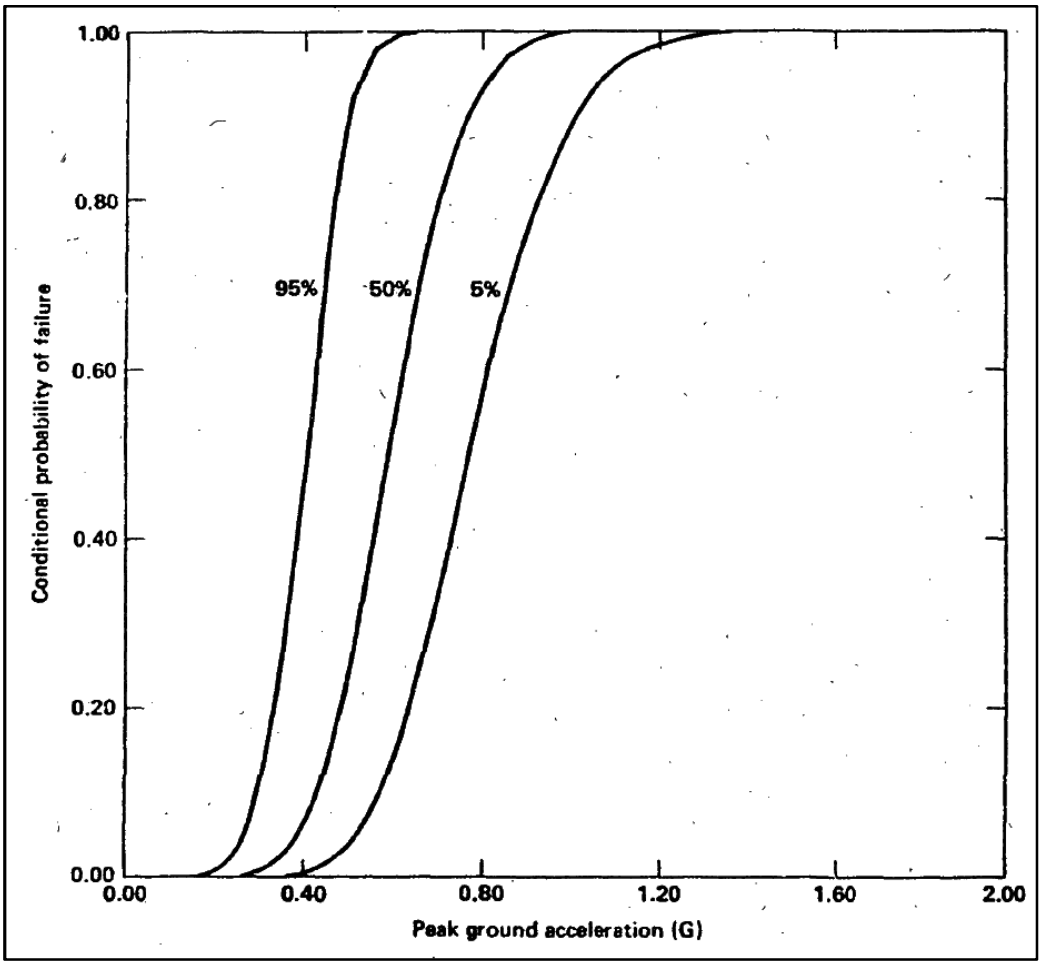


FIG. 5. Sample of plant level fragility curves for a seismically induced plant damage state [20].

Note that this method allows consideration of failures not only associated with the hazards, such as random failures, when computing the plant-level fragility (see Ref [20]).

When the analyst is interested only in hazard-related failures, then the Boolean equations can be used just to propagate the high confidence capacity values, up to obtaining the plant-level high confidence capacity.

Using a semi-probabilistic approach, the more vulnerable items against a particular hazard would be given by the minimal cut-set(s) with the lowest capacity against the external hazard. The capacity of a minimal cut-set can be approximated by the maximum capacity among the components taking part in the minimal cut-set; and the overall capacity will then be given by the minimal cut-set in the Boolean equation with the minimum capacity (i.e., the so-called Min-Max method in Ref [42]).

4.3.6. Discussion

The semi-probabilistic approach includes three basic ingredients of a full scope PSA: (1) plant specific system and accident sequence analysis, even if simplified by reducing the total number of initiating events; (2) fragility evaluation; and (3) plant-level capacity determination.

The fundamental results provided by the semi-probabilistic approach are the same as those given by the deterministic approach. Basically, the plant's weak links, any potential cliff-edge effect related to the hazard, and the threshold of hazard strength beyond which the fundamental safety functions could be jeopardized, which is given by the plant-level capacity.

However, the semi-probabilistic approach is richer in the sense that it considers all available plant systems when computing the plant-level capacity (not just a success path), and it gives some insights not readily provided by the deterministic approach, such as the influence of operator actions and potential failures not associated with the hazard.

In contrast with the deterministic approach, which can be developed almost 'by hand', the semi-probabilistic approach requires specialized software and engineers trained in probabilistic methods.

The identified weaker or more vulnerable SSCs point to the way in which the fundamental safety functions will start failing under the external hazard. This result will be used in the next stage of the vulnerability assessment, where progression after the plant-level capacity is exceeded will be investigated (Section 6).

4.4. IN-PLANT EVALUATION

4.4.1. General

Assessment of safety margin against external events is performed for the 'as-is' condition of the plant. The 'as-is' condition of an installation refers to the present state and actual conditions of the NPP, considering the 'as-built', 'as-operated' and 'as-maintained' state of structures, systems and components [13] .

Hence, irrespective of the hazards applicable to a specific site, the assessment cannot be performed just 'on paper'. It always requires a plant walk down and inspection. These activities are generically termed here as 'in-plant evaluation' and are a key part of the assessment.

The objectives of the in-plant evaluation are plant familiarization, preliminary assessment, confirmation of the assessment and identification of the easy fixes, if any. The major components are:

- For each hazard, evaluate the feasibility of hazard affecting the structures or yard facilities;
- Check preliminary lists of SSCs (Section 3);
- Review of design;
- Review of 'as-is' information of the NPP;
- Develop preliminary screening rules for each applicable hazard. Screening rules allow elimination of SSCs not likely to be weak links for an specific hazard;
- Plant walk down.

The plant walk down will cover all items in the list of safety significant SSCs developed for the applicable hazard and it will focus on several modes of failure, for example:

- Direct exposure to hazard effects (mechanical; heat; water level, etc.);
- Fire;
- Indirect exposure to hazard, e.g. scabbing and spalling of concrete structures, penetration of all structures; fire-related issues, such as firefighting (water, foam), smoke, etc.; falling of missiles and debris; other systems interaction issues;
- Vibration.

The important results of in-plant evaluation are:

- Screening out of SSC items as not being the weak links for a particular hazard (verification of in-office assessment + additional screening in-plant);

- Identify the easy fixes, if any, e.g. strengthening of anchorage, installation of fire doors, reinforcing accesses (air intakes, windows, penetrations), sealing penetrations in underground conduits, etc.;
- Identification of items in the SSC list needing further investigation and their grouping; and
- Finalisation of accident sequences or success paths.

In-plant evaluation is based on the review of the plant status and on plant walk downs. These two activities are described in the following sections.

4.4.2. Review of plant status

4.4.2.1. Review of design

This activity covers the following points:

- Review identified accident sequences and/or success paths and the SSCs on these. Gather all available design information regarding these SSCs;
- Arrangement of safety functions (frontline + support + control) into independent trains/divisions and their potential coordination during extreme events;
- Confirm the required functions of the SSCs during and after the event;
- Confirm the demand environments to which the SSCs are subjected for each event scenario;
- Identify or confirm failure modes of concern as a function of the event; and
- Identify robust SSCs (robustness includes direct and indirect effects) that may be excluded from further consideration.

4.4.2.2. Review of 'as-is' information

Correspondence of design information reviewed in the previous activity with current conditions of the plant has to be verified, including plant systems.

Consideration of plant procedures is also included in the review; particularly, the consistency with the assumptions made for the selection of components (Section 3).

4.4.3. Plant walk down

A key ingredient of in-plant evaluation for any external hazard is the plant walkdown. In fact, the plant capacity assessment cannot be completed without the plant walkdown, since many failure modes can only be assessed on the spot. In addition, during the plant walkdown, is where high capacity SSCs are screened out from further evaluation, which is essential for the cost-effectiveness of the methodology.

The plant walkdown activities are completed in three principal steps: (1) walkdown preparation, (2) the preliminary screening walkdown or walk-by, and (3) the more detailed walkdown. These steps are described in the following. Certain special topics, such as co-located facilities at the site and the potential of spatial interactions, are examined in Section 4.4.4.

Nevertheless, it may be said that plant walkdowns are only able to perform 'static' checks (layout, arrangement, equipment configuration, distances). Functionality checks can hardly be done during walkdowns and need to rely on the design reviews described above.

4.4.3.1. Walkdown preparation

Plant walkdown preparation includes the following activities:

(1) Plant familiarization:
- General plant documentation have to be assembled, including safety analysis reports, system descriptions, piping and instrumentation diagrams (P&IDs), electrical one-line drawings, operating procedures, plant general arrangement drawings, plant mechanical and electrical equipment location drawings, PSAs for internal and external events, and any other beyond design basis assessments;
- Plant access requirements have to be met, including radiation protection, safety practices and security practices. Adherence to the 'as low as reasonably achievable' (ALARA) and dose optimization principles is required.

(2) Plant documents on the selected safety significant SSCs have to be consulted or created and the demand on each item needs to be defined.

(3) A database of the SSCs have to be prepared summarizing the evaluation of each item in the SSC for the demand. It is expected that the Selected SSC List of a nuclear power plant will comprise a few hundred items.

(4) Individual SSC data sheets have to be prepared containing some of the above mentioned information. If necessary, the data have to be supplemented with field and office generated SSC specific evaluations, including field notes; safety and engineering analyses performed; and field modifications.

(5) An in-plant walkdown plan has to be developed indicating the number of teams and the composition of each team. It is expected that more than one team will be used, with the total number depending on the issues to be considered and the experts required. The columns of this table could be as follows:
- SSC No: A unique numerical identifier for the SSCs that may contain location, system or other information.
- SSC name: Descriptive information on the SSCs (e.g. auxiliary building, diesel generator 1A, etc.).
- SSC ID No: Plant tag or plant specific identifier.
- Description: Brief description of the SSCs (e.g. horizontal pump; motor operated valve).
- Hazard scenario No: Identifier linked to a master list of scenarios to be evaluated.
- Location: Location identifier to aid in planning the in-plant walkdown and evaluating the consequences of the hazard event.
- Physical loading conditions: Identifiers of the type of loading conditions to be considered that provide guidance on the experts required and in-plant walkdown access, and on combined loading conditions to be evaluated (e.g. shaking, impact plus fire, etc.).
- Impact: Direct and indirect impact effects to be considered in the evaluation. Direct impact effects are conditions such as direct missile impact; indirect impact effects are conditions such as scabbing of concrete and vibration induced loadings.
- Explosion/blast: Blast effects to be considered can be direct or indirect. Direct effects are blast pressures; indirect blast effects are conditions such as vibration induced loadings.
- Heat/fire: It refers to heat from a fire or direct flame effects on the SSCs.
- Smothering and related conditions: They may arise as a result of smoke, toxic chemicals or firefighting techniques. This failure mode may affect personnel or

systems; for example, smothering of the diesel generator system could occur if the air intake system is inundated. Control room habitability and on-site personnel safety have to be evaluated.

- Flooding: Flooding from internal or external sources may need to be evaluated.

Table 9 in Ref [19] provides a sample format for individual data sheets in the evaluation of SSCs with regard to physical loading conditions. In the pre-walkdown stage, the basic information identifying the SSCs under consideration is entered into the forms. The remainder of the table is filled out upon completion of the walkdown and evaluations. This table is based on the data sheets used for SSC evaluations for seismic events. For the seismic evaluation case, unique data sheets exist for each of 22 equipment categories (see for example Ref [19]). Each category has unique equipment characteristics and conditions that need to be evaluated to verify the seismic performance. These data sheets, called 'screening evaluation work sheets' or SEWS, can be used as a basis for developing similar worksheets for the evaluation of other external events. The data to be collected and evaluated may need to be modified to take into account non-vibrational modes of failure that is, loading conditions such as heat, humidity and direct impact.

4.4.3.2. Preliminary screening walk-by

The preliminary screening walk-by has to achieve the following objectives:

- Determine the location and accessibility of each SSC item in the plant;
- Identify any other SSCs needed for safe shutdown or hazard prevention or consequence mitigation, which could then be added to the list of safety significant SSCs;
- Review and validate screening of SSCs with respect to capacity considerations (direct and indirect effects);
- Identify potential easy-fixes;
- Group all the components located within or on larger items of equipment;
- Group components within the same location, particularly in the same vital area, for evaluation of spatially common environments;
- Evaluate whether SSC capacity is adequate (large enough) for the specified event(s);
- Document conclusions.

The preliminary screening walk-by visually examines those SSCs that are accessible. There are three alternative disposition categories for each item on the SSC:

- Disposition 1: For SCCs in this category, capacity is well below the demand imposed by the reference event.
- Disposition 2: For items in this category, capacity cannot be judged to be above or below the demand imposed by the reference event without further evaluations being carried out.
- Disposition 3: For items in this category, the capacity well exceeds the demand imposed by reference event.

The preliminary screening walkdown have to be fully documented. The main result of the preliminary walkdown is the identification of the selected safety significant items (Section 3) that are obviously robust. These items are categorized as Disposition Category 3 and are therefore excluded from further evaluation. Items in Disposition Categories 1 and 2 require a more detailed in-office and in-plant evaluation.

4.4.3.3. Detailed screening walkdown

The detailed screening walkdown is to be performed for all SSCs whose capacity for the defined reference event has not been verified. This includes in-plant evaluations and, in many cases, further

analytical calculations and evaluations. Two categories of SSCs result:

(1) SSCs in the first category are those that were not excluded from further consideration during the preliminary walk-by. At this stage, walkdown engineers evaluate these systems and components in more detail and make a judgement as to whether or not the component requires further analysis or modification.

(2) For SSCs in the second category, plant modifications are clearly warranted. In these cases, the walkdown engineers suggest that the modifications be implemented.

The detailed screening walkdown have to be thoroughly documented. It is advisable to supplement the documentation with photographic and/or video records. Table 8 in Ref [17] can be used as a reference for summary documentation. In the same way, Table 9 of Ref [17] can be used as a reference for documenting the SSC evaluations, with supporting material attached.

4.4.4. Special topics of in-plant evaluation

4.4.4.1. Type and number of co-located facilities

A nuclear power plant site may have several reactor units, possibly with interdependent safety or support systems. Multi-unit sites often assume the availability of companion unit systems when addressing non-common-cause events. In addition, other critical facilities may be present within the plant boundary, such as spent fuel storage in fuel pools or dry cask storage. All co-located facilities may require simultaneous mitigation measures when subjected to extreme external events. The evaluation has to take all onsite facilities into consideration, including any interdependence of their safety systems.

4.4.4.2. Spatial interactions

The plant walkdown is a key tool for identifying spatial interactions which could potentially affect the performance of the selected SSCs subjected to a specific event and that could render them inoperable. A major concern in these areas is 'housekeeping'. The identification and assessment of potential interactions requires good judgment from the walkdown team.

Falling & Impact

Falling is the structural integrity failure of an item that could fall, impact and damage a selected SSC item. For the interaction to be a threat to a particular item the impact must contain considerable energy and the target must be vulnerable. For example, a light fixture falling on a 10 cm diameter pipe may not be a credible damage threat to the pipe. However, the same light fixture falling on an open relay panel is an interaction that could cause damage and have to be addressed.

Scabbing of concrete due to missile impact on a building element (wall, diaphragm or roof) may be a viable failure mode for delicate equipment in the range of the falling concrete. Unreinforced masonry walls are a common source of falling interaction during seismic or impact events.

Proximity

Proximity interactions are defined as conditions where two or more items are close enough that the behaviour of one may have consequences for the other(s).

Spray and flood

Spray and flood can result from failure of piping, systems or vessels that are not properly supported or anchored. Inadvertent spray hazards to SSC items are most often associated with wet fire protection piping systems. The most common source of spray is leakage caused by impact induced failures of sprinkler heads. Since fire and heat are potential hazards throughout the plant site, particularly in

buildings and compartments, the walkdown have to evaluate the vulnerability to spray of all selected components.

Generally, design evaluations of fire and fire suppression systems will have taken spray vulnerabilities into account. If spray sources can reach equipment sensitive to water spray, then the source needs to be back-fitted, usually by adding a support. An alternative is to protect the target by installing a spray shield. Large tanks may be potential flood sources. The walkdown team, with the assistance of plant personnel, needs to assess the potential consequences of a flood source failure and the ability of the floor drainage system to mitigate the consequences of such a failure.

4.4.4.3. Tornado/hurricane missile survey

Potential wind-borne missiles are identified by means of specific missile survey walkdowns. This is described in Section 5.2.3.3. A missile survey walkdown covers the entire plant area, generally up to 750 m from the safety significant SSCs. The walkdown identifies the potential Missile Origin Zones, with the following information for each zone:

- What is in each zone, buildings, parking lots, what targets, etc.;
- What are the kind of missiles that could be generated;
- What are the minimum and maximum injection heights of missiles generated in the zone.

The information gathered during the walkdown is then used for definition of a spectrum of missile types and maximum velocities to be considered in the assessment (Section 5.2.3).

4.5. RESULTS

The output of the activity of plant capacity assessment is the strength of each of the applicable hazards below which there is high confidence that fundamental safety functions will not be jeopardized.

Additionally, a list of ‘weak links’ is produced for each hazard. For each of the items included in this list, the computed capacity is given; that is, the hazard severity level beyond which failure may be expected.

The weak links point at the most likely way in which the fundamental safety functions will start failing under a particular external hazard. This information will be used in the next stage of the vulnerability assessment, where progression after the plant-level capacity is exceeded will be analysed (Section 6).

5. PLANT CAPACITY ASSESSMENT FOR SELECTED HAZARDS

The following sections provide sample approaches that may be used to assess the plant capacity against selected hazards. It is recognised that there may be alternative approaches available to the operating organizations, which could be used for the same purpose if adequately justified.

5.1. EARTHQUAKE

Methodologies for earthquake safety assessment are well developed and have been applied extensively worldwide in the past 25 years. Seismic safety assessment methods for existing installations are described in Ref [11]. Detailed guidance is available in Refs.[16, 19, 47, 48]. Therefore, only a general overview is given in the present report, focusing on the application to seismic vulnerability assessment.

It has to be recognized that procedures for plant capacity assessment against other external hazards have been traditionally inspired by the procedures used for earthquake hazard.

5.1.1. Selection of methodology

Three methodologies are available for seismic safety assessment:

- Deterministic seismic margin assessment (SMA)
- Semi-probabilistic seismic margin assessment (PSA-based SMA)
- Seismic probabilistic safety assessment (S-PSA)

All three methods are mature and, for the purposes of a vulnerability assessment, all methods are valid choices.

S-PSA is an integrated process whose end goal is to provide an estimate of the overall frequency of a pre-determined plant level damage state, such as reactor core damage, or of the frequency of large radioactivity releases. It is a method developed for seismic risk assessment. The S-PSA includes consideration of the uncertainty and randomness of the seismic hazard, uncertainty and randomness of component failure rates conditional upon earthquake ground motion, and a logic tree required to calculate plant level damage states from component and system failure rates, including also random failures and operator errors.

In the context of the present vulnerability assessment, the key results from the S-PSA method are the following:

- Dominant accident sequences initiated by a seismic event, from which the most likely scenarios can be derived;
- Plant-level fragility curves, from which the seismic safety margin can be computed;
- Seismic vulnerabilities or weak links, based on dominant contributors to plant-level fragility.

The Seismic Margin Assessment (SMA) methods were developed as a simplification of the Seismic Probabilistic Safety Assessment (S-PSA) method. Two seismic margin assessment methods were developed in the 1980s and 1990s: one by the US-NRC [20] and the other by the Electronic Power Research Institute (EPRI) [19]. These seismic margin assessment methods were developed as simplified alternatives to the S-PSA. The SMA methods differ from the S-PSA in that they were specifically developed to assess the seismic safety margin of nuclear power plants above the design basis earthquake. This margin is often expressed as a ground motion parameter that represents a ‘High Confidence of Low Probability of Failure’ (HCLPF) for the overall plant and individual structures, systems, and components (SSCs). A HCLPF capacity is a conservative, but realistic capacity, and in

simple terms it corresponds to the earthquake level at which, with high confidence, it is extremely unlikely that failure will occur.

The SMA methods were designed to avoid arguments associated with the seismic hazard, which have often proved highly contentious and difficult to reconcile. In contrast to the S-PSA, they do not provide estimates of seismic risks such as annual frequencies of core damage or adverse public health effects.

In the context of the present vulnerability assessment, the key results from the SMA are the following:

- Seismic safety margin at component level and at plant level (HCLPF capacities);
- Seismic vulnerabilities or weak links based on SSCs with lower HCLPF capacities.

5.1.2. Deterministic seismic margin assessment

The deterministic SMA methodology was originally developed by the EPRI [19] and it is based on the 'success path' approach (Section 3.2). One (or more) success paths must be identified. Each success path consists of a selected group of safety functions capable of maintaining the nuclear installation in a safe state or bringing the nuclear installation to a safe state and of maintaining it there for an agreed upon time. The individual SSCs needed to accomplish each of the success paths are then identified and become the basis for the rest of the SMA analysis. This list of items is denoted by different names depending on the particular practice. It is usually known as the Safe Shutdown Equipment List (SSEL). However, sometimes it is termed as the Seismic Equipment List (SEL) or as the Selected Structures, Systems, and Components (SSSC).

As stated in NS- G 2.13 [11], the SMA defines and evaluates the seismic capacity of each of the SSCs on the success path(s). For the SMA, capacities of SSCs are defined as High Confidence of Low Probability of Failure (HCLPF) values. In a probabilistic sense, the HCLPF capacity is the earthquake severity with about a 95% confidence of less than 5% probability of failure or an equivalent mean confidence of a 1% failure probability [11]. Although defined conceptually in a probabilistic sense, HCLPF values are almost always calculated by deterministic methods. Deterministic guidelines have been developed and demonstrated to yield the approximate probabilistic definition.

Quantification of the plant HCLPF capacity for the SMA can be achieved relatively simply by evaluating the success paths, given the HCLPF capacity values of SSCs comprising them [11]. The smaller HCLPF capacity of the SSCs comprising the success paths is taken as the plant-level capacity. The components with the smaller HCLPF capacities correspond to the seismic weak links.

In summary, the SMA method is comprised of the following steps (see Figure 6) [11]:

(1) Selection of the Review Level Earthquake (RLE), which is the reference seismic event (see Ref [47]);

(2) Selection of the assessment team;

(3) Plant familiarization and data collection;

(4) Selection of success path(s);

(5) Determination of seismic response of structures for input to capacity calculation;

(6) Systems walkdown to review preliminary success path(s), select success path(s), and SSCs;

(7) Seismic capability walkdown;

(8) HCLPF capacity calculations (SSCs and plant-level).

HCLPF capacity calculations are many times performed following the Conservative Deterministic Failure Margin (CDFM) approach [19]. This approach provides the HCLPF capacity using design-like computations. The main ingredients of this approach are given in Table 3.

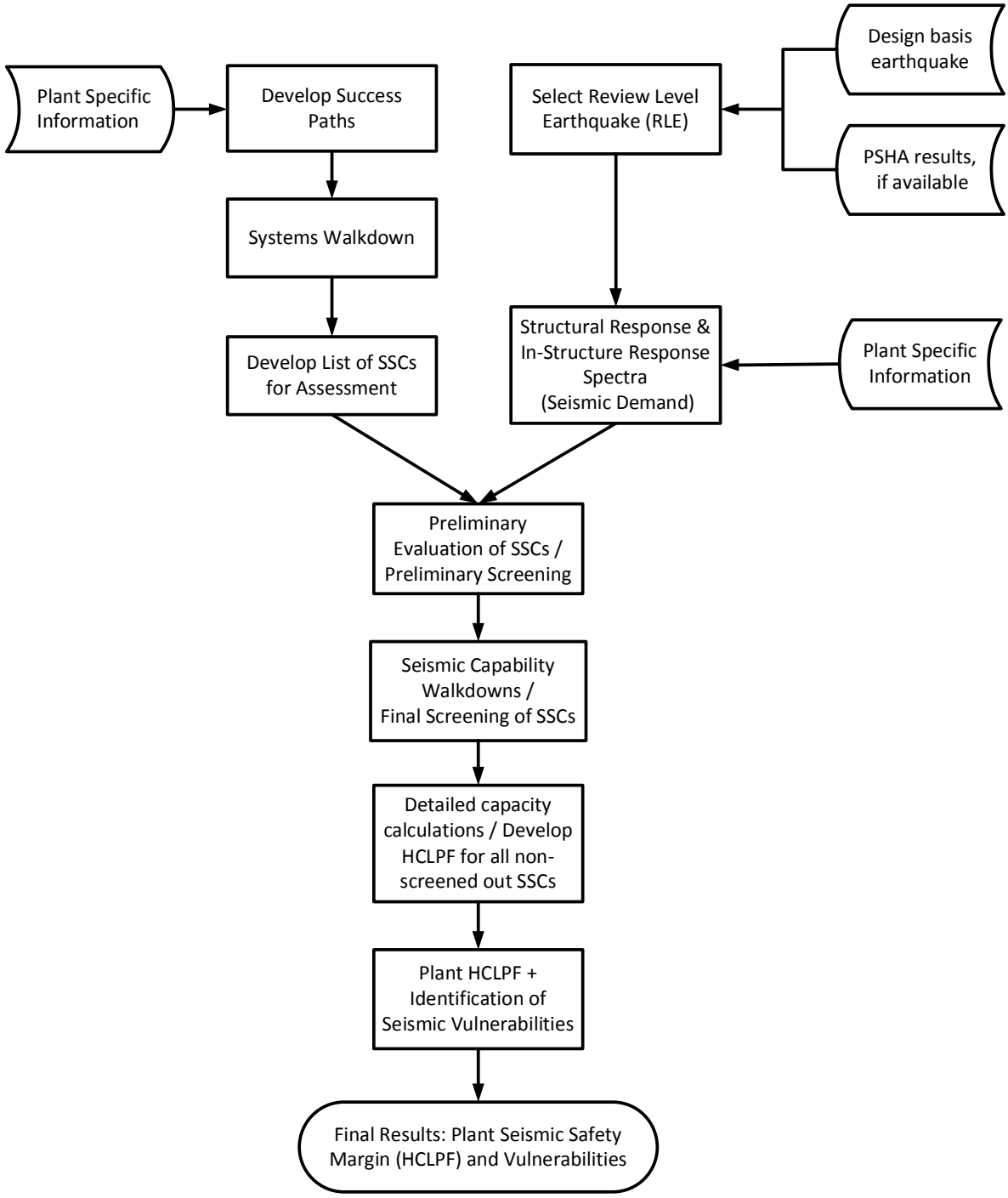


FIG. 6. General workflow of the deterministic SMA method.

HCLPF capacity of SSCs with functionality requirements cannot be obtained just by calculations, unless functionality depends only on keeping structural integrity. Functionality during or after the extreme event normally requires to be demonstrated via testing.

The 'bottom-line results' of a well-executed SMA consist of estimates of the seismic capacities of each of the SSCs analysed, from which are derived estimates of the seismic capacities of the needed

safety functions, and then of the one (or more) success paths, leading ultimately to an estimate of the seismic capacity of the plant as a whole. In actual practice, a typical SMA is usually structured so that the estimated seismic capacities of many of the SSCs under consideration are lower bounds for the capacities rather than realistic estimates. This is due to the fact that estimated capacities used for screening purposes are based upon conservative assumptions.

In summary, the SMA end products of interest are:

- Plant HCLPF capacity, meaning the ground motion level at or below which there is a high confidence of successfully achieving the defined end state for the required time frame;
- Identification of high seismic capacity components with reference to the RLE;
- HCLPF capacities of selected components and success paths as a whole;
- Identification of low capacity components (more vulnerable items or 'weak links');
- Identification of operations that lead to low plant HCLPF values.

5.1.3. PSA-based seismic margin assessment

The NRC SMA method, or PSA-based SMA, was developed as a semi-probabilistic simplification of the full S-PSA method in Ref [20] and it is now used in the seismic safety assessment of standard designs in Ref [49]. The main difference with the EPRI SMA method or deterministic SMA, described in the previous section is the system analysis philosophy. The PSA-based SMA method works in the 'failure space'. It uses the event/tree fault tree approach to delineate accident sequences. SSC selection and the computation of plant margin are based on the identified accident sequences (Section 3.3). On the other hand, the deterministic SMA method works in the 'success space'. It uses the concept of 'success path' for the selection of SSCs and the computation of the seismic margin (Section 3.2).

The core of the methodology remains the same for both methods. That is, the selection of the RLE, the review of plant seismic design information, the development of in-structure response spectra (response of structures to the RLE), the seismic capability walkdown and the relay chatter review are basically the same in both methods.

Following the PSA-based SMA approach, once the Selected SSC List is available, screening of rugged SSCs can be performed based on simple conservative assessment of capacities. Normally, SSCs with an estimated capacity larger than the RLE are screened out. After screening-out rugged components, the seismic fragility evaluation of the remaining SSCs can be performed using the hybrid method in Ref [45]. The hybrid method combines the computation of a HCLPF capacity using the CDFM approach with a conservative estimate of the composite variability coefficient, β_c, in order to produce a mean fragility curve for the component.

The HCLPF capacity value for an SSC is determined as the value corresponding to 1% failure probability on the mean fragility curve for the SSC.

Note that the numerical value for the plant HCLPF capacity is determined at the sequence level, not at the component level. Therefore, given the component and system redundancies, only those components in the minimal cut sets whose capacities are deemed to control the sequence level HCLPF capacity are considered to be the more vulnerable items ('weak links').

The seismic margin is given by the overall plant level HCLPF capacity. The plant-level HCLPF capacity could be determined based on the sequence-level HCLPF values for all sequences as identified in the plant-specific system and accident sequence analysis. The Min-Max method is acceptable for computing sequence-level HCLPF values in Ref [42]. The plant-level HCLPF is therefore the lower bound of the sequence-level HCLPF values and it gives the plant-level capacity.

The effort required to develop a PSA-based SMA is less than the effort required for a full S-PSA. However, it is slightly larger than the effort required for a deterministic SMA, since the list of selected components (SSSC) tends to be somewhat larger with the PSA-based SMA (see Section 3.3). The payback is that the PSA-based SMA gives a better insight about the contributions to the seismic risk and it allows for a consistent consideration of random failures and human errors.

In the recent years, the PSA-based SMA method has been used extensively to justify seismic safety margins of new designs, before the nuclear installation is actually built. For those cases, the RLE is set equal to the seismic design response spectra scaled by a factor corresponding to the target seismic margin (e.g. 1.4 or 1.67).

In summary, the PSA-based SMA end products of interest are:

- Overall plant-level HCLPF capacity;
- Identification of high seismic capacity components with reference to the RLE;
- Seismic accident initiation events and accident sequences and event/fault trees considered in the analysis;
- Seismic capacities for the items in the list of selected components (SSSC), with emphasis in the identification of low capacity components;
- Risk-significant SSCs, dominant cut-sets and sequences;
- Sequence level HCLPF capacities.

5.1.4. Seismic probabilistic safety assessment

As mentioned above, to perform an S-PSA, a probabilistic seismic hazard analysis (PSHA) for the site of interest is required (Section 7.2.1).

However, in the context of a vulnerability assessment, approximate hazard curves can be used to establish the shape of the appropriate uniform hazard response spectra (UHRS) and the reference level for the ground shaking to be used for computation of the seismic structural response. The UHRS shapes are required because the seismic structural response of the buildings is needed to obtain the component fragility curves referenced to the ground motion parameters.

In summary, the S-PSA is comprised of the following steps (Figure 7):

(1) Seismic hazard assessment (Section 7.2.1);

(2) Selection of the assessment team;

(3) Plant familiarization and data collection;

(4) Systems/accident sequence analysis leading to event trees/fault trees modelling and SSC identification;

(5) Determination of seismic response of structures, systems and components for input to fragility calculations;

(6) Seismic capability walkdown;

(7) Fragility calculations for SSCs;

(8) Risk quantification.

Note that some of the steps have common elements with SMA methodologies.

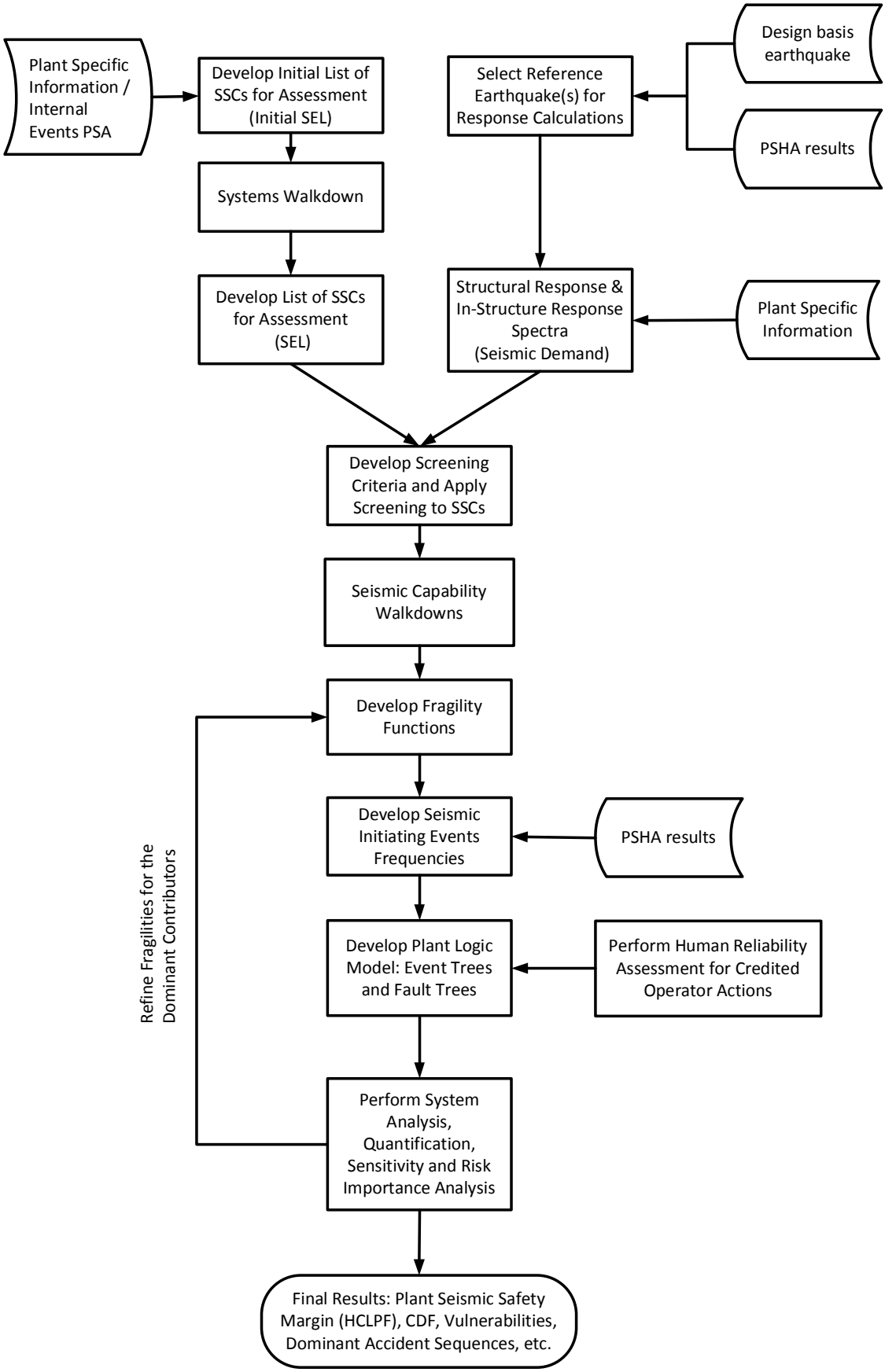


FIG. 7. General workflow of the seismic PSA method.

The systems models of the internal events PSA are to be modified for initiating events and for the responding system behaviour, i.e., the frontline and support systems called into action to prevent the progression of the initiating event to core damage or other undesirable end states. A frontline system is a system that is capable of directly performing one of the accident mitigating functions, e.g. reactivity control, core heat removal, etc. A support system is a system that provides a support function for one or more of other systems, e.g. electric power, cooling, etc. Progression of the accident sequence from the initiating event to core damage is modelled with event trees. The individual failure of components towards system failure is typically modelled with fault trees. In all cases, these trees are modified to account for seismic induced failures, i.e., adding basic events representing failure of SSCs due to seismic impact. Typical initiating events for S-PSAs are loss of offsite power, Loss of Coolant Accidents (LOCA) of various sizes, transients, etc. Based on a combination of engineering assessments and judgment, S-PSA analysts act to limit the number of initiating events to those that are credible. However, at the same time, the analysts may need to consider additional sequences introduced by seismic events. Fragility functions are derived for SSC failure modes identified by the fragility analysts. Systems models representing the containment and other accident containment mitigation systems are appended to the sequences leading to core damage or other failure end state. Boolean expressions of system behaviour are developed and quantified.

The S-PSA end products of interest are insights derived from the model and modelling process and the quantitative end state metrics of core damage frequency and large release frequency (LRF).

In the context of vulnerability assessment, the key results are the plant level fragility data, that is, the conditional probability of not performing the safety functions for a given earthquake strength, and the components which most contribute to the overall risk. For the vulnerability assessment, the plant-level fragility is especially relevant at the low probability range.

The main contributors to plant-level fragility point out to the seismic weak links.

In summary, when S-PSA is carried within a vulnerability assessment, the end products of interest are:

- An appreciation of accident behaviour;
- An understanding of the most likely accident scenarios induced by earthquakes;
- Identification of dominant plant-level seismic fragility contributors: components, systems, sequences, and procedures;
- Seismic fragilities of SSCs and seismic margin as defined by HCLPF capacity values.

5.2. HIGH WINDS AND TORNADOES

The general framework and detailed guidance for plant capacity assessment against high winds and tornadoes are defined in Ref [50] and Ref [51]. The following sections provide the reader with the key aspects.

5.2.1. Reference strength for the hazard

Strength of wind hazard is normally defined by the maximum gust speed in the free field at a specified elevation over ground surface (e.g. 10 m). Gust speed is the average wind speed over a short period of time, typically 3 seconds or less. From this value, wind speed profiles can be built using the ground surface roughness at the site in Ref [52]. These profiles give the undisturbed (free field) wind speed as a function of elevation.

Most nuclear power plant structures have excellent wind resistance, especially when they have been designed for seismic loads. Major vulnerabilities have been identified only where non-seismically designed structures had a potential for collapsing on safety-related structures or equipment. These items include exhaust stacks, unprotected walls, light roofs, outside wiring and cabling, etc.

In view of the above, a large margin over the design wind speed is normally to be expected and the reference hazard strength for the safety margin assessment have to be set significantly larger than the design wind speed for safety related structures. Note that wind pressure is related with the square of wind speed. Hence, doubling the design wind speed would produce four times the design pressures.

Other potential vulnerabilities have to do with unprotected features, located outdoors, which are directly exposed to wind or wind borne missiles. However, these are easily identified during plant walkdowns and their wind capacity improved with a relatively low effort.

Normally, the wind with the reference strength is assumed to blow in any direction. However, in some sites there are clearly preferred wind directions for strong winds. In those cases, the reference strength wind could be assumed to blow in the preferred directions.

5.2.2. Wind response analysis

In this step, dynamic pressure/suction on wind exposed surfaces, pressure variation at air intakes/outlets and mass and speed of potential wind born missiles are to be determined, for the reference wind strength. This is sometimes termed as the 'demand'. For this purpose, a whole range of engineering tools can be used, from wind load design formulas, to wind tunnel or computational fluid dynamics simulations in Ref [52]. According to the guidance in Table 3, demand is to be computed using best estimate parameters and procedures, that is, with no conservative bias.

Note that the wind acting upon the plant buildings is not the free field wind any more. Interference effects, such as sheltering by other buildings or Venturi effects in passages between buildings may have a strong influence in the dynamic pressures. For example, shielding effects of various structures at the site results in an increase of wind speed through a constricted space or a decrease where it may be slowed down due to obstructions. Such funnelling characteristics describing the channelling of winds around structures have a very important influence on the wind forces. The actual forces are also determined by the structural shapes because wind pressure and forces are related to the wind velocity by a shape factor. Another factor important in this regard is the vertical distribution of wind velocity, which is a function of terrain roughness.

5.2.3. Capacity of structures, systems and components

As with other hazards, the most general way of expressing the wind capacity of a component is its wind fragility. Wind fragility is defined as the conditional probability of failure of an SSC as a function of the wind strength parameter. As mentioned above, the wind strength parameter V is normally selected as the maximum gust speed in the free field at a specified elevation over ground surface (e.g. 10 m). Using the results of the wind response analysis, the demand over the structures is computed as function of the same strength parameter V. The capacity could then expressed in terms of median value V_m and logarithmic standard deviations β_R and β_U reflecting the randomness in capacity and uncertainty in the median capacity, respectively. For simplicity, the logarithmic standard deviation β_c, defined as the composite variability, is often used to define a single mean fragility curve.

A conservative value of capacity could be defined as the HCLPF capacity: it is the value at which the mean conditional probability of failure is 1 percent. When a log-normal fragility model is used, the HCLPF capacity is expressed as median capacity times $exp\ (-2.33\ \beta_c)$.

In the context of the present publication it is expected that wind capacity calculations will be performed by direct computation of the HCLPF capacity following the philosophy of the CDFM method (Table 3). If required, a mean fragility curve or a full family of fragility curves could be prepared from the HCLPF value by estimating the composite variability β_c or the logarithmic standard deviations β_R and β_U, respectively.

Wind loading effects include the aerodynamic forces produced by the dynamic pressure component of the wind flow, the associated atmospheric pressure change within the core (for tornado), and impact forces produced by objects picked up and accelerated by the wind field. These wind loading effects

may damage the building housing the equipment of interest or the equipment itself if it is exposed. Failure modes to be considered include structural failure (local and global) under wind pressure or suction; functional failure (HVAC or diesel engine systems); and failure from impact by wind borne missiles.

The capacity analysis for a SSC depends on the definition of failure modes and the potential interaction of individual failure modes as discussed in the following sections. Note that detailed capacity calculations are only performed for the SSCs not screened out after the plant walkdown.

5.2.3.1. Local response

The first set of failure modes that has to be considered corresponds to local structural failures at the surfaces directly exposed to wind pressure/suction forces. These include portions of building enclosure (walls, façade panels, roof panels, doors, etc.) used to transfer the wind loads to the building's main structural system.

This type of local structural failure is the most commonly observed during strong wind events. Typically, these failures do not cause a major collapse, but they might affect the safety significant components located in the immediate vicinity of the failure and, in addition, produce a change in the ambient pressures within the building.

In analysing the failure of indoor equipment (within the buildings), it is conservatively assumed that a failure in the enclosure causes the failure of all sensitive equipment protected by the failed portion of the enclosure.

Wind capacity analysis for these failure modes usually involves assessment of structural capacity of the enclosure elements themselves and assessment of mechanical capacity of the connection to the main structural system. Dynamic effects may have a significant influence in the structural response when natural frequencies are smaller than 2 Hz.

5.2.3.2. Global response

A second set of failure modes that has to be considered corresponds to the global failure or global instability of the main structural system of the buildings under the wind loads. These failures would be able to produce a major collapse of the building.

Wind capacity analysis for global failure modes involves assessment of structural capacity of the main structural system under the wind loads. As for the local response, dynamic effects can usually be neglected when natural frequencies are larger than 2 Hz.

The wind capacity of typical nuclear plant structures in these global structural failure modes is very large, especially if they are concrete structures that have been designed for seismic loads. Hence, in most of the cases, these global failure modes will not be the weak links against the wind hazard and they will be screened out using simple bounding calculations.

In any case, when analysing the failure of indoor equipment, it is conservatively assumed that the failure of a structure causes the failure of all equipment dependent on or within the structure.

5.2.3.3. Impact by wind-borne debris

The aerodynamic forces produced by extreme winds can accelerate objects and produce missiles that impact structures and components. The resulting impactive loads constitute one of the principal loading effects of extreme winds. Wind-borne missiles can include a wide variety of debris types, such as roof gravel; construction materials such as plywood sheets, wood beams, steel pipes, cladding, and structural steel; automobiles; storage tanks; equipment, and tree branches and stems. The heavy missiles with low area-to-weight ratios will generally be rolled or tumbled along the ground. Lighter-weight missiles with higher area-to-weight ratios can be lifted and will fly considerable distances.

Two basic approaches have been used in wind-borne missile analysis. The traditional deterministic approach uses a spectrum of several missile types and maximum velocities to be considered in design or assessment. Using a wind field model and a missile trajectory model, maximum missile speeds are calculated for each missile type. These analyses use simplified 3D trajectory models and an average drag coefficient [52].

The second approach is based on a probabilistic analysis covering a much broader class of potential missiles. This approach also requires a wind field model and a missile trajectory model. Probabilities of missile impact are estimated for each structure or component. These results can be used directly in probabilistic risk studies [50].

Both deterministic and probabilistic methods to evaluate missile effect require the wind field and trajectory models to predict the characteristic velocities of missiles. The impact effects are generally evaluated using empirically-based penetration, perforation, or spall equations. For certain types of missile, overall structural dynamic response analysis may also be required.

As a rule of thumb [50], maximum velocities for wooden missiles are generally about 75% of the horizontal wind velocity. For steel pipe missiles, the maximum missile velocity is about 40 to 60% of the horizontal wind velocity. For automobile missiles the maximum missile velocity is about 18 to 20% of the horizontal wind velocity.

Missile impact effects include local response (penetration, perforation, and spall) and overall response (such as dynamic shear effects at the edge supports of the impacted wall). Local response effects are estimated by semi-empirical formulas that take into account the missile type and target materials [50]. Overall response is analysed through dynamic response analysis considering deformation of the missile and the impact force time history. The velocity and orientation of the missile are important input parameters to determine missile impact effects. In deterministic analyses, the missile impact is assumed to have a velocity vector normal to the target surface and the missile axis is collinear with the velocity vector. In probabilistic analyses, the velocity vector and missile obliquity can be treated as random variables.

In a particular site, potential wind-borne missiles are identified by means of specific missile survey walkdowns. The survey covers the entire plant area, generally up to 750 m from the safety significant SSCs. The Missile Origin Zones are established initially using plant drawings and aerial photos of the plant. Generally 20-50 missile zones are established, with the following criteria:

- What is in each zone, buildings, parking lots, what targets, etc.;
- The minimum and maximum injection heights of missiles are constant for a zone;
- Plant grade changes are handled through changes in zones.

Afterwards, during the walkdown, the following information is collected for each zone:

- Potential missiles present in the zone. Generally, the following general categories of missiles are considered, based on aerodynamic considerations:
  - Cylinders, such as cylindrical rods or pipes;
  - Rectangular rods;
  - Plates;
  - I-shaped beams;
  - Angles or channels;
  - Frames or trusses;
  - Spheres or balls;
  - Vehicles;
  - Trees.

- Missile-source buildings or structures: buildings which have not been designed as high wind or tornado resistant and, therefore, can be a source of missiles for other structures or components. Estimation of missiles created by the failure of the building in a wind storm, with minimum and maximum injection heights, is a result of the walkdown. Non-concrete frame buildings are to be included in the survey;
- Equipment: light weight equipment not bolted to a heavy engineered steel or concrete frame have to be considered as potential missiles. If the equipment is bolted down to concrete or heavy steel frame and is unlikely to fail in a wind storm, then it does not have to be counted during the survey;
- Turbine building and containment façade: each floor of the turbine building needs to be surveyed separately and will include evidence of any loose materials (pipes, conduit, etc.) stored within these buildings;
- Trees: trees with a diameter of 12 cm or greater at breast height have to be counted within the survey. Single trees/small groups of trees will be counted as individual trees. For larger wooded areas within 360 m of targets, tree quantities are estimated from area density (trees per square meter) in a representative zone;
- Minimum and maximum missile injection heights: they refer to the height above the base elevation of the zone or missile source structure at which the centre of mass of the missiles are stored within the missile source. The minimum injection height is noted as the approximate centre of mass of the lowest missile of each type located within the missile source zone or building and the maximum injection is noted as the approximate centre of mass of the highest missile of each type located within the missile source zone or building.

5.2.3.4. Atmospheric pressure changes

Atmospheric pressure change (APC) loadings result from the variation in the atmospheric pressure field as a vortex moves over a structure. Atmospheric pressure change loads are of practical engineering significance only for tornadoes, with the combination of relatively high translational storm speed (generally greater than about 13 m/s) and maximum pressure drop in the centre of a rapidly rotating vortex.

The estimation of APC loads requires a model of the tornado wind field and knowledge of the rate at which the structure may vent. For a perfectly sealed structure, such as a nuclear containment, the APC produces outward-acting pressures across all surfaces of the structure.

However, equalization of inner and outer pressures generally will occur for most other structures as a result of breaching of the building envelope by wind or missile effects or because of the inherent ventilation and leakage paths of the building. In addition, the slower the translational speed of the tornado, the more time available for internal and external pressures to equalize. Further, if the tornado core does not totally engulf the building, the APC loadings will apply on to the affected building surfaces.

There have been only limited analyses of pressure equalization due to tornado and the amount of venting needed such that the APC loadings do not materialize. A preliminary analysis of the mechanical ventilation system in nuclear fuel cycle facilities is reported in Ref [50]: it is estimated that 1000 cm^2 of venting per 30 m^3 of interior volume is adequate to vent buildings effectively from severe tornado APC loads. Most commercial structures have this amount of venting through the heating, ventilating, and air conditioning (HVAC) systems, exhaust fans, doors, and cladding leakage.

5.2.4. Plant-level capacity

In summary, the major steps for plant capacity assessment for high winds are:

(1) Choose the reference parameter for wind hazard and wind capacity evaluations. Normally, the parameter is the wind gust speed (e.g. wind speed averaged in 3 s) at a reference height in the free field (e.g. 10 m height). The wind speed profile as a function of height can be developed using this value and the roughness of the terrain around the site;

(2) Select wind speed reference level(s) for wind capacity evaluations. Note that wind pressure is related to the square of wind speed. Hence, doubling the design wind speed would produce four times the pressures used in design;

(3) Obtain the response of plant SCCs to the reference level wind speed(s). In this step, dynamic pressure/suction on wind exposed surfaces, pressure variation at air intakes/outlets and mass and speed of potential wind born missiles are to be determined, for each reference wind speed;

(4) Plant walkdown, in which SSCs not likely to be the more vulnerable items ('weak links') against wind are screened out;

(5) Compute HCLPF capacity of safety significant components. Failure modes to be considered include: structural failure (local and global) under wind pressure or suction, functional failure (HVAC or diesel engine systems) and failure from impact by wind borne missiles. Capacity is expressed in terms of gust speed at the reference height in the free field;

(6) If required in the following steps, estimate the uncertainties β_c for the mean fragilities. Computed HCLPFs and estimated β_c define the mean fragilities for the failure modes. Note that detailed capacity calculations are required only for those modes not screened out during the plant walkdown due to a judged large wind capacity;

(7) When following the deterministic approach (Section 4.2), use the HCLPF capacities of SSCs on the success paths to safely withstand the wind effects (Section 3.2). The lowest capacity components on the success path determine the plant-level capacity of the path and define the 'weak links' against wind hazard;

(8) When following the semi-probabilistic approach (Section 4.3), recover the accident sequences used to develop the Selected SSC List (Section 3.3); with the mean fragilities of SSCs appearing in these sequences, calculate the plant level mean fragility curve. Calculate the wind speed for which the probability of failure is 1% and identify the main contributors (SSCs) to this probability. The computed wind speed gives the wind safety margin and the main contributors are the weak links against wind hazard. Alternatively, instead of using mean fragility curves, use HCLPF values and the Boolean equations corresponding to the accident sequences to compute the plant-level HCLPF capacity using the Min-Max approach.

5.3. FLOOD

5.3.1. General

Increase of water levels in a nuclear power plant site, up to the point that water starts affecting safety related systems, may compromise the performance of the fundamental safety functions and start an accident sequence. As it is the case of earthquakes, floods can affect many areas of the facility at the same time and, as a consequence, defeat redundancy and diversity of safety systems. Electrical systems are especially vulnerable to these events.

As discussed in Section 2, there are several types and combinations of external-flooding phenomena that need to be considered, depending on the site. These include both natural phenomena (high river or lake water, ocean flooding such as from high tides or wind-driven storm surges, extreme precipitation, tsunamis, seiches, flooding due to dam failure, flooding from landslides, etc.), and man-made events (principally, release of flow from water control structures).

In general terms, deterministic, semi-probabilistic and fully probabilistic approaches for flood capacity assessment are available, that mirror the approaches used for the assessment against seismic hazard.

Deterministic capacities (flood levels) are developed from design basis analysis to ensure that operation of a nuclear power plant can be carried out with adequate levels of safety in all modes of operation and at all times. The basic concept is to determine limiting values of flood height and associated hazards such as impact forces, which, if exceeded, could lead to an undesirable state.

The fully probabilistic approach aims at identifying possible faults, deficiencies and plant vulnerabilities, and providing a balanced picture of the safety significance of a broad spectrum of issues, including the uncertainties of the results. However, it must be noted that worldwide experience about PSA external-flooding analysis is much more limited than in the seismic counterpart.

The semi-probabilistic approach is a simplification of the fully probabilistic approach that avoids the hazard related issues, but retains three of the basic ingredients: (1) plant specific system and accident sequence analysis, even if simplified by reducing the total number of initiators; (2) fragility evaluation; and (3) plant-level capacity determination.

All three methods are valid choices in the context of this publication; even though the fully probabilistic approach will cover a scope which is wider than required here.

In the following sections, the key points of both the deterministic and the semi-probabilistic approaches are presented. The results provided by these two approaches are sufficient for the purpose of identifying significant weak links. For the interested reader, the probabilistic safety assessment (PSA) against external flooding is described in Ref [50].

5.3.2. Deterministic approach

Similar to the seismic hazard, the deterministic methodology for assessing the safety margin against flood is based on the 'success path' approach (Section 3.2). One (or more) success paths must be identified. Each success path consists of a selected group of safety functions capable of maintaining the nuclear installation in a safe state or bringing the nuclear installation to a safe state and of maintaining it there for an agreed upon time. The individual SSCs needed to accomplish each of the success paths are then identified and become the basis for the rest of the analysis.

The assessment defines and evaluates the flood capacity of each of the SSCs on the success path(s). Capacities of SSCs are defined as High Confidence of Low Probability of Failure (HCLPF) values. In a probabilistic sense, the HCLPF capacity is the flood severity (e.g. flood height) with about a 95% confidence of a 5% frequency of failure; or an equivalent mean confidence of a 1% frequency of failure.

Analysis involves looking for the ways through which the water could reach the SSCs considered in the success paths and computing the flow capacities of those ways for the reference flood severity, including:

- Drainage systems, which could by-pass flood barriers;
- Building penetrations, whose seals may not be flood resistant for the reference flood height;
- Doors or other openings in the building enclosures, which may not be water-tight or which could structurally fail for the reference flood height.

For exposed equipment and structural components, the analysis involves also 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.

Component capacity calculations are usually simpler than in the seismic case, since flood-caused failure of equipment is typically due to immersion, and it is usually assumed that equipment submerged by the flood waters, and not specially protected, will fail, meaning that it will fail to perform its safety function. Hence, once the flood height is determined in a particular room or plant area, it is immediate to identify the 'failed' equipment.

Failure of building structures could also happen. It can be global, such as due to a foundation failure; or local, such as failure of a wall or barrier leading to leakage or major flooding through the wall or barrier. Typically, for structures, overall stability (sliding, overturning, scouring and floatation) and wall integrity are assessed for the reference flood height.

Evaluation of the plant HCLPF capacity (flood level) can be achieved relatively simply from the HCLPF capacity values of SSCs comprising the success paths. Plant HCLPF capacity is taken as the plant-level capacity. The components governing the plant-level capacity correspond to the items more vulnerable to flood ('weak links'). It is to be expected that, due to the plant layout, many items share the same elevation and, consequently, a small increase in water level is able to produce many simultaneous failures ('cliff edge' effect).

In summary, the deterministic method is comprised of the following steps:

(1) Selection of the review level flood, which is the reference flood event. The review level flood is usually defined in terms of flood height;

(2) Selection of the assessment team;

(3) Plant familiarization and data collection;

(4) Selection of success path(s);

(5) Determination of flood heights at the position (room, area, etc.) of SSCs comprising the success paths, for input to flood capacity calculation. Note that in this step flow paths and flow ingress are to be determined and some capacity calculations might be needed to assess resistance of seals, doors, or walls in order to prevent water penetration into buildings;

(6) Systems walkdown to review preliminary success path(s), select final success path(s), and SSCs;

(7) Flood capability walkdown, screening out of high capacity components (e.g. equipment located at high elevations);

(8) HCLPF capacity calculations (SSCs and plant-level).

The results consist of estimates of the flood capacities, expressed as flood height at the site, of each of the SSCs analysed. From these capacities, estimates of the flood capacities of the needed safety functions are derived; and then, of the one (or more) success paths, leading ultimately to an estimate of the flood capacity of the plant as a whole.

In summary, the end products of interest are:

- Plant HCLPF capacity, meaning the flood height at or below which there is a high confidence of successfully achieving the defined end state for the required time frame;
- Identification of high flood capacity components;
- HCLPF capacities of selected components and success paths as a whole;
- Identification of low flood capacity components (weak links);
- Identification of operations that lead to low plant HCLPF values.

5.3.3. Semi-probabilistic approach

5.3.3.1. Selection of structures, systems and components

Within the semi-probabilistic approach, the Selected SSC List is obtained using the event tree/fault tree method (Section 3.3). Those external-flooding-event tree/fault tree models are almost always based on the internal-events, at-power PSA systems model, to which are added basic failure events derived from the information developed in the initial flooding vulnerability analysis. Considerable screening out of parts of the internal-events systems model is also common, where appropriate. The analysis consists of developing event trees and fault trees in which the initiating event can be either the extreme flood itself or a transient or loss-of-coolant accident induced by the extreme flood (Table 2).

One key consideration is that many large external floods occur only after significant warning time, which allows the plant operating personnel to take appropriate steps to secure the plant and its key equipment. The analysis team may sometimes take credit for warning time and compensatory actions, if the plant's planning and procedures allow.

Potential operator actions and mitigating measures to be considered when modifying the internal events PSA models are:

- Temporary barriers (time to construct and effectiveness etc.);
- Closing of flood doors and hatches – are there procedures in place?
- Draining of the room using pumps (failure rate, human errors, etc.);
- Personnel access to safety equipment or controls (focus of the walkdowns);
- Reduced likelihood of system recoveries after an external flood event;
- Potential unavailability of off-site response resources.

It is vital that the analysis capture the important dependencies among external flood caused failures (e.g. spatial or environmental dependencies) since the external flood could affect multiple SSCs at the same time. The clogging of intake structures and other flow paths by debris related to the flooding must also be considered, and a walkdown is important to ensure that this issue has been evaluated properly.

During an extreme flood, the restoration of safety functions can be inhibited by any of several types of causes; these include damage or failure, access problems, confusion, loss of supporting staff to other post-external flood-recovery functions, and so on. Careful consideration of these must be given before recoveries are credited in the initial period after the external flood event. This is especially true for externally caused loss of off-site power given that the damage could be to switchyard components or to the off-site grid towers, which are generally difficult to fix quickly.

5.3.3.2. Capacity of structures, systems and components

The next step is to assess the flood capacity of the selected SSCs. The objective is to identify those SSCs that are susceptible to the effects of external floods and to determine their plant-specific failure probabilities as a function of the severity of the external flood. The flood height is normally selected as a global parameter for describing the severity of the flood, but all other characteristics of flooding have to be considered in the capacity analysis.

It is to be noted that there are very few examples of formal probabilistic flood fragility analysis of nuclear power plant SSCs. The methodology described here is similar to that used for other external hazards (e.g. seismic and wind).

The scope of fragility analysis is based on the flood hazard type and magnitude and how the plant including operators will respond to a flooding situation. As a first approximation, the systems analyst may group the SSCs of interest to the external flooding assessment into those that are enclosed in buildings and those that are outdoors in the yard. The fragility analyst may then screen out some of the

buildings based on their elevation and/or their capacity to withstand the flood (depending on the design criteria). External barriers that are considered in this screening include building walls and roofs, flood doors, flood walls and berms.

For the remaining buildings and outdoor SSCs, flood fragilities are developed using the hybrid method in Ref [45], after computing the HCLPF capacity. Fragility functions may be developed using empirical observations, analytical approaches, engineering judgement or some combinations of the above. They may be characterized by a step function (cliff-edge type failure, as in overtopping failure modes) or by smooth functions (as for failure modes associated with static and dynamic loading). The loads to be considered are hydrostatic, hydrodynamic and debris (missile impact and clogging). Figure 8 gives an example of a family of smooth flooding fragility curves.

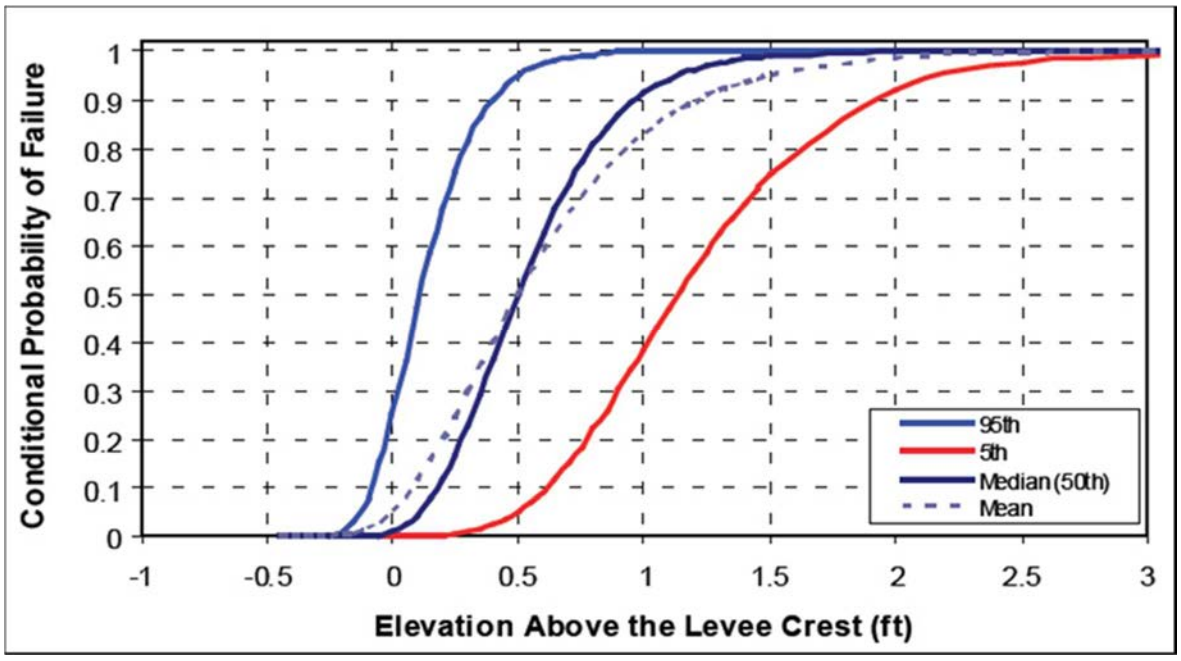


FIG. 8. Example of flooding fragility curves.

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. The analyst 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. The analysis has to include length of warning time, since plant personnel may be able to secure equipment in a safe configuration. Further, the analysis must include whether the failure of an item of equipment would leave it in a fail-safe position. Also, flood waters may only partially submerge an item of equipment, so the analysis must determine how much partial submersion would be sufficient to cause the failure.

Failure of structures could be global, such as due to a foundation failure, or local, such as failure of a wall or barrier leading to leakage or major flooding through the wall or barrier. Most nuclear power plant structures have inherent resistance to flooding, by design. Major vulnerabilities have sometimes been identified for certain structures, but usually, the equipment housed therein is not crucial to overall plant safety. The plant walkdown could play a major role in identifying potential problems, supplemented by an evaluation of structural drawings.

Failure modes to be evaluated for structures include:

- Penetration or leak;
- Wall integrity;
- Stability (sliding, overturning, scouring and floatation).

When the flood reaches an equipment item (especially electrical equipment), the analyst may judge that it results in failure. Once the flood enters a room, the propagation of the flood to adjacent rooms can be assessed using the internal flooding PSA model, taking into account that source and volume of water may be significantly different and actions to limit or reduce the inflow of water in the internal flooding may not be successful in this case.

5.3.3.3. Plant-level capacity

The plant-level capacity against flood is given by the plant-level flood fragility curve. Plant-level fragility is obtained by combining the component fragilities using the Boolean expression for the accident sequences used in the selection of SSCs (Section 3.3).

In the context of the present vulnerability assessment, the key results from the semi-probabilistic method for flood capacity assessment are the following:

- Plant-level fragility curves or plant-level HCLPF capacity, from which the plant flood capacity can be computed;
- Plant vulnerabilities or weak links, based on dominant contributors to plant-level fragility or plant-level HCLPF capacity.

5.4. AIRCRAFT IMPACT

The general framework and detailed guidance for plant capacity assessment against aircraft impact are defined in Refs. [18, 53, 54]. The following sections provide the reader with the key aspects.

5.4.1. Reference strength for the hazard

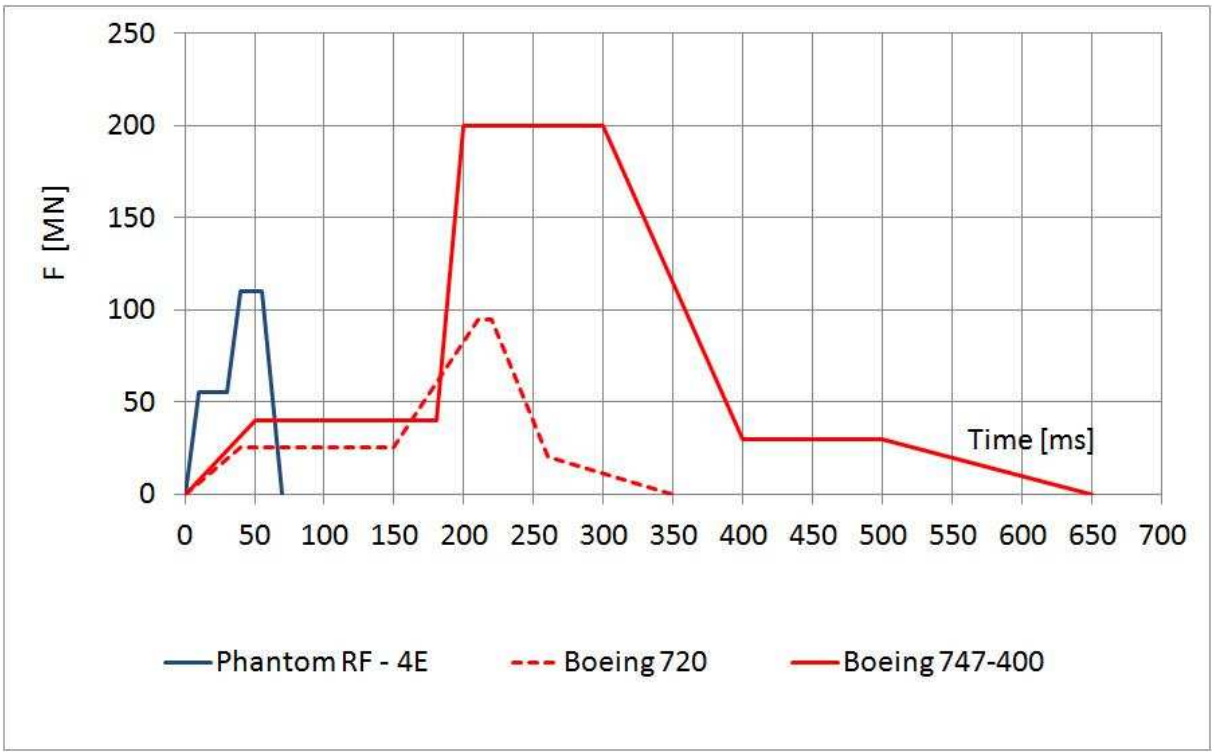
For the hazards analysed in the previous sections, the strength is usually defined using a single parameter with a continuous variation; for example, maximum flood level or the maximum ground acceleration. In the case of aircraft impact, the strength of the hazard depends on the size of the aircraft in the possible impact scenarios. Continuous variation of size does not occur in practice, since size depends on the categories of aircraft in operation. For the purposes of the present vulnerability assessment, the categories in Table 4 are considered. Note that the table defines four categories of civil aircraft and a single category of military aircraft.

TABLE 4. AIRCRAFT CATEGORIES FOR CAPACITY ASSESSMENT

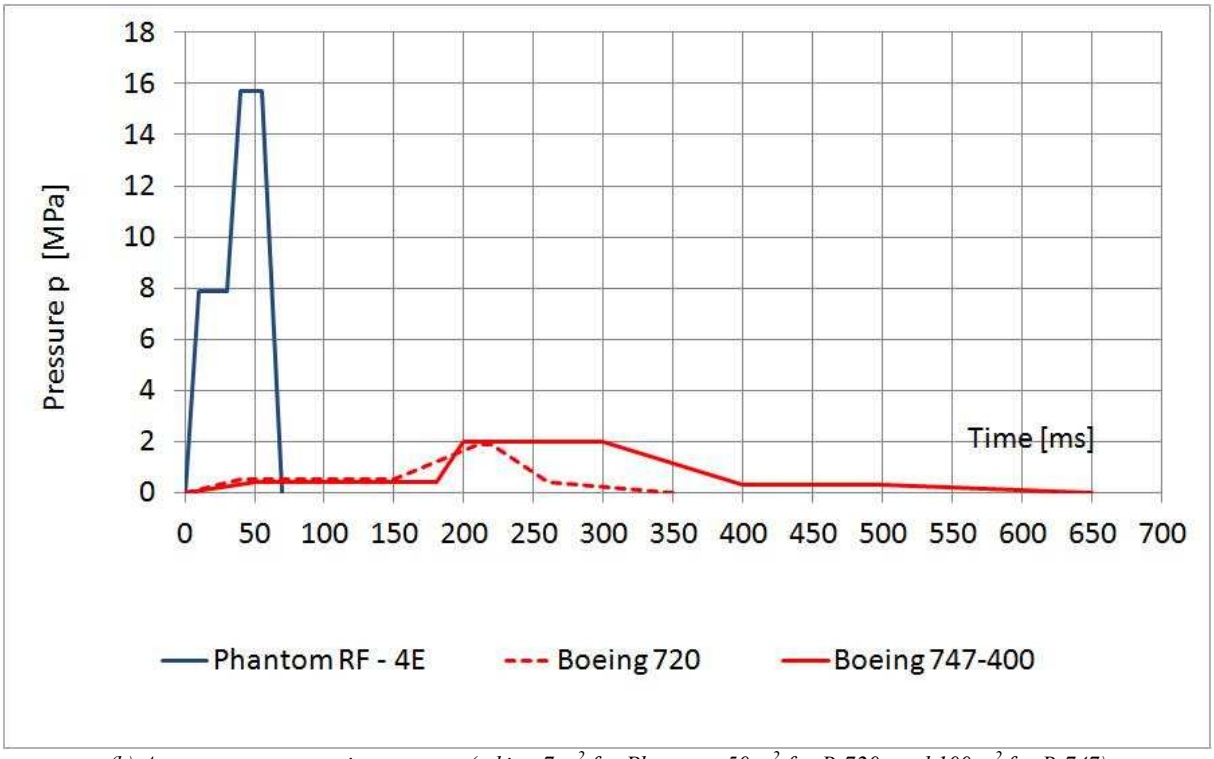
Category	Maximum Take-Off Weight MTOW (kg)	Velocity range (m/s)	Examples
A	< 20000	70 – 160	General aviation planes Cessna 210, LearJet 23, Canadair WaterBomber
B	< 100000	70 – 160	Light weight passenger planes Boeing 720, Boeing 737, Airbus A320
C	< 200000	70 – 160	Medium weight passenger planes Boeing 767, Airbus A300
D	> 200000	70 – 160	Heavy weight passenger aircraft Boeing 747, Airbus A340, Airbus A380
Military fighters	< 35000	< 220	Eurofighter, Rafale, Phantom

Note: Velocity ranges correspond to generally accepted limits for low level flying close to an industrial facility [55]. At present, there is no international standard giving aircraft impact velocity values for assessment of beyond design conditions

For illustration purposes, Figure 9 shows the impact force and average pressure time histories derived using the Riera method in Ref [54] for normal impact at assumed velocities of some of the aircraft included in the table in Ref [55].



(a) Total force (elaborated from Ref. [55])



(b) Average pressure on impact area (taking 7 m^2 for Phantom; 50 m^2 for B-720; and 100 m^2 for B-747)

FIG. 9. Typical impact load time histories for several aircraft types.

Note that the shape of the time histories is similar, but the force peak, total impulse, maximum average pressure and total duration of impact vary from one category to the other. The force peak is not

necessarily the most relevant damage indicator for civil structures, if the corresponding impacted area is very large. For assessing local damage, the maximum pressure or the maximum force per unit length along the perimeter of the impacted area can be considered, in some cases, the most relevant damage indicator in Ref [56]. The size of the impacted area, the weight of the semi-hard impacting bodies (engines) and the amount of fuel that could lead to a fire after the impact are also linked to the category of the aircraft [54].

For the capacity assessment against aircraft crash, the reference strength is selected by defining the aircraft category that have to be considered and the speed at impact. After selection of the aircraft category and speed, the rest of parameters defining the impact (e.g. impact load time history function, area of application of the load, parameters defining the engines, amount of fuel) can be obtained using the procedures described in Ref [54].

The selection will depend on considerations such as the location of the airport or airways with respect to the nuclear power plant, the kind of air traffic in the region and the type and size of aircraft that could accidently impact the plant. For a postulated aircraft impact, it is expected that the competent authority of the Member State will specify the category to be used. Once the type of aircraft has been selected the reference strength parameter for fragility or HCLPF capacity evaluation is normally taken as the speed at impact.

5.4.2. Response of the plant

Once the reference strength has been selected (i.e., aircraft type and aircraft speed), hazard scenarios have to be developed based on the plant layout, the topography of the plant vicinity and the layout of nearby facilities, if any. The configuration of the plant and its surroundings may prevent direct impact on some buildings or plant areas. Flight mechanics of the reference aircraft can be used to rule out these impacts.

Hazard events have to conservatively envelope all impact possibilities. To help in the selection of events for further study, the concept of 'zone of influence' can be used. This concept has been developed from the analyses of the few cases of aircraft impacts with engineered structures (buildings). Particularly, the Pentagon and World Trade Center (WTC) performance reports provide useful guidance that might be applied to the NPP case [57, 58]. It needs to be said that the feedback from these two cases is related to civil structures which are not as strong as the majority of civil structures found in safety buildings of NPPs. As a consequence, the following considerations have to be carefully used and adapted to each particular case.

The results of the studies assessing those two impacts found that, initially, the damage was confined to a roughly triangular shape, extending along the direction of the approach. In the case of the Pentagon (Boeing 757, Category B aircraft in Table 4) the damage swath was approximately 25 m at the point of entry into the building and extended to a depth of approximately 70 m. Less severe damage, caused by flying debris and secondary missiles, was found to extend beyond the initial zone of impact.

In the case of the Pentagon impact, fire damage, due to burning of the jet fuel and to secondary fires caused by ignition of on-site combustibles, extended into the areas unaffected by the impact, until contained by the building fire suppression systems.

The concept of the 'zone of influence' could be applied to nuclear installations for the purpose of screening an initial set of possible impact events. Since the structures in the nuclear installation will normally be stronger than the Pentagon and the World Trade Center, the zones of influence found in these two cases will provide upper limits. By imposing the damage and debris triangles on a scaled representation of a nuclear plant, aligned along each determined approach path(s), one can obtain a bounding approximation of the areas of damage likely to occur to the relevant building. The footprint of the fire and smoke damage can be obtained by extending the zone of influence out until met by a fire barrier that has not been damaged by the initial impact or subsequent debris. In Ref [59], the zone

of influence is referred to as ‘damage foot print’ and damage rules for developing the damage foot print for physical damage of buildings by aircraft impact, by debris and by fire/smoke are described.

One would expect that this concept may provide reasonable, initial estimates of the damage caused by an aircraft impact to a NPP based on the evidence given by past events. Clearly this methodology could not be applied to certain structures within a NPP: hardened and robust structures, such as the containment building, would provide additional protection when compared to the structure of the Pentagon building. These key structures, whose failure could lead to significant, immediate consequences, would require additional evaluation to ensure that their integrity can be maintained. However, the concept could serve to focus the evaluation on those critical events, where there exists the possibility of damaging a larger number of safety significant components. Additionally, for each selected event, the concept can serve to differentiate the areas at which little damage is to be expected from the areas where components are highly likely to be failed in the crash.

Implementation of this concept results in a visual representation similar to that shown schematically in Figure 10 for aircraft crash in one direction.

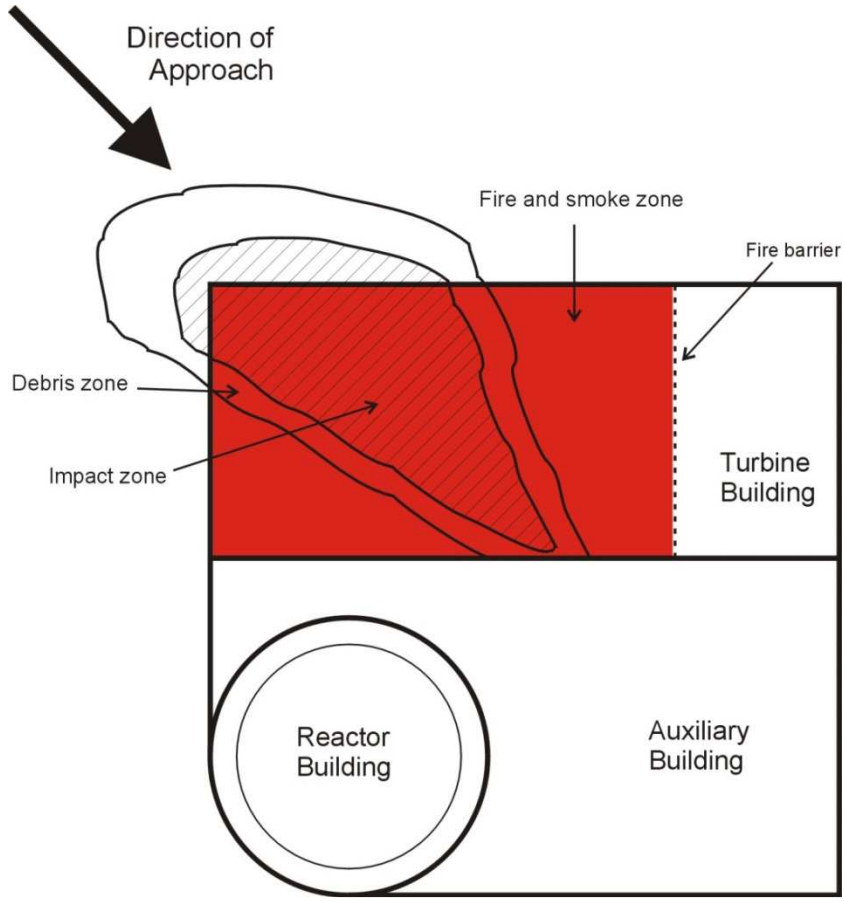


FIG. 10. Simplified schematic of a nuclear power plant indicating the three zones of influence following an aircraft impact.

When the success path approach is used to select the safety significant components (Section 3.2), it is possible that the success paths need some adaptation to the selected events, with the intent that in each case, at least one success path remains out of the area severely damaged by the impact. In other words, in the case of the aircraft impact hazard, the selected components will likely depend on each selected event.

For example, assume that the emergency cooling system is located primarily on the north side of the plant, whereas the shutdown maintenance cooling system is located on the south side, with the reactor building between them. Preliminary analysis has shown that either may be relied on to maintain the

basic cooling requirements for removal of decay heat. Consider the postulated aircraft approaching from the north and the south directions for evaluation by the zone of influence approach. For the case of approaching from the north, using the zone of influence concept, one assumes that the emergency cooling system is unavailable. However, one has reasonable assurance that the maintenance cooling will survive the impact, debris, and fire, thus assuring that basic cooling functions are maintained. The opposite would be true for the approach from the south.

Caution has to be exercised, however, if this methodology is to be used to exclude events from further consideration. Due to the uncertainties associated with this method, one must have a high degree of certainty that the essential safety functions are maintained. Also, for open areas such as a turbine hall, the zoning might be an underestimate, whilst for a cellular structure with many interior walls such as a control building the effects would certainly be more confined. Detailed consideration therefore needs to be given to postulated affected buildings and plant, and the methodology could be applied by a multidisciplinary, experienced team in this domain.

The zone of influence methodology may serve also to identify clear vulnerabilities. For example, some NPPs may locate the primary and the secondary control room within close proximity to each other. When the damage footprint is imposed on the plant layout, assuming that it is feasible for the aircraft to approach from any direction, one would see that there is a good possibility that both control rooms may be lost simultaneously, or that the access to the secondary control room is impeded due to the severe fires expected.

A final observation is that the zone of influence depends on the event, but also on the structural barriers. A particular structure may withstand the impact but an adjoining structure may fail and collapse on the first structure. The potential for such interactions have to be examined in the in-plant review.

In summary, the zone of influence is constructed for each possible event as follows:

(1) The impact zone is developed based on the impact location and the barriers (i.e., walls and roofs of buildings). If these barriers are damaged by impact or missile, it is assumed that the SSCs housed within the building are no longer functional.

(2) When the barrier is damaged by the missile or if the missile (aircraft) itself is damaged resulting in missiles, the debris created by these events have to be assessed and the area over which the debris spreads have to be evaluated; the SSCs within this debris zone are also assumed to be not functional.

(3) If there is fuel available in the form of jet fuel of the impacting aircraft or because of damage to yard tanks with flammable inventory (e.g. diesel fuel oil tanks), the fire zone have to be evaluated based on the structural damage due to the impact, the amount of fuel, the presence or lack of fire barriers, and emergency fire mitigation measures. The propagation of structural damage due to the fire has to be assessed. Reference [54] has the detailed procedures for this evaluation. In general, the footprint of the fire and smoke damage can be obtained by extending the zone of influence until met by a fire barrier that has not been damaged by the initial impact or subsequent debris.

(4) The SSCs within this fire and smoke zone are assumed to be not functional.

Thus, the concept of ‘zone of influence’ can be used for the purpose of preliminary screening of events. Actual component capacities are obtained as described in the following section.

5.4.3. Capacity of structures, systems and components

The prevention of penetration of the impacted outer shell or wall of a structure against the load applied by an aircraft crash represents the main goal of the protection of the nuclear power plant. The maximum impact load per unit surface provides the indication for the possibility of local overstressing of the structure and initiation of the penetration processes. An assessment of the danger of penetration

has to be therefore performed not only for the maximum loads related to the whole airplane but also for their parts impacting with the same velocity but acting on a much smaller surface. The response of a building structure due to the crash of an airplane is mainly dependent on the type of the airplane, the design concept of the structure and thickness of the outer shell of the structure as well as the location of the impact region on the building.

In order to assess the effectiveness of the overall protection concept of a nuclear plant building subjected to impact, fire, and other concomitant events, the following need to be checked:

- The global stability (overturning) of the safety related structure;
- Major structural damage such as collapse of large portions of the building;
- The penetration resistance of the impacted outer walls/shells;
- The integrity and functionality of the safety relevant systems and components;
- Fire resistance.

The stability checks have to be performed for the loads applied by the airplane acting on the corresponding building at the upper regions considering the local soil conditions. The other potential failure modes are discussed in the following.

For plant-level capacity assessment, the fragility or the HCLPF capacity for the safety significant SSCs, such as buildings, are calculated. Fragility is defined as the conditional probability of failure of SSC for a given value of the hazard reference parameter (e.g. aircraft speed). The capacity is then expressed in terms of median value and logarithmic standard deviations β_R and β_U reflecting the randomness in capacity and uncertainty in the median capacity, respectively. For simplicity, the logarithmic standard deviation β_c, defined as the composite variability, is often used.

A conservative value of capacity could be defined, borrowing from the seismic PSA literature [48], as the HCLPF capacity: it is the value at which the mean conditional probability of failure is 1 percent. The HCLPF capacity is expressed as median capacity times *exp* (-2.33 β_c).

Evaluation of the fragility of SSCs relies to a large extent on the combined expertise and experience of the engineering safety personnel carrying out the evaluation. It is to be pointed out that fragility evaluations of SSCs exposed to aircraft impact have not been conducted extensively so far. Hence, there is not much reported experience in the estimation of variability (β_R and β_U or β_c).

In structural analyses involving severe nonlinearities, such as aircraft crash computations, it is not always easy to assess whether a modelling assumption is conservative or not. Hence, the analyst tends to work under best estimate assumptions, which will produce median centred capacity results, not HCLPF capacity results. Estimation of variability (e.g. β_c) requires the performance of sensitivity studies that are not always done in practice, due to lack of resources.

For input to the plant-level capacity assessment, the HCLPF capacity is to be estimated for the relevant failure modes. For estimation of HCLPF capacity from median centred capacity results, an estimate of the composite variability β_c is required. The reader is referred to published research that investigated this variability for aircraft crash analyses in Refs. [18, 55].

5.4.3.1. Local response

The sequence of localized loading effects consists of three stages: missile penetration into the target; spalling and scabbing of the target; and, potentially, missile perforation completely through the target. These terms are defined in Ref [54]:

Penetration – the displacement of the missile into the target. It is a measure of the depth of the crater formed at the zone of impact.

Spalling – the ejection of target material from the front face of the target (i.e., the face on which

the missile impacts).

Scabbing – the ejection of material from the back face of the target (i.e., opposite the face of impact).

Perforation – the missile fully penetrates and passes through the target.

The term 'perforation velocity' refers to the initial missile velocity which is just sufficient to fully perforate the target with residual velocity equal to zero [54]. The term 'residual velocity' refers to the exit velocity of missile that has an initial velocity greater than the perforation velocity.

Such local damage modes would not, in general, result in structural collapse, but instead are considered because of their potential to damage safety-related systems or components. The induced velocity of the scabbed material or the residual velocity of the perforating missile could potentially cause equipment/system failures.

The primary local response effect of interest is the perforation of a compact, high density, but crushable engine through reinforced concrete walls. In addition, scabbing of concrete from the inside surface of the structure is considered if critical equipment for plant shutdown is located at or near the back surface of the concrete wall at the location of missile impact.

Given that an impacting engine has an initial velocity that exceeds the perforation velocity associated with a primary structural target wall, the damage potential of the crushed engine mass impacting on secondary structural concrete walls or a steel containment shell at the residual velocity must be determined. The residual velocity of the perforating missile may be predicted by considering the residual kinetic energy (the initial kinetic energy of the missile less the energy loss during perforation) is imparted to the crushed engine mass and a volume of concrete which is also ejected. After perforation of a primary wall, the exiting casing and shaft is now a compacted semi-solid missile with the approximate diameter of the engine casing. Thus, the local damage potential of the crushed engines impacting on secondary concrete targets can be predicted using the same empirical formulas, but with a reduced mass and slightly different modification factors to account for the residual crushability of the remaining engine mass [59].

For impact on steel containment shells, additional empirical formulas based on solid missile tests on steel plates are available for prediction of perforation potential [60]. In this case, the residual crushability of the remaining engine mass is not considered.

Reference [54] gives a set of empirical formulas, with their applicability domain, which cover:

- Missile penetration depth;
- Wall thickness required to prevent scabbing of concrete;
- Wall thickness required to prevent perforation of concrete;
- Residual (exit) velocity of missile.

These formulas provide a simplified approach to the assessment of structural integrity for local loading on nuclear plant structures. Note that these formulas are empirically derived using missile test data and they commonly give the best estimate values; the variability in the test results is not explicitly stated. For detailed discussion of these and other available formulas, the reader is referred to Ref [56].

5.4.3.2. Global response

Global structural response effects refer to the overall building behaviour in response to the applied aircraft impact loading [61]. The global response could result in major structural damage, such as collapse of large portions of the building walls, floors, and load carrying members. The airplane impact will also potentially induce vibrations throughout the building, but these vibrations are judged not to challenge the structural boundaries, which are the focus of this section.

While local damage is associated with the penetration of a missile into the wall, resulting in scabbing of concrete from the rear face and ultimately local fracture of rebar allowing perforation of the wall by the residual missile, global structural damage is, in the general case, associated with the excessive deformation of the entire structural system, assuming that local perforation does not occur [61]. In impact analysis, global structural damage of the target structure can be evaluated analytically based on (1) missile initial velocity and deformability, and (2) target inertial, structural, and dynamic characteristics. Depending on the availability of data on these characteristics and the intended level of detail of analysis, one of the following methods of evaluation can be used as described in Ref [54]:

- Force-Time History analysis method: in this method, the impact force time history is first determined based on the aircraft crushing strength information and impulse conservation principles, assuming that the target is rigid. The force time-history so obtained is then applied to a mathematical model of the structure in a time history analysis. Based on the internal forces and the associated stresses due to the computed response, the structure's capability to maintain integrity is then evaluated. (The time history analysis will also yield displacement/acceleration time histories throughout the structure that can be used to assess equipment functional capability during and after the impact).
- Missile-Target Interaction analysis method: in this method, a combined dynamic analysis model of both the missile and target is developed, and the dynamic response is determined as an initial velocity problem. The nonlinear models are typically significantly larger and more complex than those used for the Force-Time History analysis method. Accordingly, this method requires more detailed inertial and stiffness data of the missile than the above time history analysis method but can potentially provide more accurate results.

When strong interaction between local and global impact effects is expected, the simultaneous occurrence of both loadings has to be taken into account.

5.4.3.3. Vibration effects on equipment inside building

Shock damage is evaluated in the zone of influence (damage footprint) in order to determine the potential for affecting safe shutdown or other equipment selected for evaluation. While safety-related safe shutdown equipment has been seismically qualified, the frequency spectrum associated with an aircraft impact is typically higher than the spectrum associated with earthquakes [54].
All equipment within the shock damage footprint (or zone of influence) is assumed to fail at the time of impact unless such equipment has been evaluated and shown to withstand the shock loading. In most cases, the fire and/or physical damage footprint will envelope the shock damage footprint. If this is the case, only cabling and electrical equipment that is credited to operate for a specified time following the impact needs to be evaluated to determine if it is within the shock damage footprint.

For the purposes of defining the damage footprint, Ref [59] mentions susceptibility distances for different equipment types; however, the numerical values are not provided as they are deemed to be safeguards information. The shock damage distances are measured from the centre of initial impact and then along a structural pathway to the affected equipment (i.e., shock is transmitted through walls, floors and ceilings but not across open air space). If other adjacent buildings are seismically separated from the impacted building, this distance applies only within the building that is directly impacted.

If detailed response analysis of the structure is performed for aircraft impact [53], the evaluation of the equipment inside the structure have to be in terms of in-structure response spectra (ISRS), which define the frequency range of interest for the equipment from an engineering point of view.

Table 3-3 of Ref [59] provides fragility acceleration values for various equipment categories, depending on their level of sensitivity to shock. Each equipment category is associated with a median fragility value (probability of failure of the equipment equal to 50% with a 50% level of confidence).

Based on these median values, it is possible to estimate the corresponding HCLPF capacity values for each category, using as a first approximation the uncertainty parameters ß given in Ref [62]. Based on the HCLPF capacity, it is possible to assess the consequences of the crash in terms of equipment functionality, by comparing the calculated in-structure response spectra with the corresponding HCLPF capacities, for a given equipment category.

5.4.3.4. Jet fuel fire

Section 2.3 of Ref [54] discusses the fire sources, different fire events such as fire ball and pool fire, and the methods for evaluating the potential fire effects.

Due to the size and design of containment structures, a large fire could be anticipated outside the containment even if the containment is not breached by the impact. Such a fire might affect offsite power supplies, diesel generators, etc. In evaluating containment damage events, consideration may be given to the effects of such a large fire outside containment. In addition, the impact of an aircraft on the containment is likely to lead to significant debris being dispersed below the area of impact. As such, adjacent buildings, penetrations, and commodities being routed through penetrations have to be evaluated for damage due to falling debris and concomitant effects such as jet fuel fires. Falling debris could be large, such as portions of the fuselage or wings of the aircraft, aircraft engines, or landing gear. SSCs housed in damaged adjacent buildings need to be evaluated for the effects of falling debris and jet fuel fires.

After assessing general damage, the following scenario is to be evaluated. It is assumed that external fires caused by aircraft impacts are of relatively short duration and will not have a significant impact on systems necessary to provide cooling of fuel in the reactor vessel or spent fuel pool. This assumption is based on the following factors: (1) there is an abundance of oxygen available to support combustion of the fuel and (2) firefighter access to the fire is typically good. The in-plant evaluation needs to assess the potential for jet fuel to penetrate underground conduits that contain piping, cables, and other commodities. If no flow path exists, then the potential for failure of commodities inside the conduits may be screened out. If a flow path exists, the potential for fire and its effects on SSC items needs to be evaluated.

If the aircraft perforates the structure, an internal fire will result, both from burning jet fuel and the ignition of secondary combustibles. The fire damage caused by an aircraft impact can extend well beyond the physically damaged area due to the overpressure effects from the initial fireball and the spread of fuel through open pathways within the structure. Upon impact, an internal fireball occurs due to the combustion of dispersed jet fuel spray, mist and droplets. This fireball can cause an overpressure that is capable of failing doors, windows, and blow-out panels, especially in the impact zone, that are not rated for at least 35 kPa. The overpressure will be transported throughout the building through larger openings (hatches, grating, etc.) and through stairwells. The expected mode of failure for typical metal fire doors is buckling of the door. Doors that fail due to overpressure are no longer capable of closing. As the fireball grows through openings and failed doors, additional doors and compartments could be threatened. Ventilation ductwork in the physical damage footprint is expected to be severely crushed and torn. As a result, ventilation ductwork that passes through the physical damage perimeter is assumed to also provide a pathway for the fireball, smoke and combustion gases to enter adjacent compartments. Reference [59] has a two-step process for identifying the potential new compartment connections due to overpressure and for spread of fire damage through connected compartments

Much of the fuel will be consumed in the initial deflagration and most of the remaining fuel will coat internal structures and equipment. The quantity of liquid available to pool and flow to other areas is limited but can easily pass through relatively large openings such as grates and blown doors. While it is possible for fuel to pass through small openings, only openings that have a linear perimeter exceeding 30 cm need to be considered in this analysis [59]. The assumption is that a ventilation controlled internal fire will burn for several hours, thus preventing operations personnel from being able to take manual actions in these areas. All SSCs are assumed lost immediately in the physical

damage footprint. All cabling and electrical equipment in compartments affected by fire spread beyond the physical damage footprint are considered to be available for five minutes [59]. It has to be noted that during a long-duration fire, building structural capacity might be affected and partial or global collapse caused by structural degradation becomes possible [54].

5.4.4. Plant-level capacity

In summary, the major steps for plant-level capacity assessment for aircraft crash are:

(1) Review the aircraft to be considered by type, size, angle of attack and amount of jet fuel.

(2) Choose the reference parameter for fragility or margin evaluation, e.g. speed at impact.

(3) Define impact events to conservatively envelope all impact possibilities. Screen those events using the concept of 'zone of influence' and select the most unfavourable event for further study. Adapt the list of safety significant components (Section 3) to each selected event, if necessary.

(4) For each selected location of impact, refine the definition of the zone of influence used for screening (i.e., impact zone, debris zone and fire and smoke zone). Identify the SSCs that are within this zone of influence. Depending on the structure impacted, there may or may not be any damage or breach (e.g. containment may withstand the impact from aircraft including engine without damage whereas the auxiliary building may be breached). Therefore, some SSCs may be affected by the impact of aircraft while others may be affected by secondary missiles and/or heat generated by jet fuel fire.

The empirical formulas for local behaviour and the global response procedures discussed above are used to determine if the structure is damaged or not for this aircraft impact [54].

For the amount of jet fuel available at impact, the fire and smoke zone is determined. The zone is also dependent on the resistance of the structure impacted. Depending on aircraft type, mass at impact (including fuel), and other parameters, there is a strong correlation between the amount of jet fuel flowing and ignited, and the impact loadings. The joint probability distributions for impact and heat loading conditions are difficult to derive. Instead, we define probabilities of failure for impact and heat as independent variables, but in fact the jet fuel fire and the size of the impact are coupled. Hence, the governing failure mode is defined to be either (i) impact or (ii) fire, whichever is more critical. A conservative approximation is to assume that all equipment including piping and cabling within the zone of influence are lost.

(5) Calculate the median (best estimate) speed of aircraft for breach, or instability (i.e., overturning or sliding) of the building; estimate the uncertainty β_c in this speed.

(6) Calculate the median and uncertainty β_c for other SSCs due to secondary missiles and heat loading.

(7) When using the semi-probabilistic approach, go back to the system analysis (Section 3) and develop the final accident sequences; with the fragilities of SSCs appearing in these sequences, calculate the plant level fragility. Calculate aircraft speed for which probability of failure is 1%.

(8) When using the deterministic approach, use the HCLPF capacities of SSCs on the success paths to safely withstand the impact of aircraft, secondary missiles and heat loading. The lowest capacity SSC on the success path determines the margin of the path. This procedure could be repeated for selected impact locations and the plant margin against aircraft impact is the lowest of margins so calculated.

5.5. EXPLOSIONS AND HAZARDOUS RELEASES

Release of hazardous substances could be a significant hazard for sites located in the proximity of other industrial facilities or near important ground transportation routes. The hazard comes from the release of explosive or toxic substances. Explosions of transported goods or released gas clouds could damage plant components. Toxic releases could harm plant operators in the control room.

This hazard might be unnoticed, since comprehensive statistics of hazardous material transportation are sometimes unreliable or non-existent, especially for road traffic. However, the general margin assessment framework of Section 4 is still valid. The following sections delineate the application of this general framework. More detailed guidance can be found in Ref [18]. Only the deterministic approach is considered for this particular hazard.

5.5.1. Reference strength for the hazard

For hazard originating in transportation routes, hazard depends on the hazardous material traffic and the type of transportation means (e.g. small liquefied natural gas truck, 25 ton rail wagon, etc.). When no reliable statistics are available, a deterministic approach could be followed for the selection of the reference strength of the hazard, by considering an accident of the most unfavourable transportation means allowed to circulate on the nearby routes. In addition, when there are several possible locations for accidental explosions or releases, and the locations with the most severe effects cannot be clearly identified beforehand, all the potential most severe locations have to be considered in the analyses.

In case of nearby industrial facilities, the amounts of stored hazardous materials have to be provided by the competent authorities. A deterministic approach could also be taken for selecting the reference strength, assuming the release or the explosion of all hazardous substances stored in the facility.

5.5.2. Analysis of consequences in the site

In this step the consequences of the reference strength events identified in the previous step are to be determined.

In general, the effects of explosion of importance to structural response are:

- Incident and reflected pressure (mainly from detonation);
- Time dependent overpressure and drag pressure;
- Blast generated missiles;
- Blast induced ground motion (mainly from detonation);
- Heat or fire.

An explosion near the plant would create a pressure wave that impinges on the structures or yard equipment. The pressure pulse that reaches a particular surface depends on parameters such as the distance to the explosion and the orientation of the surface. Typical pressure time histories are shown in Ref 54. Before the capacity of the SCCs can be assessed, the effects (pressure) of the explosion at the exposed surfaces have to be determined. This is done following the procedures described in Ref [56]. Typically, the peak overpressure, either side-on or reflected overpressure, is used as the reference parameter to define the effects on a particular location. At shorter distances from the explosion source, blast generated missiles, heat or fire may need to be also considered [54].

For the evaluation of fire impacts exterior to the plant structures, typically fires are modelled as pools which are situated adjacent to plant structures unless it can be demonstrated that the fire location is elsewhere. A crash of a rail or road tanker carrying a flammable liquid is an example of an exterior plant fire event. For the fire scenario, it is typically assumed that the entire load is spilled instantaneously on the ground, resulting in a pool fire. The occurrence of a simultaneous fireball, however, is not feasible. A methodology which has been developed to calculate the average diameter for an instantaneous spill is described in Ref [54]. The primary mechanism for damage from such fires

is thermal radiation. Depending on the circumstances and conditions leading to such an event, different types of open fires may result. For example, ignited releases can produce pool fires, jet flames, vapour cloud fires, or fireballs, all of which behave differently and exhibit markedly different radiation characteristics.
For toxic chemical releases, atmospheric diffusion and dispersion up to the control room air intakes needs to be assessed and the toxicity of the control room atmosphere has to be determined as a function of time for each reference strength event. The possibility of automatic isolation of control room atmosphere, triggered by chemical detectors installed at the air intake, is an important factor to consider when assessing the consequences of the reference strength release.

5.5.3. Capacity of structures, systems and components

For explosions, the type and extent of damage (local damage, excessive deformation, functional failure due to vibration) to the selected safety relevant components when subjected to the reference events is to be investigated. As for aircraft impact loading, the structure failure modes to be examined are those modes that affect the required performance of the structure: overall instability, loss of structural integrity (e.g. missile perforation, partial structure collapse), loss of leak tightness, loss of support for SSCs or functional failure due to induced vibration.

Capacity evaluation is generally limited to building structures housing the safety relevant equipment and exposed large equipment such as yard tanks and substation structures. As in the case of aircraft impact, for each failure mode, the median capacity and the uncertainty in the capacity can be estimated using the procedures of response analysis described in Ref [54]. Fragility is usually defined as a function of peak free field side-on overpressure P. The mean fragility, defined by the median P_m and the composite uncertainty β_c is normally used. The median capacity is calculated with the best estimates for the different parameters that are used to describe the loading and to perform capacity evaluations.

Regarding the computation of HCLPF capacity values, the same comments made in Section 5.4.3 regarding severe nonlinear events apply. A judicious combination of conservative values of parameters is to be used to obtain a HCLPF capacity, based on the philosophy given in Table 3.

Note that, after explosion capacity assessments, a revision of the success paths used for the selection of SSCs (Section 3) may be necessary in order to increase the overall plant capacity.

In the case of toxic releases, the exceedance of the toxicity limits at the control room means that the operator will not be able to take necessary actions any more, unless procedures are in place for the use of special protection outfit (masks, dress, etc.).

5.5.4. Plant-level capacity

In summary, the major steps for plant-level capacity assessment for explosion hazards are:

(1) Describe the characteristics of the reference explosion;

(2) Calculate the overpressure at different structures within the NPP;

(3) Assess if each structure can safely withstand the overpressure (compare with HCLPF capacity);

(4) If a fire is postulated, determine the capability of exposed structures against the heat load;

(5) Structural collapse is assumed to result in failure of all equipment, piping and cabling within the structure. Partial collapse of structures have to be addressed for its impact on equipment, piping and distribution systems housed or supported therein;

(6) From the success paths developed for the NPP, assess if a success path could be achieved without the SSCs conceded to have failed because of explosion effects;

(7) If Step 6 is successful, the NPP has enough capacity against the specified explosion hazard;

(8) Estimate the parameters of the explosion that would result in not achieving the success path. This is the plant-level capacity in terms of explosive parameters.

This procedure could be repeated for different hazard originating locations and the plant margin against explosives is the lowest of margins so calculated.

In the case of a toxic chemicals release, the major steps for safety margin assessment are:

(1) Describe the characteristics of the reference release;

(2) Calculate the time history of chemical concentration at the air intake of the control room under the most unfavourable atmospheric conditions (i.e., wind conditions, stability category, etc.);

(3) As a function of control room habitability systems and leak-tightness, obtain the time history of chemical concentration in the control room atmosphere;

(4) Determine the times at which the toxicity limits that would disable the operators will be reached and check adequacy of procedures for the use of protective clothing or breathing aids;

(5) If Step 4 is successful (i.e., toxicity limits are not reached or procedures are adequate) the NPP has enough capacity against the specified release hazard;

(6) Estimate the parameters of the release (e.g. released mass) that would result in not reaching the toxicity limits or in procedures being adequate. This is the plant-level capacity in terms of the chemical release.

The sequence could be repeated for different hazard originating releases and the plant margin against these releases is the lowest of plant-level capacity so calculated.

6. ASSESSMENT OF PERFORMANCE OF FUNDAMENTAL SAFETY FUNCTIONS

6.1. GENERAL

For each of the selected hazards, the exceedance of the plant-level capacity will result in damage to components required for the performance of the fundamental safety functions (Section 3.1), starting with the more vulnerable SSCs identified during the assessment described in the previous sections.

Thus, at the next step of the vulnerability assessment, the prime objective is to evaluate the robustness of the plant in terms of design features and procedures against progression of the accident scenarios started from failure of the more vulnerable SSCs. The goal now is to identify the expected plant response after the plant-level capacity is exceeded, from which specific actions to improve safety could be devised.

6.2. CONNECTION WITH THE CAPACITY ASSESSMENT

Since the more vulnerable SSCs are different from one hazard to the other, each of the applicable hazards has the potential to produce a different accident scenario. The scenarios of interest here are those which are initiated by the failure of the more vulnerable SSCs, in addition to the induced initial plant conditions considered in the selection of the components (Section 3).

Hence, the analyst needs to revisit the systems models used to select the SSCs (Section 3), assume that the weak SSCs fail, and follow the sequence of events that will lead to the loss of the fundamental safety functions, as defined in Ref [41]:

(1) Control of reactivity;

(2) Removal of heat from the reactor and from the fuel store;

(3) Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

In this activity, in contrast to the work for selection of components (Section 3), the analyst needs to take into account the likely conditions after the extreme event occurrence. For instance, conditions such as partial site devastation, overstressed operators, or severe environmental conditions (smoke, fire, etc.), are to be taken into account.

As a result, for each applicable hazard, an accident scenario and the progression in time of the scenario will be obtained.

For example, let us consider that ‘flood due to meteorological causes’ has been identified to be an applicable hazard for a particular site with a PWR. Following, for instance, the success path approach in Section 3, the analyst considers the ‘loss of off-site power’ as the initiating event for selecting the safety significant components. Let us assume further that the safety margin assessment (Sections 4 and 5) has shown that once the flood level reaches elevation 50 m, the essential service water pumps will fail (more vulnerable SSC). Then, the analyst goes back to his systems modelling and checks if there is another possibility for cooling the component cooling heat exchangers. He/She might find out that with external means (e.g. portable diesel pumps and water sources) it would be possible to provide the necessary cooling for some time. After that time, no cooling will be possible under the assumed site conditions (e.g. roads cut off and heliport flooded). Hence, the analyst will assume failure of the component cooling system. This will lead, for example, to the failure of the residual heat removal system and to the failure of the spent fuel pool cooling system. At this point, for the assumed site conditions, the analyst will check for alternative means for residual heat removal both from the reactor and the spent fuel pool; and for the time available up to the failure of the alternative means. This process will continue until reaching fuel damage. As a result, the series of failures up to fuel damage and the time frame will be identified.
The intended assessment process is illustrated in Figure 11, for a fictitious PWR under a flood scenario in which the plant flood capacity is exceeded. The flood most vulnerable SSCs identified

during the flood capacity assessment are the essential service water pumps. Hence, the starting point is the loss of this pumps at $t = 0$. After this loss, a series of sequential losses at particular times takes place, eventually leading to fuel damage. Note that the actual site conditions and equipment availability are considered in the assessment.

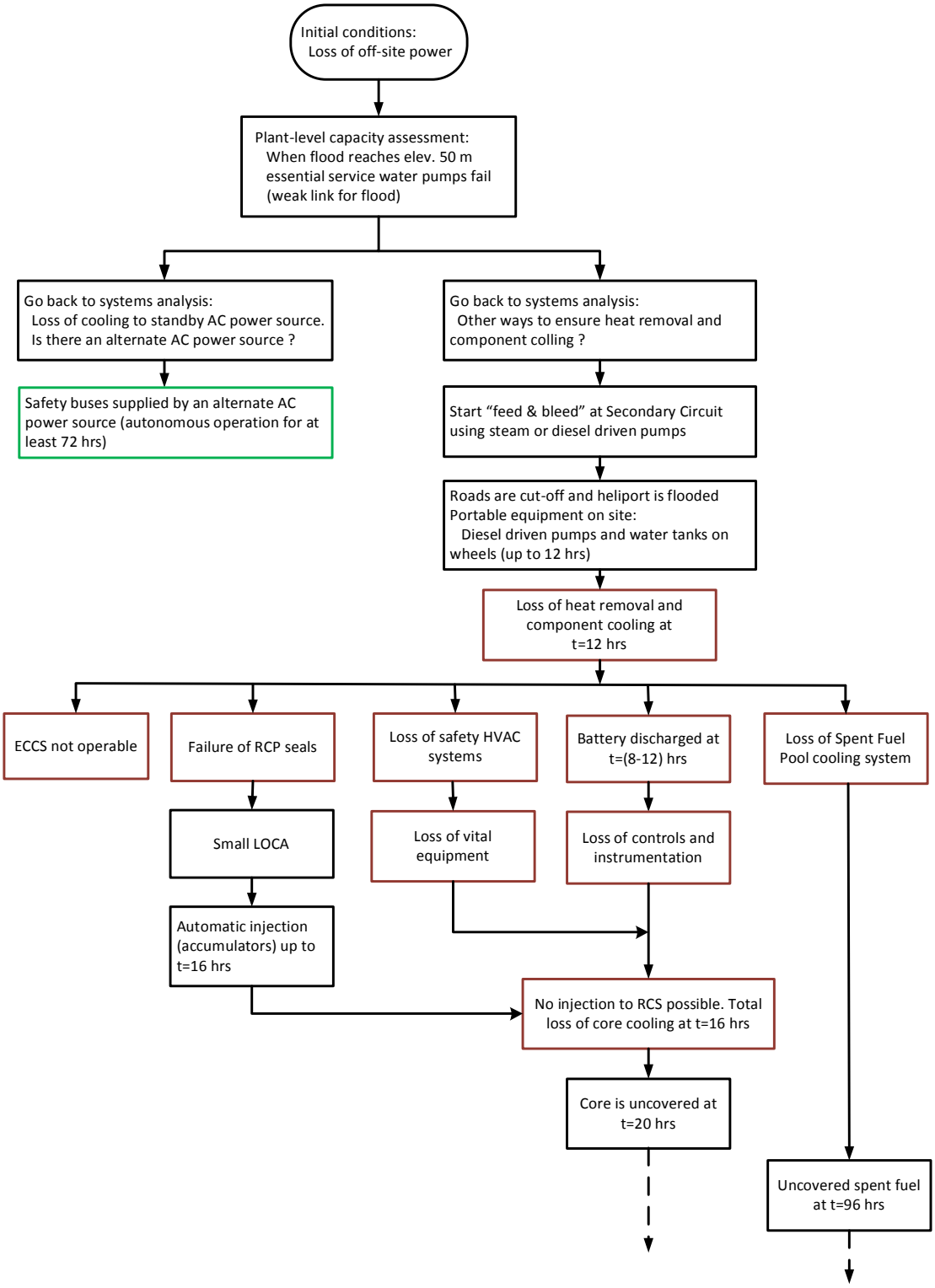


FIG. 11. Simplified flowchart showing an assessment of safety functions for a PWR after exceeding the plant's flood level capacity (for illustration purposes only)

It is to be noted that, for many plant designs, the ultimate heat sink and the normal and emergency power supplies are the part of the installation most exposed to external hazards. Hence, in some cases,

for the purpose of assessing the plant response after exceedance of the plant capacity, it could be sufficient to analyse two enveloping scenarios, such as a station black-out[7] (SBO) and a loss of ultimate heat sink. This needs to be confirmed taking into account plant specificities in each case. From those two scenarios, the SBO event is normally the most limiting case owing to the small time available to prevent fuel damage.

6.3. SCOPE OF THE ASSESSMENT

The scope is the examination of scenarios potentially leading to fuel damage and radioactive releases, once the plant-level capacity against the applicable hazards is exceeded.

Ideally, the exercise will provide information about the time frame between the exceedance of the plant-level capacity and the potential radioactive releases. Additionally, in this process, possible measures to mitigate or to delay the consequences could be identified.

In performing the assessment, important considerations are:

- Site conditions when plant capacity against applicable hazards is exceeded: unavailability of access routes, partial site devastation, overstressed operators, smothering, etc.
- Equipment actually present on site and available for use under plant procedures, including equipment not necessarily taken into account when preparing the Selected SSC List (Section 3).
- Potential interaction between plant units at multi-unit sites and potential simultaneous failure of containments. Guidance can be found in Ref [51].

6.4. ASSESSMENT PROCEDURE

6.4.1. General

For each applicable external hazard, the assessment consists in determining the plant response following the failure of the most vulnerable SSCs identified in the plant capacity assessment described in Sections 4 and 5.

The assessment is deterministic. The more vulnerable components are assumed to fail and, afterwards, a sequential and progressive loss of the remaining systems is postulated, once their operation is no longer possible according to the 'as-is' condition of the plant (e.g. batteries depleted, tanks emptied, reservoirs depleted, etc.). The time frame (time milestones) of the resulting sequence of events is a key result of the exercise.

The assessment is to consider the same operational modes taken into account for the selection of the safety significant components (Section 3): plant power, fuel condition, system alignments and availability according to the plant technical specifications, etc. In this regard, when a plant is composed from several units, the postulated conditions would affect all units and facilities simultaneously, and that degraded conditions could exist for the implementation of alternative power supply or cooling methods, particularly those that entail measures that have not been foreseen in the plant design.

The assessment is to reflect the provisions already included in the plant design basis. In addition, the assessment is to reflect the strengths of the design in terms of redundancy, diversity, physical

[7] As defined in IAEA Safety Standard No SSG-34 Design of Electrical Power Systems for Nuclear Power Plant [63], SBO is a plant condition with complete loss of all AC power from off-site sources, from the main generator and from standby AC power sources important for safety, to the essential and nonessential switchgear buses. DC power supplies and uninterruptible AC power supplies may be available as long as batteries can supply the loads. Alternate AC power supplies are available.

separation and other features relevant to cope with stepwise losses of supply sources and functionality. In this regard it is relevant to determine the limiting situations that could arise for accomplishing the safety functions when supplies fail (cliff edge effects) and the measures that are already in place or could be implemented to avoid reaching these situations and improve the defence in depth provisions.

As already mentioned, the analysis starts from the failure of SSCs with lowest capacity originated by the extreme events, as resulted from the previous plant capacity assessment (Sections 4 and 5). The analysis of consequences of these failures can be facilitated by a number of methods and tools, such as:

- Plant off-site and off-site electrical diagrams;
- List of electrical bus bar loads;
- Plant configuration or dependency matrixes;
- Failure mode and effect analysis (FMEA);
- PSA analysis models and risk monitors;
- Plant simulators;
- Plant Safety Analysis Report.

Priority has to be given to the extent possible to tools and documentation that are part of a management system programme (quality assurance). The analysis needs also to identify additional measures, such as the use of portable equipment, alternative water supplies, etc. with consideration of possibilities for sharing equipment and supplies between different units at the same site and the safety implications for both.

The analysis needs to be accompanied also by the necessary information about the plant and its systems that are necessary for a good understanding of the assessment.

The assessment of the plant design and organizational provisions to cope with the extreme events is to conclude on their adequacy and completeness. Recommendations are to be provided for improvements in areas where the weak links are identified and where additional measures to increase robustness could be incorporated.

Important aspects are the independence of mitigation equipment from other interacting SSCs (e.g. buildings, structural supports, cooling water for pumps and diesel generators, instrument air, ventilation, etc.); potential improvements related with the functional independence and separation of the plant equipment; and the provision of alternate heat sinks independent from the main Alternate Current (AC) power supply.

The assessment needs also to conclude whether the challenges to the equipment and personnel resulting from extreme external hazards are adequately addressed, including a list of items where those may be improved, as well as topical areas where the technical basis used for specific analysis could be improved.

Recommendations are to be provided wherever applicable to give the plant clear indication what are the weaknesses that still need to be addressed and what additional measures to increase robustness could be incorporated.

6.4.2. Example: Loss of AC power supplies

This section has been reproduced with some modifications from IAEA TECDOC 1770, [64].

The plant essential switchgear buses which feed safety loads are normally supplied from the preferred power supply; any disturbance in the grid, off-site as well as on site AC power sources may have consequences on the availability of power supply. The plant electrical systems normally involve the following AC power sources:

- Off-site power supplies;
- On-site power supply (main generator, house load operation capability);
- Standby AC power supplies, providing power in any operational state when power supply to the essential switch gear bus is lost, or in the case of LOOP event, as defined in Ref [63];
- Alternate AC power supply or in case of SBO, as defined in Ref [63]; and
- Any other AC power supply (e.g. mobile) that can be deployed and connected to the AC switchgear buses (e.g. as part of the accident management measures).

The sequential loss of these AC power supplies may result from extreme external hazards. Particularly, the grid is commonly part of the preferred power supply for the NPP and the safety power systems. During normal at-power operation, the AC power supply to the plant is normally provided from the main generator, which will dampen variations arising from the grid. The grid provides stable off-site AC power, that is, it needs to be capable of withstanding load variations and anticipated operational occurrences (AOO) on the transmission system without exceeding the specified voltage limits and frequency limits. However, the vast majority of the extreme external events within the scope of the present publication will likely cause the unavailability of the grid and the main generator for a long period of time, even in cases where redundancy and diversity are present in the off-site AC power supply sources.

Plant capabilities for operating in an 'house load mode', that is, automatic disconnection of the plant generator from the grid and rapid reduction in reactor output to supply power for the plant's own consumption, can sometimes be considered in the short term, where this is an established feature of the design and where it can be demonstrated that the extreme event would not affect this capability.

The example in this section corresponds to an external hazard (e.g. flooding) whose most vulnerable SSCs are the on-site emergency power generators. A 'loss of off-site power' induced initial condition has been assumed for compiling the Selected SSCs (Section 3) and, during the plant capacity assessment (Section 4), it has been determined that the stand-by AC power sources (e.g. emergency diesel generators) are the most vulnerable SSCs against this hazard. Hence, the starting point for the assessment of the performance of fundamental safety functions against the hazard is the loss of both the off-site power and the emergency diesel generators.

In this case, the loss of off-site power propagates to an SBO event. SBO is defined in Ref [63] as a plant condition with complete loss of all AC power from off-site sources, from the main generator and from standby AC power sources important to safety to the essential and nonessential switchgear buses. Direct Current (DC) power supplies and uninterruptible AC power supplies may be available as long as batteries can supply the loads. Alternate AC power supplies are available. The SBO is characterized for each plant design by SBO coping time, i.e., time available from loss of all AC power to the safety buses until onset of core damage if no counter measures. The coping time varies per plant design and is in the range of 40 minutes to 9 hours[8].

Normally, countermeasures are in place to be implemented within the coping time in order to prevent the core damage. However, the possibility of restoration of AC power strongly depends on the conditions of the plant and its surroundings created by the extreme event. Typically, the longer the coping time, the higher is the probability that the AC power will be restored within coping capacity.

As a design provision for SBO, the plants normally have options to feed buses from alternate AC power source(s), [41]. The alternate AC power source(s) is typically started and aligned to the

[8] Credit can be taken for equipment which operates automatically without need of AC power, e.g. turbine driven emergency feed water pumps, turbine driven generators for cooling reactor coolant pump seals, as well as diesel driven feed water pumps that start automatically following SBO.

respective AC bus manually and provide power to DC or instrumentation buses, or to a limited amount of vital equipment.

The alternate AC power source capacity is limited and cannot supply large loads (e.g. cooling systems for turbine condenser, or residual heat removal from suppression pool of boiling water reactors). In view of the limited capacity of the alternate power source, it is considered a temporary solution until the AC power supply is recovered from either off-site or standby AC power sources.

The alternate AC power source is typically capable of supplying its loads for several days and therefore there is generally low risk with respect to its mission time during a short duration SBO event. The access routes, pre-designed connection points, procedures for the deployment, connection, loading, training of designated personnel, maintenance, surveillance and testing requirements need to be well defined and in place. Conditions after an extreme external event affecting the site are to be considered in the design of alternate AC power source.

The alternate AC power supply may also be ensured by a number of redundant and diverse systems; furthermore, at some plants, there is a second level defence ensured by either stationary power systems or portable power means that are qualified to withstand extreme external hazards.

As a result of these considerations, after a SBO event, typically three possibilities exist:

- SBO event which can be recovered within the coping time (i.e. preferred power source or standby AC power source is recovered);
- Extended SBO events where an alternate AC power source is connected within the coping time but it is required to continuously operate for a long period of time;
- SBO event that cannot be recovered and that eventually leads to fuel damage.

In the present example, the first possibility has to be ruled out, since both the preferred power source and the standby AC power source (diesel generators) are assumed to be failed.

In the second possibility, the key parameter is the time at which the alternate AC power source will cease operation (e.g. by running out of fuel). After this time, the SBO will become unrecoverable and fall into the third possibility.

The analysis of the third possibility will lead to the assessment of the accident sequence up to reaching core damage, which is the purpose of the present exercise.

Typically, the following aspects will need to be reviewed in detail in order to define the time sequence of events leading to fuel damage after the SBO event:

- Availability of equipment in the short and long term, including:
  - Core cooling equipment not requiring AC power, e.g. turbine driven pumps. Consideration needs to be given to steam, instrument air, DC power, room ventilation that they might need.
  - Batteries depletion time and measures to prolong it, e.g. disconnecting some loads, using portable chargers, etc.
  - Degradation of barriers, e.g. development of main coolant pump seal LOCA.
- Assessment of the consequences of loss of batteries and subsequent failure of DC power supply and instrumentation, including the identification of instrumentation that can provide local measures without power supply, e.g. some types of pressure and level meters.
- Assessment of the time available until the onset of core/fuel damage if remediation measures are not taken. Assessment of measures foreseen to prevent it, including:

- Equipment already available on site, e.g. from other units and off site, that could be brought or connected to the plant.
- Assessment of the time required for such measures and availability of competent staff to perform them.
- Assessment of the automatic actions, protective measures, interlocks, or other features in the electrical systems, reactor protection system, load sequencer or other systems, that could prevent the connection of foreign equipment or cause unexpected events.
- Assessment of the equipment mission time including consumables necessary to operate the equipment itself, but also sufficient capacity of water in emergency feedwater tank or condensate storage tank. The necessary equipment mission time until replenishment of supplies is to be assessed using site-specific information, which takes into account the possibilities for the authorities to clear blocked roads and other transportation ways, and the arrangements made by the plant operator to ensure the supplies.

– Identification of the limiting situations that could arise and additional measures (design modifications, procedures, etc.) that could be taken to enhance the robustness of the defence in depth.
– Contingency measures already in place for energizing certain predefined loads using temporary provisional cable connection from available resources or mobile battery chargers to keep at least one station battery charged and to maintain the minimum set of critical instrumentation and control equipment.

The environmental conditions for which the alternate equipment is qualified are relevant for the assessment. Capability to withstand the applicable extreme events has to be confirmed.

The assessment needs to also check compliance with additional recommendations provided in Ref [63] regarding measures for SBO events, such as sharing power supplies with other units, and measures to extend the duration of DC power supply.

6.4.3. Example: Loss of ultimate heat sink

As per definition in Ref [65], the ultimate heat sink is normally a body of water, the groundwater or the atmosphere, to which some part of or all residual heat is transferred in normal operation, anticipated operational occurrences or accident conditions. The heat sink considered here is not the one used to evacuate heat from the turbine condenser during normal operation, unless it is also the same used for residual heat removal.

Depending on the site characteristics, a design may include more than one ultimate heat sink. Also at sites with several units, it could be possible that several units share an ultimate heat sink, and even heat transport systems to them, in which case potential interaction between units need to be considered.

The example in this section corresponds to an external hazard whose most vulnerable SSC is the essential service water pump house (i.e. a whole building). A ‘loss of off-site power’ induced initial condition has been assumed for compiling the SSCs for assessment (Section 3) and, during the plant capacity assessment (Section 4), it has been determined that the pump house will be the most vulnerable SSC against this hazard. Hence, the starting point for the assessment of the performance of fundamental safety functions against the hazard is the loss of both the off-site power and the loss of the essential service water pump house, including the essential service water pumps.
The assessment here refers to the ultimate heat sink itself and not to the intermediary heat transport systems to remove heat from the core. Note that the heat sink includes not only the body of water or

the atmosphere, but the structures (pools, water intake, etc.) associated with them. Therefore, a failure of the heat sink includes the excessive accumulation of mud, dirt, etc. in the water, the plugging or failure of intake structures, etc., particularly during extreme event conditions. It can no longer be claimed that the ultimate heat sink cannot fail on the basis that the atmosphere or the sea will always be available.

As with the loss of power supplies in the previous example, if several heat sinks are available in the design, the assessment have to consider the stepwise failure of the heat sinks, and that they will remain unavailable for a long period of time. Realistic considerations can be made for supplying the plant with back-up water inventories, e.g. fire trucks, after a certain period of time.

The assessment needs to consider the alternative water sources existing in the design that could be available for ensuring the fulfilment of the safety functions, the provisions to protect them and to align them to the heat removal systems.

The assessment needs to determine the time available from the loss of the ultimate heat sink(s) until the onset of core/fuel damage without the use of external resources. It has to provide information on the provisions in the design and necessary actions and time needed to use alternative resources to restore heat removal using alternative heat sinks. In doing this assessment, account needs to be taken of the potential severe conditions on the site after an extreme event; the availability of equipment on site or brought to the site to connect and pump water into the systems; the necessary time to bring alternative heat sinks into operation; and the availability of qualified personnel to do it, considering also that all units on the site have been affected by the extreme event.

As a result of the assessment, potential weaknesses in the defence in depth are to be identified, as well as additional measures that have to be incorporated to eliminate them or increase the robustness of the plant.

6.4.4. Example: Combined loss of ultimate heat sink and station black-out

The example in this section corresponds to an external hazard whose most vulnerable SSC is the primary ultimate heat sink structure, which leads to immediate loss of the on-site emergency power generators, due to loss of cooling. A ‘loss of off-site power’ induced initial condition has been assumed for selecting the SSCs (Section 3) and, during the plant capacity assessment (Section 4), it has been determined that the structure housing the primary ultimate heat sink (e.g. essential service water pond) is the most vulnerable SSC. Hence, the starting point for the assessment of the performance of fundamental safety functions against the hazard is the loss of the off-site power, the loss of the ultimate heat sink, and the on-site emergency power generators.

This extreme scenario have to be considered taking into account the similarities and overlapping effects of SBO and loss of ultimate heat sink for preserving the fundamental safety functions. The analysis has to determine the following:

- For how long fuel damage (both in the reactor core and spent-fuel pool (SFP)) can be prevented upon failure of the ultimate heat sink(s) and SBO conditions, without external support to restore these supplies.
- Provisions in the design and necessary internal actions to recover from this scenario, if any.
- Necessary external actions to prevent core/fuel damage accounting for the situation prevailing at the site after the extreme event; the availability of equipment on site or brought to the site; the necessary time to make equipment operable; and the availability of qualified personnel to do it, considering also that all units on the site have been affected by the extreme event.

The design provisions to cope with SBO and loss of ultimate heat sink has to be checked against environmental conditions associated with the extreme external events. In particular, the capability of equipment to remain functional needs to be assessed for the likely conditions following the extreme external events.

The equipment credited for coping with SBO and with loss of ultimate heat sink and events has to be autonomous and ensure consumables necessary to operate the equipment itself, but also sufficient capacity of water in emergency feed water tank or condensate storage tank needs to be present. The time during which the equipment will be available has to be determined by analysis, considering potential effects of the extreme external hazards.

The plant loss of ultimate heat sink coping time is typically greater comparing to SBO coping time; for some power plant designs however, SBO and loss of ultimate heat sink events may have similar or same coping times.

7. RISK ESTIMATES

7.1. GENERAL

The methodology described in the previous sections will identify the vulnerabilities against the applicable extreme external events. However, unless the results of the corresponding probabilistic hazard assessments are available, the methodology will not be able to provide an estimate about the actual risk posed by the installation.

It is expected that the easy fixes of weak links will be implemented without further considerations. But the decision about whether a major fix has to be implemented or not have to normally be supported by the comparison between the actual risk and the safety goals established at each Member State.

The most rigorous procedure available today for establishing the risk metrics is a comprehensive Probabilistic Safety Assessment (PSA) for the applicable external hazards.

However, when the results of probabilistic hazard assessments are available (hazard curves), the plant level capacity obtained for each applicable hazard could be used to obtain a point estimate for the annual frequency of safety significant damage. This practice has been used, officially or unofficially, in a number of Member States to obtain interim risk estimates.

For each hazard, the approach involves the computation of a plant-level mean fragility curve, using the high confidence plant-level capacity, and the convolution of this fragility curve with the mean hazard curve.

The following sections give an overview of the three activities that are necessary to obtain these risk estimates, namely, the hazard assessment, the computation of a plant-level fragility curve, and the convolution of hazard and fragility.

7.2. HAZARD ASSESSMENT

Typically, hazard is expressed as a relationship between the strength of the hazard and the annual frequency of exceeding this strength (annual exceedance probability, hazard curves). Hazard curves account for aleatory variability and epistemic uncertainty. In this Section, the requirements and methodologies to assess hazard are outlined based on IAEA Safety Standards and recent work within international collaborative research programs. General requirements are given in Ref [23].

It is emphasized that, when reassessing the hazard for a particular site, updated data and state-of-the-practice methods could be used.

7.2.1. Earthquake

For most existing nuclear facilities, the primary seismic hazard is the earthquake ground shaking. Shaking is caused by the seismic waves reaching the site from the seismic source. Ref [24] provides guidance on how to derive the hazard curves. For this purpose, the probabilistic seismic hazard analysis methods (PSHA) described in the safety guide need to be used.

The results of the probabilistic seismic hazard analysis include the seismic hazard curves for peak ground acceleration and for acceleration at some spectral frequencies, corresponding to different confidence levels (Fig. 12). From these curves, the so-called ‘uniform hazard response spectra’ (UHRS) are derived, which define the seismic ground shaking in the site for different annual frequencies of exceedance (Fig. 13)[9].

[9] A response spectrum defines the amplitude and frequency content of the seismic ground motion. The Peak Ground Acceleration (PGA) is normally associated to the spectral acceleration at about 50 Hz.

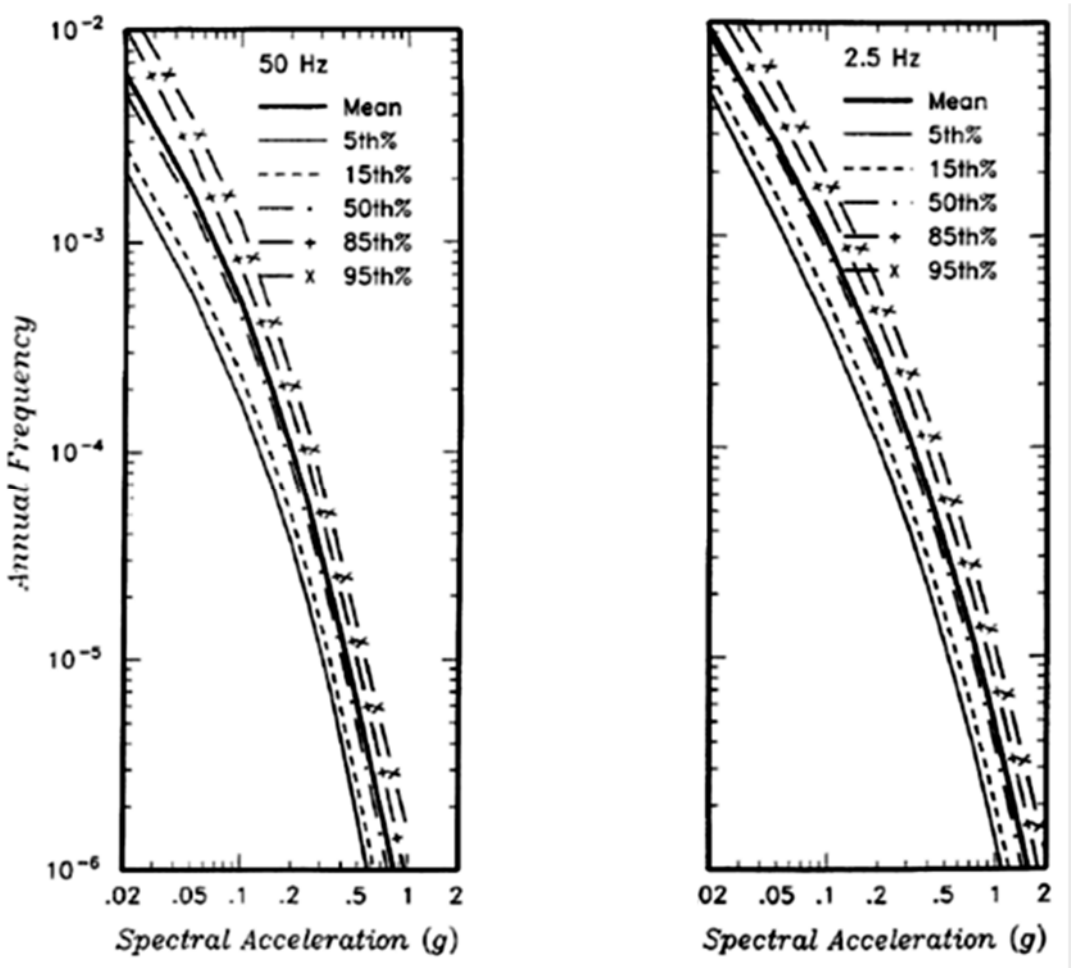


FIG. 12. Typical earthquake ground motion hazard curves for two spectral frequencies.

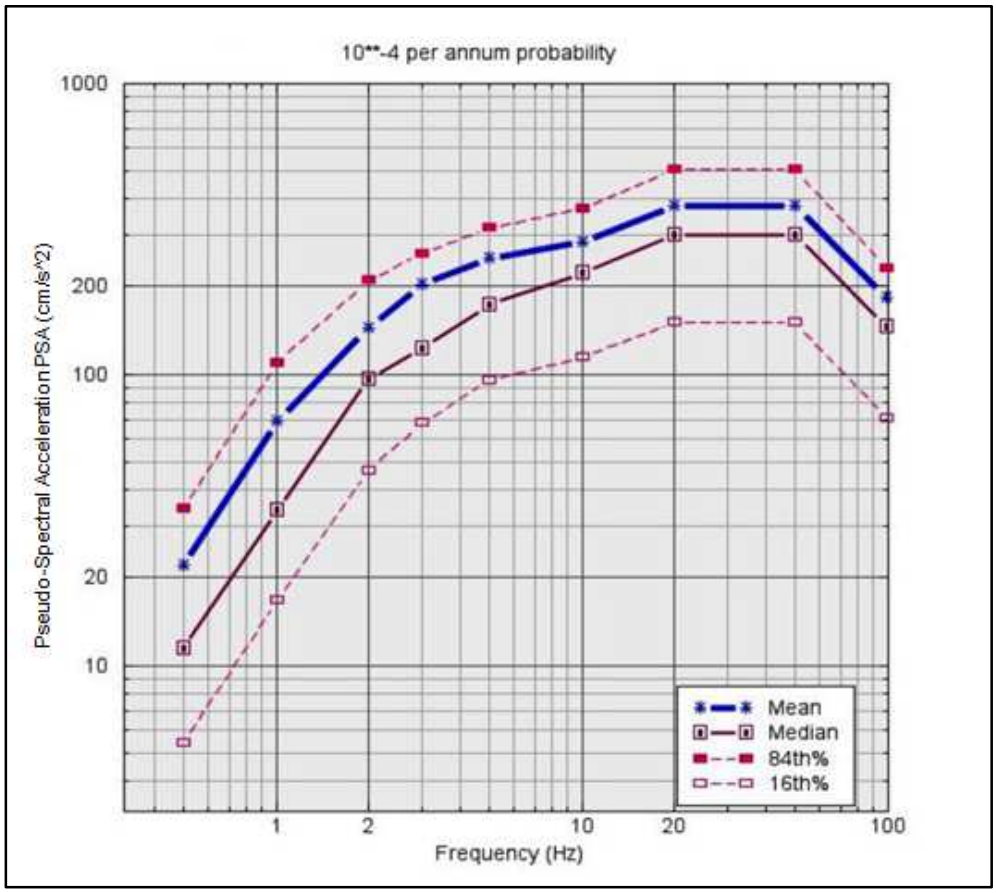


FIG. 13. Typical uniform hazard response spectra (UHRS). Spectra correspond to a hard rock site (Reproduced as courtesy of OECD NEA Ref. [66]).

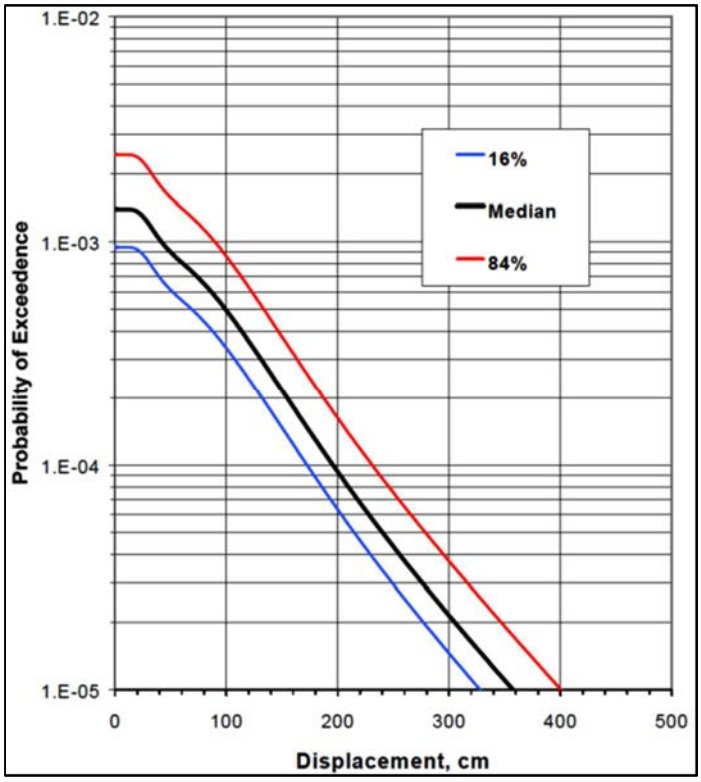


FIG. 14. Typical fault displacement hazard curves [67]

PSHA typically cover more than one site (e.g. a whole country or a whole region within a country) and typically require a substantial effort in terms of time and resources.

Ref [24] provides also guidance for the assessment of the potential for surface faulting (i.e. the fault capability) at the site. If this particular seismic hazard has not been screened out, the annual frequency of significant fault displacement (Fig. 14) can also be obtained following Ref [24] and the more detailed guidance in Ref [68]. Hazard calculations in this case follow a path analogous to PSHA methodology.

7.2.2. High winds

Ref [26] provides general guidance on assessing the high winds hazard. Ref [26] covers strong 'straight' winds, tropical cyclones (typhoons and hurricanes), and tornadoes. More detailed guidance can be found in Ref [50]. 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 or discrete family of curves) in open terrain and at a specified height (Fig. 15).

High winds associated with any meteorological event can cause debris to become wind borne missiles. Debris can be transported in any high wind event [50]. Two basic approaches have been used in windborne missile analysis. The traditional deterministic approach uses a spectrum of several missile types and maximum velocities to be considered in design or assessment. Using a wind field model and a missile trajectory model, maximum missile speeds are calculated for each missile type. These analyses use simplified 3D trajectory models and an average drag coefficient [52].

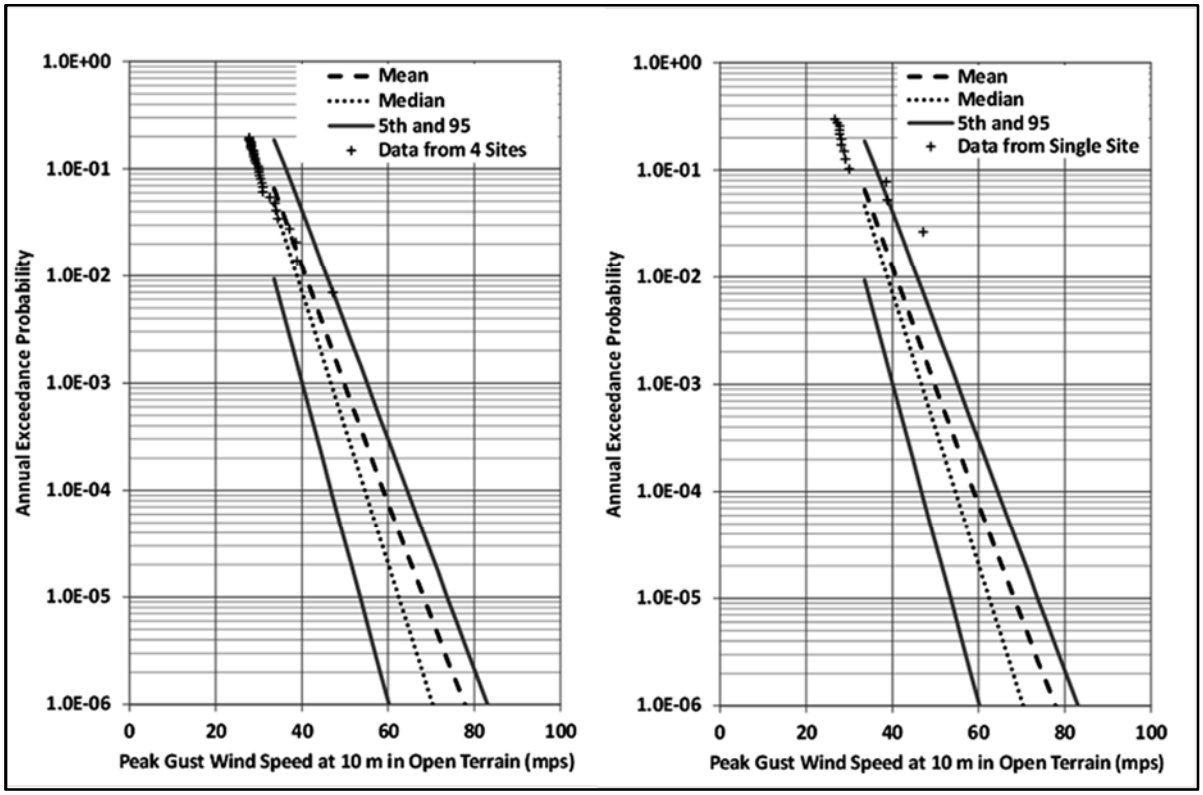


FIG. 15. Typical wind speed hazard curves (extra-tropical wind), Ref.[50].

The second approach is based on a probabilistic analysis covering a much broader class of potential missiles. This approach also requires a wind field model and a missile trajectory model. Probabilities of missile impact are estimated for each structure or component. These results can be used directly in probabilistic risk studies [50].

As an example of this technique, Fig. 16 shows a relationship between wind speed and missile velocity developed for different kinds of missiles, based on 1000 trajectory analyses for each missile, injection height, and wind speed combination [69]. The figure gives the mean value of maximum missile velocity versus the maximum tornado wind field velocity for several types of missiles and injection heights. The 90th and the 99th percentiles are shown for the 30 cm (12 inch) diameter pipe missile. As shown in the figure, for a given maximum wind speed, the maximum missile speed is strongly dependent on missile type and the injection height.

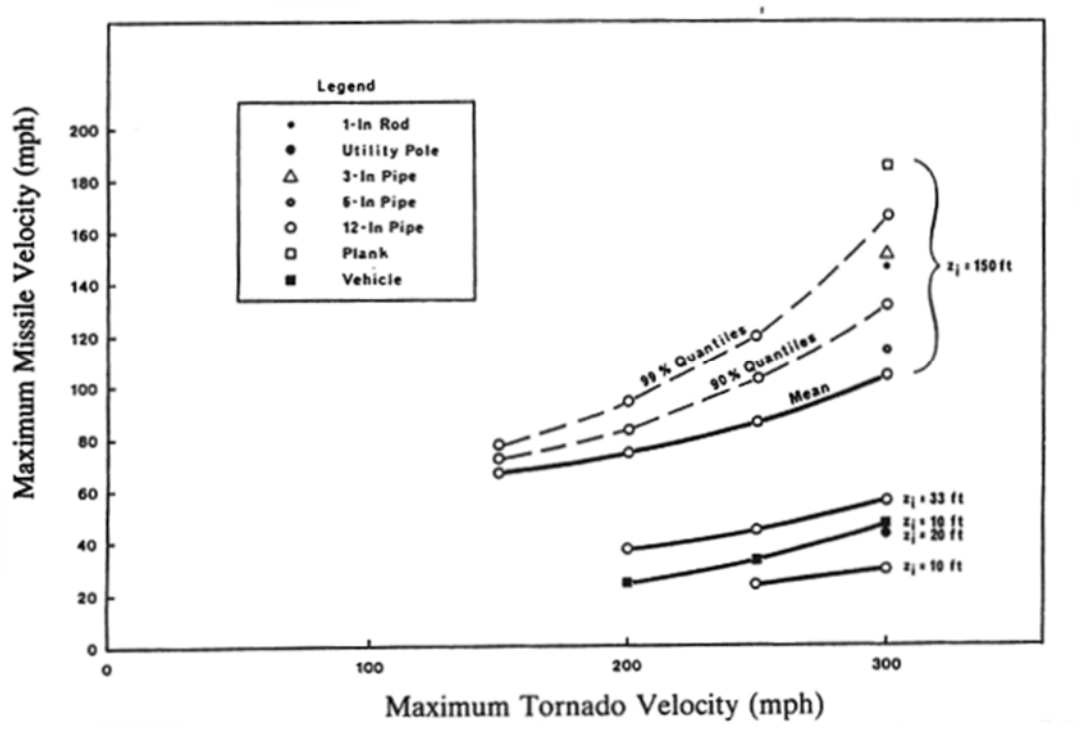


FIG. 16. Mean values of maximum missile velocities as a function of maximum wind speed. Courtesy of EPRI 1981[69]. Reproduced with permission of EPRI.

7.2.3. Flood due to meteorological and hydrological causes

The primary (not necessarily the most damaging) external flood hazard resulting from meteorological and hydrological causes is inundation of site facilities by floodwater, including potential water ingress into buildings. The inundation to the site can occur due to river flooding, storm surge and wave action, local intense precipitation or a combination of phenomena. Riverine flooding can be initiated by a combination of events, including precipitation, snowmelt, and unusually high spring temperatures. In addition, flood levels can be compounded by the effects of ice jams, debris, wind-waves, failure or mismanagement of levee systems, etc. For a coastal location, the recurrence probability for a specific storm surge level relies on the storm climatology and the local geographic characteristics.

Secondary flood hazards are those related with clogging of water intake and outlet due to sedimentation and/or debris and with hydrodynamic forces caused by the flow of water during site inundation.

These two secondary hazards are linked to the inundation level through the specific configuration of the site (e.g. the level in the river is linked to flow, and flow is linked to the velocity of water through the configuration of the river basin upstream and downstream of the site).
Flood hazards are temporal and spatial stochastic phenomena whose occurrence and magnitude (e.g. amount of precipitation and peak discharge) may be complex. As with other natural phenomena, the ability to predict their future occurrence is subject to data limitations and incomplete understanding of the physical phenomena. Flood hazard assessment for nuclear installations is currently based on deterministic approaches. In this field, a unified approach for probabilistic methods such as the one established for seismic hazard (PSHA) is not yet available. Nonetheless, recent technical and regulatory developments have established a framework for performing probabilistic analyses of flood hazards.

Ref [26] provides general guidance on how to derive the frequencies of inundation from meteorological and hydrological causes, such as local precipitation, run-off resulting from precipitation or snow melt, high tide, storm surge, 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. More detailed guidance can be found in Ref [50].

The desirable output of the Probabilistic Flood Hazard Analysis includes at least the hazard curves for flood level (median, mean and quantiles, see Fig. 17). It is important to be cautious when the Probable Maximum Flood (PMF) or any other deterministic limit is used to truncate the hazard curve. Using a non-frequency based extreme-flood estimate as a 'cap' for a frequency distribution could be inconsistent with a risk-informed process and could lead to excessive distortion of the risk profile. Note that calculation of the PMF does not provide an estimate of annual exceedance probability or uncertainty metrics. However, as part of a risk informed decision making process, comparison of the PMF against the outcome of the probabilistic analysis is desirable.

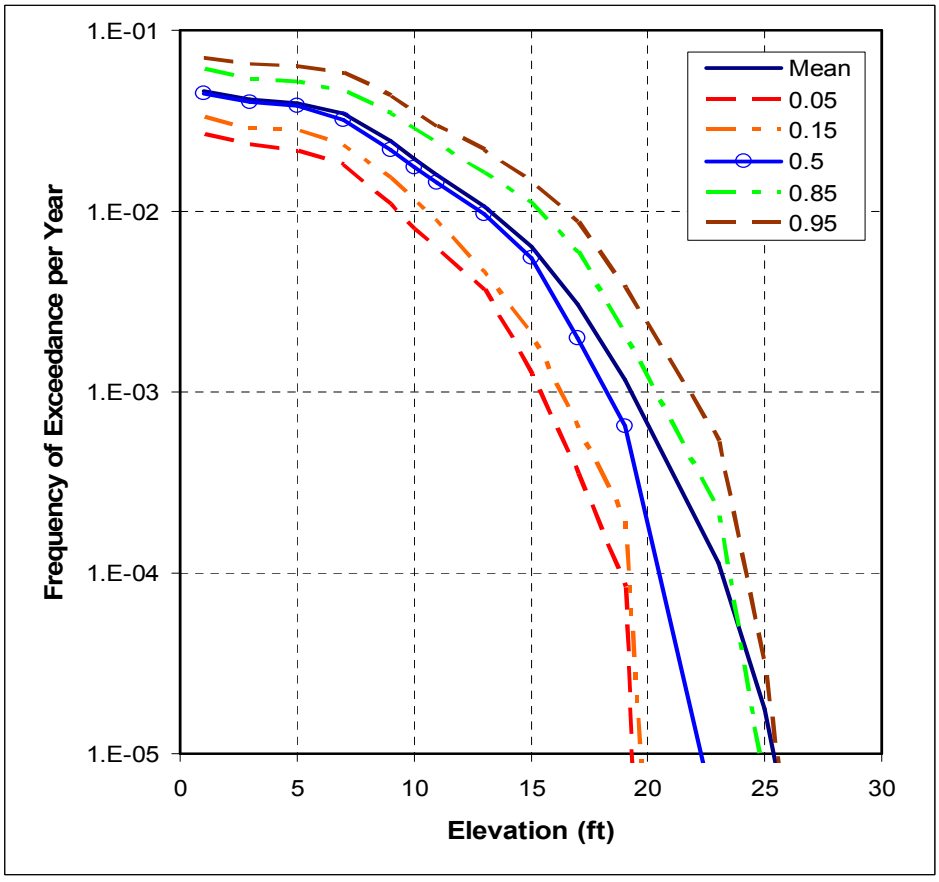


FIG. 17. Typical hazard curves for flooding.

Probabilistic techniques can be divided into two broad categories: statistical methods and detailed probabilistic analysis methods.

Statistical methods rely on extrapolation of historical data. Statistical extrapolations are typically based on time series analysis and synthesis. The 'reasonable' limit for extrapolation to low annual exceedance probabilities by only statistical means is a controversial topic. A simple analysis using site data will typically allow for the estimation of the flood events that have annual exceedance probabilities of 1 in 100 (i.e., 10^{-2} year^{-1}), or potentially 1 in 200 (i.e., $5x10^{-3}$ year^{-1}). Newer methods have been developed that allow for computing hazard curves with ranges of validity for return frequencies from 10^{-2} year^{-1} to over 10^{-5} year^{-1} with differing levels of precision [70].

Detailed probabilistic analysis methods integrate hydrologic and statistical models and the uncertainty associated therewith. This approach has some advantages over the purely statistical approach, including the utilization of paleo and historical flood data, to enhance instrumental records, and the use of Monte Carlo simulation or the Joint Probability method to combine stochastic and hydrologic models in order to develop probability of exceedance curves for hydrologic parameters.

Current practice to estimation of uncertainties in the hazard curves heavily relies on expert opinion [50]. The evaluation of uncertainties typically requires expert interpretations of data, models, etc. The assessment of sources of uncertainty has to be carried out using a structured, formal approach that identifies the sources of uncertainty and estimates their effect on the determination of maximum flood levels (e.g. development of logic trees).

7.2.4. Tornado

Tornadoes are a special case of 'high winds', whose main characteristic is that the effects are localized along a relatively narrow path, when compared with the effects of tropical or extra-tropical cyclones. Main parameters of tornado hazard models are the maximum wind speed within the tornado, path width and path length.

It has to be noted that, since the true maximum tornado wind speeds have rarely been measured, but estimated from the damage caused by the tornado, the hazard models usually rely on the categorization of the recorded tornadoes using a tornado intensity scale, such as the Enhanced Fujita scale. For each category, the intensity scales give an estimate of the maximum wind speed within the tornado. This maximum wind speed occurs over a relatively small portion of the length and width of the tornado, and most of the winds near the ground are much less than the maximum. The variation of the wind speeds along the path and across the width of the tornado is a key part of any tornado risk assessment program.

Ref [26] provides general guidance on how to derive the frequencies for the tornado hazard. More detailed guidance can be found in Ref [50]. The output of the tornado hazard analysis consists of the hazard curves for maximum tornado wind speed (median, mean and fractiles) (Fig. 18). Path widths and atmospheric pressure drops are usually correlated to wind speeds using an air flow model (e.g. the single Rankine combined vortex in Ref [71]).

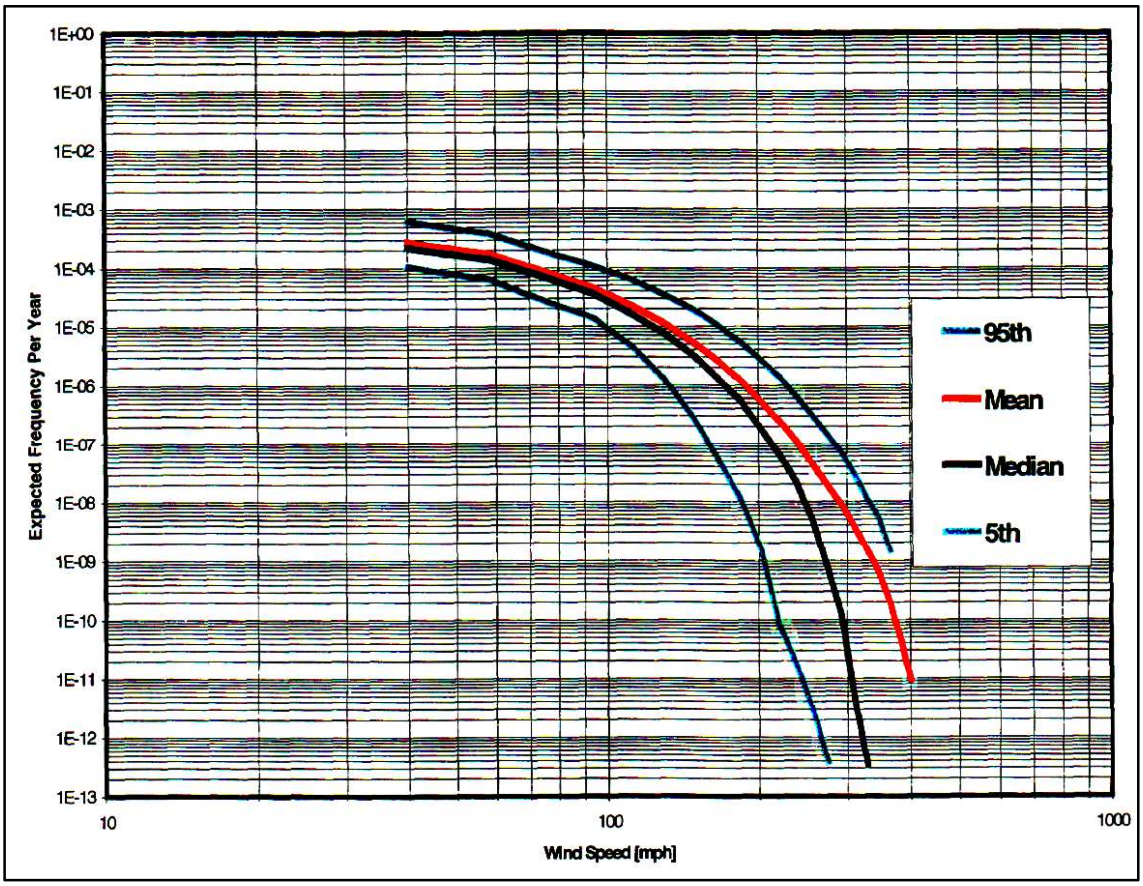


FIG. 18. Typical tornado hazard curves for a 91 x 91 m site, (Reproduced courtesy of Lawrence Livermore National Laboratory, Ref.[72].

As mentioned before, high winds associated with any meteorological event can cause debris to become wind borne missiles. However, tornado winds further exacerbate the debris problem because of the vertical lofting component of the mean wind, which is not associated with other wind-causing phenomena in Ref [50]. The discussion in Section 7.2.2 about the windborne missile hazard applies here in its entirety.

7.2.5. Flood due to long period water waves

Long period water waves can take place in large water bodies, such as seas or lakes. The most well-known waves of this kind are the tsunamis (see Annex 1). In contrast with other causes of flood (Section 7.2.3), these waves produce both a rising (run-up) and a descent (draw-down) of the water level, due to their oscillatory nature. Ref [26] provides general guidance on how to assess the tsunami and seiche hazards. More guidance can be found in Ref [73].

Typically, the hazard is assessed using a deterministic approach, in which the potential tsunami or seiche sources are identified based on the historical and geophysical data. The source parameters of earthquake, landslide or volcanic origin, as well as uncertainties of the parameters are defined. In order to account for the uncertainties regarding a source, a large number of numerical calculations are carried out under various conditions within a reasonable specific range of parameters. The range is determined from the estimated uncertainties. The effects on the NPP site, not only the maximum water level, but also the maximum drawdown and impact forces, are calculated for each source. If annual frequencies can be associated to the different source parameters, a crude estimate of annual frequency can be associated to each event and to the computed water levels.

In contrast to deterministic analysis, Probabilistic Tsunami Hazard Analysis (PTHA) integrates the many different types of tsunami generators and the multiple sources of uncertainty related to source parameters and to the numerical models for tsunami propagation. Hazard curves for maximum tsunami height and drawdown at the NPP site can be obtained, represented by the mean, median, or other specified fractiles (Fig.19). Probabilistic evaluation for the Still Water Level have to be included as part of the PTHA. The Still Water Level is a combination of tide, storm surge, and any other water level disturbance that has a period on par with or greater than the tsunami wave period. The total PTHA hazard curve must account for the joint probability of tsunami effects with other antecedent water level effects.

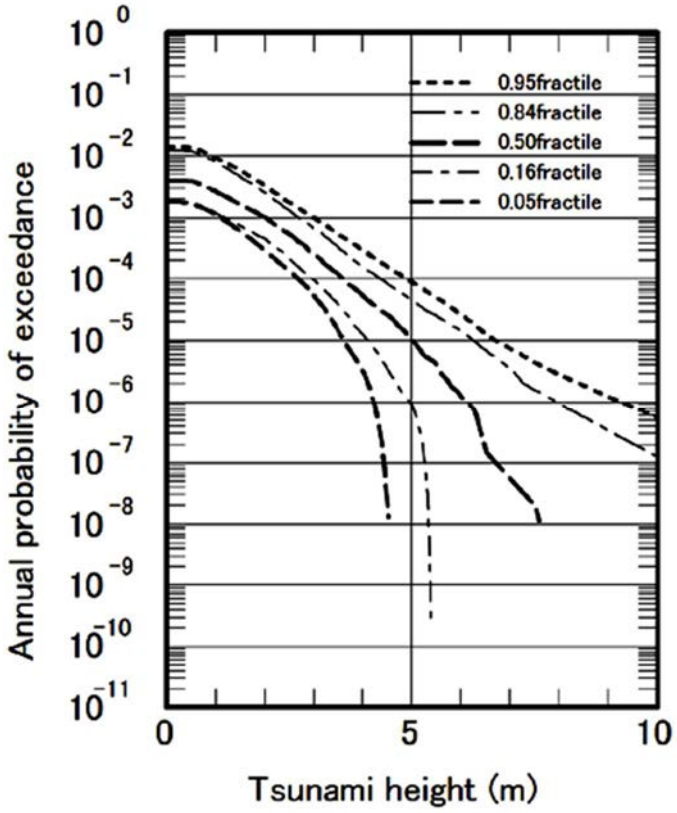


FIG.19. Example of a tsunami height hazard curve [73].

It has to be noted that a large research effort on the assessment of tsunami hazards was started worldwide after 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 PTHA is analogous to PSHA, it is not the current practice applied by Member States for assessing tsunami hazards. That is, methods for the assessment of tsunami hazards using probabilistic approaches have been proposed as described in Ref [73], but standard evaluation procedures have not yet been developed and generally applied in Ref [26].

Secondary hazards are those related with clogging of water intake and outlet due to sedimentation and debris and with hydrodynamic forces caused by the flow of water during run-up and descent. These two secondary hazards are linked to the maximum and minimum levels through the specific configuration of the site.

7.2.6. Flood due to failure of water control structures

Failure of an upstream dam or impoundment can result in a flood at a NPP. 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. Coincident failures may be

caused by a hydrologic event that overwhelms multiple dams simultaneously or a seismic event that causes two or more dams to fail. Successive failures may initiate with a single failure, which causes additional failures downstream.

Reference [26] provides general guidance on how to assess the hazard resulting from failure of water control structures, typically, dams located upstream the site. One important difference between a flood due to precipitation and a flood due to the failure of a water control structure is that the latter could generate a wave of great height moving downstream at high speed which could arrive at the plant site with only a short warning time. A considerable dynamic effect could be exerted on the plant site and on the structures built on it.
Traditionally, flooding due to dam failure has been evaluated using deterministic models by conservatively assuming that (a) the probability of failure for the dams upstream of the NPP site equals unity and (b) the timing of failure for multiple dam failures is conservative. On the other hand, probabilistic dam failure analysis involves the following: (1) identifying dams upstream of the site and their potential failure modes, (2) determining the probability and severity of events that could initiate a dam failure, (3) calculating the probability of dam failure given the occurrence of such events (i.e., develop fragility curves for each dam), and (4) determining the flood impacts downstream of the dam has to various failure modes occur.

Reference [26] 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 NPP site, not to mention the calculation of failure frequencies. The safety guide suggests that it may be more efficient to make a simple conservative analysis by assuming the failure of the structure. If the results of this simplifying and conservative analysis show no effects of flooding at the plant site, the hazard can be screened out. Domino effect of dam failure needs to be evaluated before any dam is screened out.

When the hazard cannot be screened out, typically, the effects in the NPP site are assessed using a deterministic approach, in which the potential dam failure modes are identified based on the type of dam and the characteristics of the dam site. From each considered failure mode and failure scenario, the water path through the dam and the associated flow time-history are identified. Then, the dam break flow is propagated downstream to the NPP site in order to determine the effects:

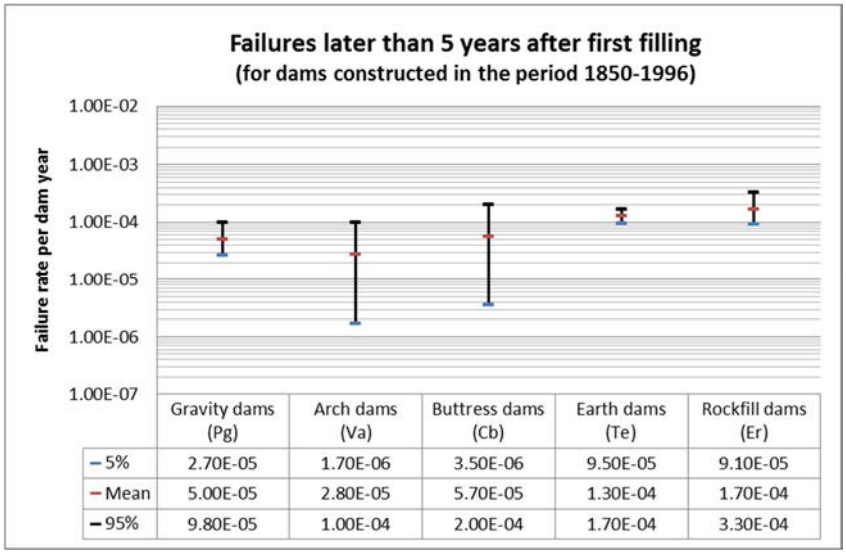
- Peak flow rate and discharge time history of the rupture event (flood hydrograph) at NPP site;
- Peak water level and time history of the water surface elevation at the NPP site;
- Possibility of blocking of intakes due to debris or ice;
- Dynamic and static forces resulting from the flow of ice and debris.

The susceptibility of dams to fail due to hydrologic forces is based on the type of dam, reservoir water level with respect to its design, dam condition, and dam operational strategies. Hydrologic failures are typically characterized by some warning due to the fact that flood events typically develop over a time scale that is monitored by dam owners and operators. For most dams, the risk of failure from a seismic event is due to vibratory ground motion, but dams built on a fault also may fail as a result of fault displacement. Alternate seismic induced events may exist and have to be analysed. This may include seismically induced landslides or avalanches that could cause the reservoir to overtop the dam.

Internal events that lead to dam failure are typically handled in one of two ways. The first method uses detailed analyses to determine the probability of failure given the design and construction details of the dam and random variability inherent in the materials used for construction. Unfortunately, this type of analysis requires a significant amount of information about the dam. Acquiring information of sufficient detail may prove difficult or impossible. Additionally, as maintenance is performed or the condition of the dam changes over time, the analysis may need to be repeated. Consequently, such a detailed approach may not be feasible. Alternatively, a Bayesian model may be used to determine the probability of an internal event leading to a failure. Bayesian models determine the probability of

failure using historical data and can be modified based on a dam's current condition. The most recent dam inspection report has to be sufficient to gauge the condition of the dam.
In order to account for the uncertainties regarding the failure mode and the flood propagation to the NPP site, a number of flood analyses are carried out corresponding to a number of scenarios of rupture and flood wave propagation. The worst case scenario or an envelope of worst case conditions are kept for design or assessment of the NPP.

If annual frequencies can be associated to the different scenarios, a crude estimate of annual frequency can be associated to each scenario and to the computed water levels.
Figure 20 shows annual failure rates of dams of different types computed from actual dam failures[10] in North America, Western Europe, Australia and New Zealand, considering dams built during two periods of time, 1850-1996 and 1930-1996. Failures due to any cause are considered; but only failures occurred later than five years after first filling are taken into account. Note that for the most modern dams, average failure rates are between 10^{-5} and 10^{-4} failures per dam and year.



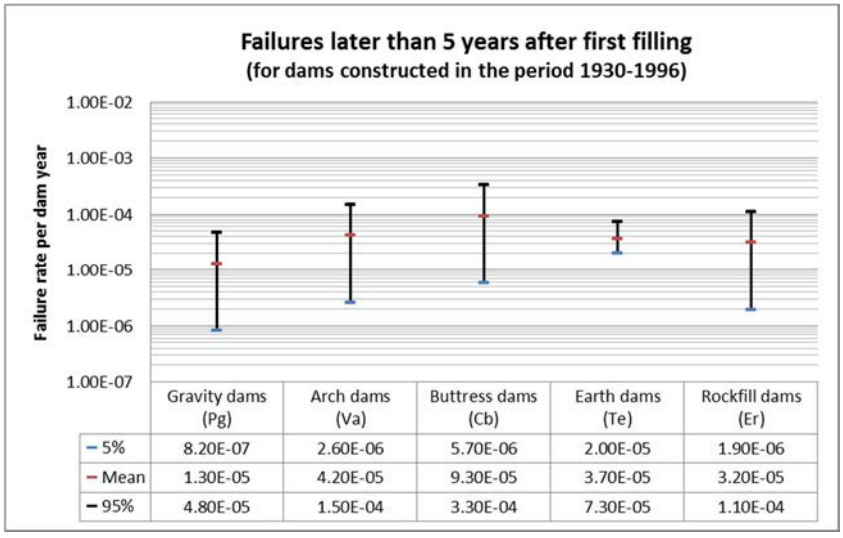


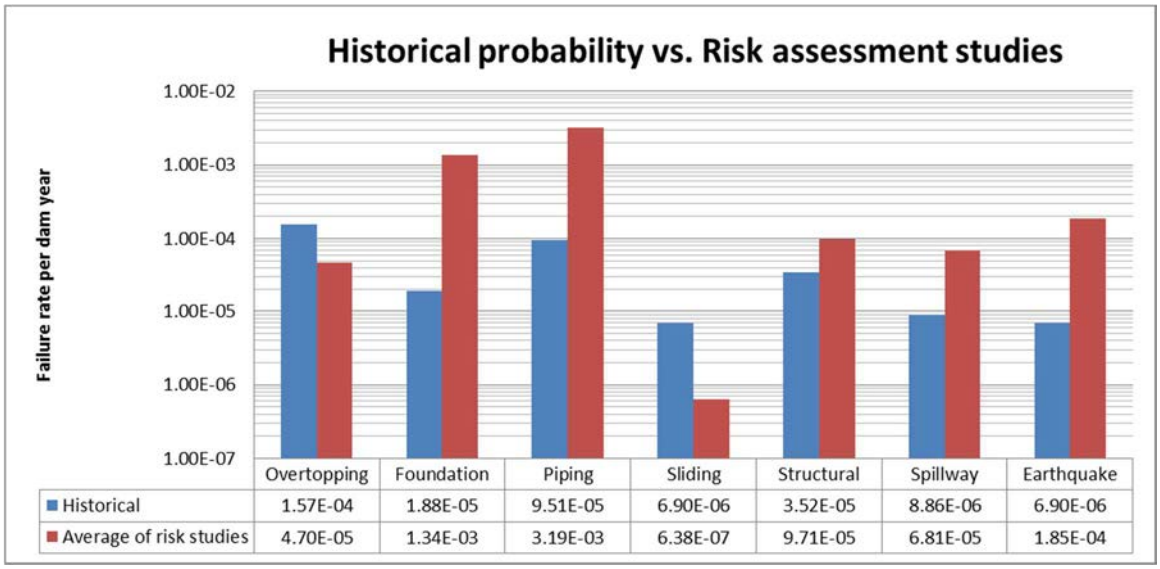
FIG.20. Failure rates of different dam types based on historical data of failures in North America, Western Europe, Australia and New Zealand (elaborated from Ref. [74]). The mean value corresponds to the failure rate considering the whole period. Percentile values indicate the range of variation of the failure rate along the period of computation. A small range indicates a fairly constant failure rate.

[10] According to the International Commission on Large Dams (ICOLD), 'failure' of a dam is the 'collapse or movement of part of a dam or its foundations so that the dam cannot retain the stored water'.

However, statistical studies based on historical records of failures can lead to inaccurate conclusions since data are not homogeneous along the period of time used for the study. For example, design, construction and surveillance techniques have improved along the time and hence, the dam samples taken at dates very far apart in time are not directly comparable. In addition, for some modes of failure, such as the seismically induced failures, the exposure to the hazard might not be uniform all over the sample and the time period for which usable information is available might not be long enough. Hence, the approach to obtain the annual frequency of a dam failure based on historical frequencies, and not on specific studies of the particular dams, provides only a crude estimate of the order of magnitude.

As outlined above, a more sophisticated approach, not yet considered in Ref [26]associates each possible dam failure mode to a load parameter (e.g. level of water in the reservoir, seismic ground acceleration) and the conditional probability of failure is computed as a function of the load parameter. This requires a detailed capacity study specific to the particular dam. From the annual frequencies of exceedance of the load parameters, the annual frequencies of failure under each of the failure modes are computed. A flood analysis is made for each failure mode in order to assess the consequences at the NPP site and, therefore, correlate annual frequencies of dam failure to annual frequencies of effects (e.g. water levels) at the site. Integration of these scenarios allows the hazard curves at the site for maximum flow rates and corresponding water levels to be obtained. The approach is described in Ref [75].

Following this approach, dam risk assessments have been carried out by some Member States within their dam safety risk management programs. Figure 21 shows how computed failure rates compare with historical failure rates for a particular set of dams. Note that, except for the overtopping and sliding failure modes, computed failure rates are larger, sometimes much larger, than historical values.



	Overtopping	Foundation	Piping	Sliding	Structural	Spillway	Earthquake
Historical	1.57E-04	1.88E-05	9.51E-05	6.90E-06	3.52E-05	8.86E-06	6.90E-06
Average of risk studies	4.70E-05	1.34E-03	3.19E-03	6.38E-07	9.71E-05	6.81E-05	1.85E-04

FIG.21. Comparison of dam failure mode rates from risk assessment and from historical data for U.S. Bureau of Reclamation dams, [76].

7.2.7. Explosion

Ref [28] provides general guidance on the assessment of external explosion hazard. The explosion hazard can come from stationary or mobile sources. When the hazard cannot be screened out based on safe distance considerations, probability of occurrence of an explosion is to be derived based on data about the frequency of explosions in industrial facilities or on transport routes in the vicinity of the site. Normally, due to lack of site specific data, reference have to be made to global accident statistics and expert judgement is required to adapt those statistics to a particular site.

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 / accident).

For industrial facilities, when enough information is available, frequency of explosion can be derived 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. From these values, probabilistic analysis procedures can be used for calculating the frequency of exceeding different levels of overpressure at the NPP structures from accidents in stationary or mobile sources in Refs. [77-78]. Overpressure values are the basic input for the structural capacity assessments. Figure 22 shows an example of overpressure hazard curves.

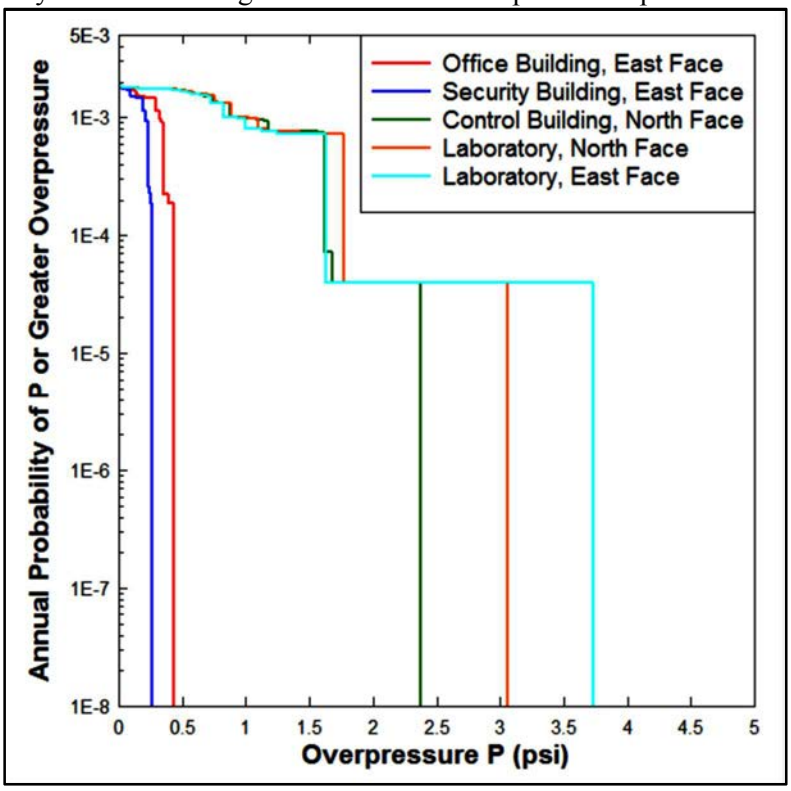


FIG.22. Overpressure hazard curves for buildings in a sample facility [78].

7.2.8. Release of hazardous substances

Ref [28] also addresses the hazard assessment of release of hazardous (toxic) fluids. The methodology is similar to the one used for the explosion hazard. The release hazard can come from stationary or mobile sources. When the hazard cannot be screened out based on safe distance considerations, frequency of occurrence of a release is to be derived based on data about the frequency of releases in industrial facilities or on transport routes in the vicinity of the site. As for the explosion hazard, due to lack of site specific data, reference have to be made to global accident statistics and expert judgement is required to adapt those statistics to a particular site.

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

For industrial facilities, when enough information is available, frequency of releases can be derived from the frequency of ruptures leading to breach of pressure boundaries of vessels or piping.
The final result of the release hazard assessment is a list of potential release sources including the amount and nature of the hazardous substance, the distance to the site and the annual frequency of release. From these values, probabilistic analysis procedures, normally based on atmospheric diffusion models, can be used for calculating the frequency of exceeding different concentration levels of hazardous substances at the control room air intakes. These concentrations are the input to assess the effects on the operators from accidents in stationary or mobile sources.

7.2.9. Extreme temperatures

Ref [26] provides general guidance on how to assess the hazard of extreme temperatures. In contrast to other meteorological hazards, extreme cold or hot air temperatures are phenomena that develop relatively slowly, that can be predicted some time in advance, and that normally do not produce significant damage unless they actuate during several hours, even days.

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 have to 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 has 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. Section 5.7 of Ref [79] can be used for additional guidance.

7.2.10. Aircraft crash

Ref [28] provides guidance to assess the hazard of accidental aircraft crashes. Three types of events are considered, each with a possibly different annual frequency:

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

(2) Crash of an aircraft flying along an airway, making use of navigation aids, or within a military flight zone. This category corresponds to most commercial aviation, using small, medium and large aircraft;

(3) Crash as a result of a take-off or landing operation at a nearby airport.

Crashes of type 2 and 3 can normally be screened out for sites located at a distance larger than 4 km from airways or larger than 30 km from airports or military training areas.

When crashes cannot be screened out based on distance considerations, the probability of an aircraft crashing in the site vicinity is determined for each class of aircraft considered (small, medium and large civil and military aircraft) by using the aircraft crash statistics. Table 5 shows an example of this type of statistics for a Western European country.

TABLE 5. EXAMPLE OF AIRCRAFT CRASH STATISTICS

Commercial aircraft	General aviation	Military aircraft
Flights per year 1000000 Average flight distance 1500 km Crashes per flight 10^{-6} Airports 80	Flights per year 3500000 Average flight distance 400 km Crashes per flight 10^{-4} Airports 400	Flights per year 600000 Average flight distance 500 km Crashes per flight 10^{-5} Airports 40

The results need to be expressed in the form of crashes per year per unit area in the site vicinity. For crashes of type 1, the crash rate is computed for a circular area 100-200 km in radius around the site, [28]. For crashes of type 2 and 3, this rate is computed using the length of airways or the airports located at a distance less than the safety distance.

The estimated probability of an aircraft crash affecting the plant may be determined in terms of crashes per year per unit area multiplied by an effective area of the site for damage to items important to safety. The size of the effective area depends on the average angle of the trajectory relative to the horizontal; the plan areas of the relevant structures and their heights, other areas relating to items important to safety; and allowances to be made for the size of the aircraft [28]. Figure 23 illustrates this concept.

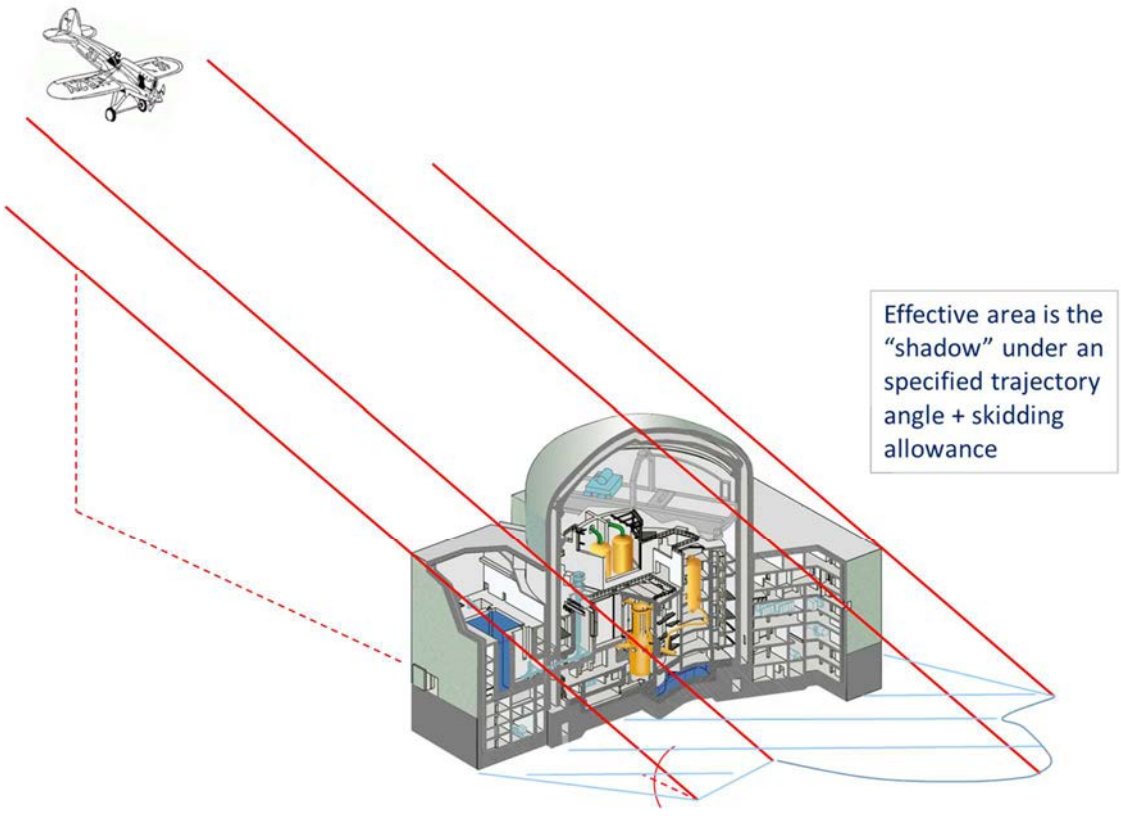


FIG. 23. Illustration of the effective area concept for aircraft crash hazard.

7.2.11. Volcanic phenomena

Volcanic phenomena are very complex and entail a large number of hazards. The IAEA Specific Safety Guide No. SSG-21 entitled Volcanic Hazards in Site Evaluation for Nuclear Installations [27] provides general guidance on how to derive the frequencies for the different volcanic hazards. Ref [27] covers tephra fallout, pyroclastic density currents, lava flows, debris avalanches, volcanic debris flows, opening of new vents, volcano generated, missiles, volcanic gases, ground deformation, volcanic earthquakes and groundwater anomalies. More detailed guidance can be found in Ref [80].

Generally, for sites located at more than 100 km from a capable volcano, all volcanic hazards can be screened out, except for the tephra fallout. As stated in SSG-21[27], the hazard assessment for tephra fallout for each capable volcano considers the potential sources of tephra, the magnitudes of potential tephra-producing volcanic eruptions and the physical characteristics of these eruptions, the frequency of tephra-producing eruptions, and the meteorological conditions between source regions and the site.

Then, numerical simulation of tephra fallout at the site is used. SSG-21[27] recognizes that in such an analysis, Monte Carlo simulation or other applicable simulation techniques of tephra fallout from each capable volcano is conducted, taking into account the variation in eruption volume, eruption column height, total grain size distribution and wind velocity distribution in the region as a function of altitude and related parameters.

In the context of SSG-21[27] such models lead to a frequency distribution of tephra accumulation, commonly presented as an annual frequency of exceedance curve for the hazard. Uncertainty in the resulting hazard curves is expressed by confidence bounds, and the basis for the selection of the confidence levels is documented.

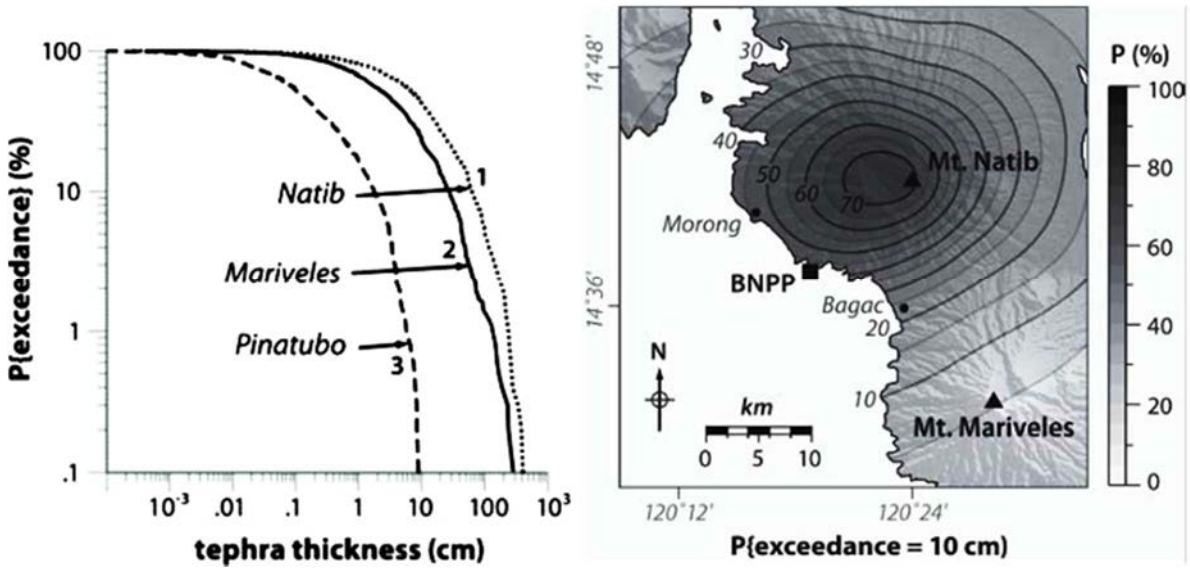


FIG.24. Hazard curves show the conditional probability of exceeding different thicknesses of tephra at the location of the BNPP, given a volcanic eruption. Graph on the left compares tephra thicknesses modelled for Natib (1), Mariveles (2), and Pinatubo (3). For a given eruption, tephra accumulation at the BNPP from eruptions of Mt. Natib and Mt. Mariveles are similar, and would likely exceed tephra accumulations associated with a Mt. Pinatubo eruption by one order of magnitude. Map on the right shows the probability contours of tephra accumulation exceeding 10 cm (approx. 100 kg m^{-2}), given an explosive eruption of Mt. Natib (contours have a 5% interval), Reproduced as courtesy of Cambridge University Press,[81].

As an example, Fig. 24 shows a conditional probability of exceeding different thicknesses of tephra at the location of the Bataan NPP (BNPP, southern part of the Luzon Peninsula, Philippines), given a volcanic eruption. When this conditional probability is convolved with the annual frequency of a volcanic eruption at the given volcanoes, the hazard curves for the tephra thickness are obtained.

7.3. PLANT-LEVEL FRAGILITY

When a plant-level HCLPF capacity has been computed following the methods described in sections 4 and 5, a mean plant-level fragility curve can be derived if a log-normal model is assumed and the composite logarithmic standard deviation β_C is estimated [45, 82]:

$$P_F(a) = \Phi\left[\frac{\ln\left(\frac{a}{C_{50\%}}\right)}{\beta_C}\right] \quad (1)$$

where:

a = hazard strength parameter (e.g. wind speed)

$P_F(a)$ = fragility = conditional probability of failure, given that hazard reaches level a

$\Phi(\,)$ = standard Gaussian cumulative distribution

$C_{50\%}$ = median capacity = $C_{1\%}\, e^{2.33\,\beta_C}$

Using this approach, the HCLPF capacity is assumed to correspond to 1% failure probability in the mean fragility curve ($C_{1\%}$). Then, an estimate of β_C is produced.

In the context of a seismic assessment, β_C lies typically within the range of 0.3 to 0.6, and the final risk estimate (see Section 7.4 below) is not very sensitive to the selected value of β_C, [45, 82]. In addition, since the resulting mean fragility curve is anchored to $C_{1\%}$ (i.e., the capacity corresponding to1% conditional probability of failure), the smaller β_C is, the more conservative the risk estimate will be.

In other contexts, different from the seismic assessment, there is less information available about how to select appropriate values of β_C and the analyst will need to use engineering judgement based on published results or in sensitivity studies.

However, in general, when assessing the kind of extreme events within the scope of the present publication, it is very unlikely that variability in plant response and capacity assessment results in β_C less than approximately 0.3.

7.4. RISK ESTIMATION

Given a mean hazard curve $H(a)$ and a mean plant-level fragility curve $P_F(a)$, then a point estimate of risk R_m can be obtained by numerical convolution of the mean hazard curve and mean fragility curve by either of two analytically equivalent equations [22, 82]:

$$R_m = -\int_0^{+\infty} P_F(a)\,\frac{dH(a)}{da}\,da \qquad R_m = \int_0^{+\infty} H(a)\,\frac{dP_F(a)}{da}\,da \quad (2)$$

where $H(a)$ is the mean hazard exceedance frequency corresponding to hazard strength a.

The resulting point estimate of risk R_m can be used as an estimate of the annual frequency of safety significant failure due to the hazard.

8. DOCUMENTATION

The publication describing the vulnerability assessment and its results have to include the following points:

(1) Selection of applicable hazards, according to the hazard screening process described in Section 2 of the present report. The application of the screening criteria to the specific site is to be described, together with any bounding analyses performed to support the screening. As a result, the hazards selected for the vulnerability assessment will be itemized.

(2) Selection of components, according to the methods described in Section 3 of the present report. Normally, different lists of SSCs will be developed for the different selected hazards. The lists and the basis for each list have to be included in the publication;

(3) Plant-level capacity for the selected hazards, obtained according to the methodologies described in Sections 4 and 5 of the present report. The partial and final results have to be documented, together with the process. For each applicable hazard, the following final results are relevant:

- Plant-level capacity, that is, the threshold below which fundamental safety functions will not be jeopardized
- List of 'weak links' against the hazard, with the associated capacity (mean fragility or HCLPF capacity)

(4) Performance of fundamental safety functions, once the plant capacities are exceeded, according to the methods described in Section 6 of the present report. For each applicable hazard, the most likely sequence of events and the timing of each sequence have to be given in the publication, together with their bases.

(5) Risk metrics, if computed from the plant-level capacities and available hazard assessments, as described in Section 7. If available, the hazard assessment has to be documented in a manner that facilitates applications, upgrades, and peer review. The publication describing the hazard assessment has to identify the project team member, their roles and responsibilities, peer reviewers, models, modelling assumptions, process for evaluation of uncertainties, supporting data, hazard quantification, software used, the results and the results of the sensitivity evaluations, and the peer review findings and conclusions.

(6) Conclusions and recommendations, with a summary of the weak links found all over the assessment and the suggested improvements, if any. If no risk estimates are computed, suggested improvements will refer to modifications in plant or procedures which, with a relatively small investment, will produce a significant improvement in margins, in the performance of the safety functions after the margins are exceeded or in the severe accident management.

(7) Composition and qualifications of the team performing the assessment.

9. REVIEW TEAM COMPOSITION AND PERSONNEL QUALIFICATION

The review team performing the vulnerability assessment is a multidisciplinary team made up of participants with the following expertise:

- Systems engineers with knowledge of the installation's systems, in particular front-line and support systems to address the fundamental safety functions;
- Operations personnel with experience in the operation of the systems (operations personnel are essential to provide real operation experience of the systems);
- External events capacity engineers (civil, mechanical, electrical, instrumentation and control, fire, internal flood, etc.), for the safety margin assessment;
- Hazard experts, for providing input on reference level hazards.

Systems engineers must identify all reasonable alternate means to bring the installation to a stable and safe condition. They also must identify all elements that comprise the frontline and support system components together with the associated electrical, fluid, and pneumatic systems for each of these success paths. The systems engineers have the principal responsibility for selecting the safety significant components and to define the likely accident sequences once the safety margin analyses identify the weak links for each applicable hazard.

Plant operations personnel have to be intimately knowledgeable about normal and emergency operating procedures and operator responses to abnormal situations. These experts have to be aware of instrumentation and actuation systems required to support those operator actions that may be required to accomplish the fundamental safety functions

External events capability engineers are responsible for the capability walkdowns and for screening out components from further evaluations for the safety margin assessments. They define additional effort to be expended on evaluations of individual SSCs, for those components not screened out. Capability engineers perform their functions in the field and in the office.

The review team have to incorporate plant owner's personnel, to the maximum extent possible, so that results and insights obtained during the assessment can be utilized in installation operation, upgrading, and accident management.

The review team is led by a steering group of individuals who possess the following qualifications:

- Knowledge of the failure modes and performance of structures, tanks, piping, process and control equipment, active electrical components, etc., during extreme external events;
- Knowledge of nuclear design standards, design practices, and equipment qualification practices for nuclear installations;
- Ability to perform fragility/margins-type capability evaluations including structural or mechanical analyses of essential elements of nuclear installations;
- General understanding of Probabilistic Safety Assessment (PSA) systems analysis and conclusions;
- General knowledge of the installation's systems and functions.

It is not necessary that each member of the steering group individually has strong capability in all of these areas or strong experience on external event effects. However, in the composite, the steering group have to be strong in all of these areas. A good composite makeup of the group would include systems engineers, plant operations personnel, and capability engineers.

The steering group has a key role during the plant walkdowns, where engineering judgement has to be applied in order to screen out from further consideration the SSCs not likely to be the weak links against a particular hazard.

Requirements for implementing a formal quality Management System may be established by the NPP owner. The Management System specification has to identify the standards that need to be met. However, since the activities involve the assessment for beyond design basis conditions, the requirements will normally be less demanding than for activities related with design.

APPENDIX A: GUIDELINES FOR INDEPENDENT REVIEW

A.1. INTRODUCTION

A.1.1. PREAMBLE

The application of the vulnerability assessment methodology described in the main body of the present publication requires a significant amount of engineering judgement. This is especially true for the activities involving:

- Selection of hazards applicable to the specific site.
- Screening-out of rugged structures, systems and components, for each applicable hazard.
- Identification of potential failure modes, for the screened-in structures, systems and components, and
- Assessment of performance of fundamental safety functions, once the plant level capacity is exceeded, for each applicable hazard.

Use of engineering judgement is encouraged, in order to have cost-effective assessments; but a necessary consequence is the need for an external validation of the assessment. The intent here is not to have a formal quality control process, but to conduct a review by independent individuals in order to validate the technical decisions taken along the process and the final results. The emphasis is on the technical soundness.

Therefore, the independent review have to go through the whole process and, at the discretion of the reviewers, check how the main technical decisions were taken, how the main results were obtained and whether they are reasonable and consistent with good practice, according to their experience. A plant walkdown is a key component of the independent review, since it will provide first-hand information about the plant and its surroundings and it will allow direct observation of the key issues.

This appendix provides guidelines for the team performing the independent review and suggests a way to document the review. The guidelines have not been understood as a rigid framework. On the contrary, the ultimate responsibility rests on the independent review team and, based on its judgement, the team might want to adapt or modify the guidelines to better assess a specific case. The guidelines are therefore intended to help each reviewer formulate his/her review plan in conjunction with his/her own experience.

A.1.2. PURPOSE OF THE INDEPENDENT REVIEW

The purpose of the independent review is to validate the vulnerability assessment performed according to the methodology described in the main body of the present publication.

The objective is to ensure that an open/transparent process has been used, in accordance to the methodology, that the process has produced reliable, traceable, factual information, and that the documentation accurately describes the process and the results.

A.1.3. SCOPE OF THE INDEPENDENT REVIEW

The independent review includes the following activities:

(1) Selection of the review team;

(2) Review of documents defining the ‘as-is’ condition of the plant;

(3) Review of activities carried out during the vulnerability assessment, namely:
   - Team composition and personnel qualification
   - Selection of applicable hazards

- Selection of components
- Plant capacity assessment for the selected hazards
- Performance of the fundamental safety functions
- Risk estimates, if applicable
- Management system and documentation

(4) Plant walkdown;

(5) Conclusions and documentation.

These activities are described in detail in the following sections.

Rather than an inspection or an audit, the independent review is intended to be a technical exchange between the team performing the assessment and an independent team of reviewers, who could have performed the assessment. Ideally, after going through the available information, the review team puts itself in the position of the team who has performed the assessment and sees how it would have proceeded in complying with the methodology and what would have been its findings.

A.1.4. STRUCTURE OF THE GUIDELINES

The rest of the Appendix comprises two additional sections.

Section A-2 is devoted to the suggested methodology for the review. It covers the sources of information, the review techniques and the organization of the review, including preparation, implementation, reporting and final documentation.

Section A-3 provides the technical guidance for the review. The section has been divided into seven sections, corresponding to the different areas of review. For each area, the technical focus of the evaluation is given, together with the expectations, and examples of documents likely to be needed for the review in the area.

A.2. REVIEW METHODOLOGY

A.2.1. SOURCES OF INFORMATION

A.2.1.1. Basis for the review

The basis for the independent review is the methodology for assessment of vulnerabilities to extreme external events, as described in the main body of the present publication.

A.2.1.2. Documentation provided by the counterpart

As input, the independent review requires two categories of documentation:

- General information about the plant and its near-regional area.
- The required information is normally provided by the updated Safety Analysis Report, [83]. It includes data about the site (geography, geology, climatology, hydrology, seismicity, etc.), about the nuclear technology and plant layout, about the main structures, systems and components, about the design bases, design codes, etc.
- Specific information about the vulnerability assessment that has been performed
- This information will be included in one or several reports, according to the recommendations given in Section 8, in the main body of the present publication.

A.2.2. REVIEW TECHNIQUES

The independent review will typically use four steps to perform the assessment and, if applicable, develop recommendations. These steps are defined in very general terms in the following sub-sections. The details are given in Section A-2.4 and Section A-3.

A.2.2.1. Review of written material

As a first step, the review team goes to the written information provided as input (Section A-2.1.2).

In this step the team familiarizes itself with the plant and its environment and acquires an overall perspective of the work done by the counterpart for the vulnerability assessment.

A.2.2.2. Discussion and interviews

After the review of the written material, the review team is ready for discussion with the counterpart, including interviews with key persons, in order to clarify particular aspects of the vulnerability assessment or to identify how the key technical decisions were taken and how the key results were obtained.

After this stage, the review team need to have a clear understanding about how the counterpart made the assessment.

A.2.2.3. Direct observation

In this phase of the review, the review team performs a plant walkdown. The purpose of the walkdown is to have a sound basis for developing an independent opinion about the key topics

Once the review team develops an independent opinion, the coincidences and discrepancies with the assessment made by the counterpart are to be identified for discussion during the next phase of the review.

A.2.2.4. Discussion of evaluations and conclusions with counterpart

The opinion of the review team is to be discussed with the counterpart after the walkdown and the reasons for the discrepancies are to be investigated. During the discussion, additional documents might be reviewed or missing information could be identified.

As a result the review team will be able to draw conclusions and to produce a set of recommendations.

A.2.3. WORK WITH THE COUNTERPART

Except for the review of the written material, all steps of the review include interaction with the counterpart. The review team has certain level of freedom to establish the required interaction according to the needs specific for a particular plant. However, the following goals have to be achieved:

- The review team has to familiarize with the plant and its near-regional area up to the point needed to have a sound basis for its judgement;
- The review team has to understand the overall flow and the key decisions taken during the vulnerability assessment, up to the point needed to produce well based conclusions and recommendations; and
- The counterpart has to understand how the independent review was performed and the basis for the conclusions and recommendations.
-

A.2.4. ORGANIZATION

A.2.4.1. Preparation

A.2.4.1.1 Appointment of the review team

As a first step, a review team have to be appointed. The review team have to meet two basic requirements: should

- The individuals in the team should not have been involved in the work to be reviewed;
- The team, as a whole, have to have the qualifications required for the Steering Group defined in Section 9 of the present publication , namely:
  (1) Knowledge of the failure modes and performance of structures, tanks, piping, process and control equipment, active electrical components, etc., during extreme external events;
  (2) Knowledge of nuclear design standards, design practices, and equipment qualification practices for nuclear installations;
  (3) Ability to perform fragility/margins-type capability evaluations including structural or mechanical analyses of essential elements of nuclear installations;
  (4) General understanding of Probabilistic Safety Assessment (PSA) systems analysis and conclusions;
  (5) General knowledge of the installation's systems and functions.

A good composite makeup of the team would include systems engineers, plant operations personnel, and capability engineers. The size of the team depends on the complexity of NPP and the number of applicable hazards. However, it is unlikely that a team with less than three members complies with the qualification requirements.

Normally, a review team leader will be designated, who will coordinate the work of the team and will interface with the counterpart. Informal preparatory meetings or exchange of information will normally take place before the official start between the team leader and the counterpart.

A.2.4.1.2 Kick-off meeting

As a first activity, normally the review team leader will call for a meeting of the review team.

The purpose of this meeting is to provide information about the context of the review, to define the overall approach to the review, to discuss the role and responsibilities of each person (e.g. areas of review) and to agree on a tentative schedule. In addition, any questions not covered in these guidelines have to be discussed.

A short meeting with the counterpart may also be arranged at the occasion of this kick-off meeting.

A.2.4.1.3 Tentative schedule

During the kick-off meeting, a tentative schedule has to be set up for the review.

In a general case, the key milestones for the review schedule are as follows:

(1) Appointment of the review team. Designation of interface persons with the counterpart.
(2) Submittal of basic information about the plant and its surroundings.
(3) Submittal of reports describing the vulnerability assessment.

(4) Meeting with the counterpart, after first analysis of the submittals. Review of detail documentation not submitted previously. Questions & Answers.

(5) Plant walkdown

(6) Meeting with the counterpart, after the walkdown. Preliminary conclusions. Requests for additional information.

(7) Delivery of the independent review final report. Conclusions and recommendations.

For a typical plant, the first four milestones could be completed in less than about six weeks, after the submittal of the relevant documents to the review team. The meeting in (4) can normally be scheduled to last between two and five days. Ideally, it takes place just before the plant walkdown.

A well-organized plant walkdown for review purposes could cover all the important issues in less than a week, including plant formalities and required specific training for the review team. However, access to some areas of the plant could be restricted during normal operation and suitable dates, compatible with plant procedures, have to be identified. It is common that the dates available for the walkdown govern the overall schedule for the review. Hence, the review team have to define the requirements for the walkdown (areas to visit, equipment to inspect, etc.) as soon as possible.

After the walkdown, the review team will have completed its understanding about the plant and its vulnerabilities. In a meeting after the walkdown, these preliminary conclusions will be communicated to the counterpart and requests for additional information will be make, if required for the preparation of the independent review report.

The independent review report, with the final conclusions and recommendations, can normally be delivered about two weeks after the previous meeting. If necessary, a final meeting to present the report and the conclusions can be scheduled.

Note that if the scope of the walkdown includes areas not accessible during normal operation, then it would need to be scheduled during a plant outage.

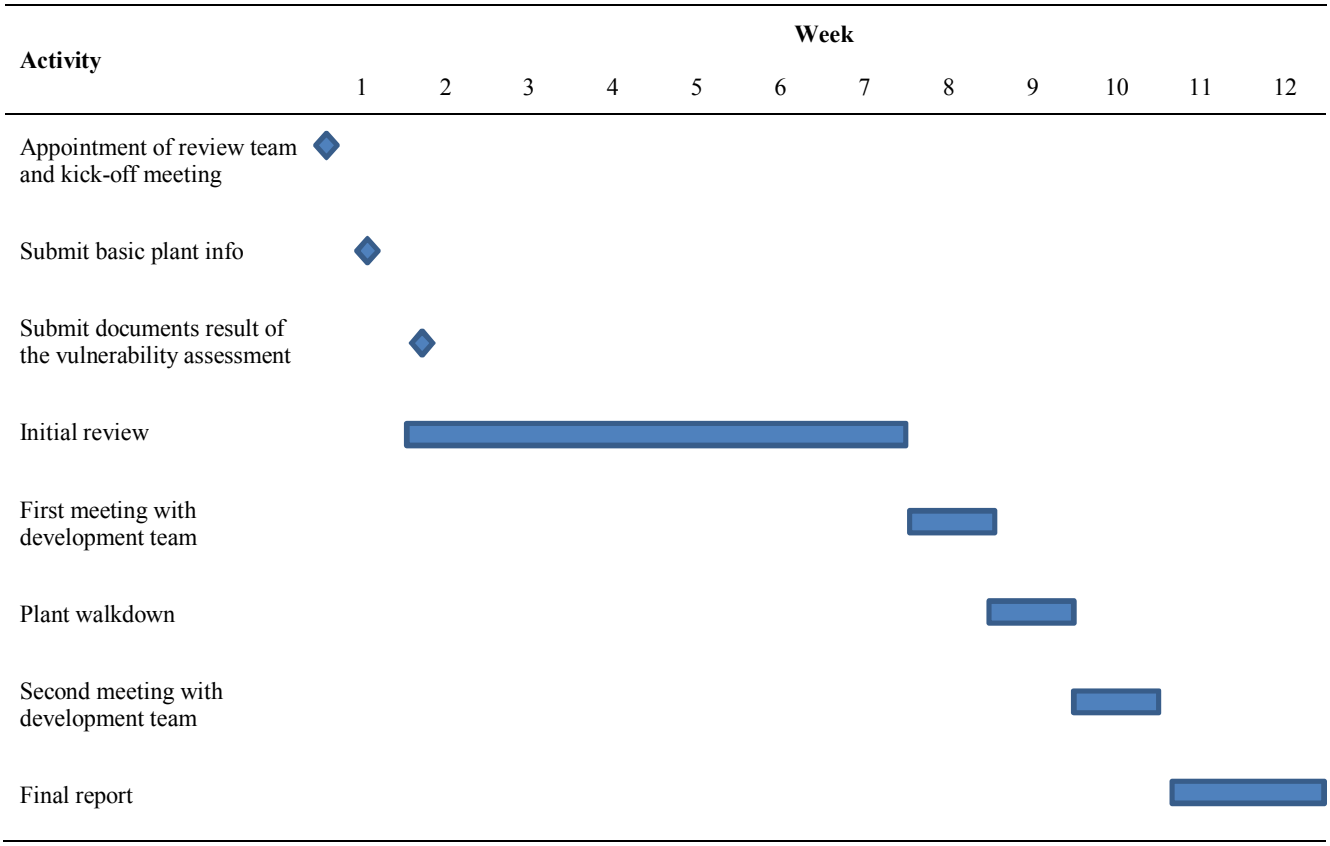


FIG. A-1. Typical schedule for an independent review.

Figure A-1 gives a typical Gantt chart for the independent review in a general case, assuming that the review starts when the vulnerability assessment is practically finished. However, there is no need to wait until the end of the assessment for starting the review. In fact, it could be advisable to review the critical areas (see Section A-3) shortly after the work on them has been completed by the development team. In that case, a set of smaller reviews with simpler schedules will take place along the development of the project.

A.2.4.2. Implementation

A.2.4.2.1 Review of documentation

The first activity of the independent review is the review of the documents submitted by the counterpart. This is an office-based activity with two main objectives:

- Familiarization with the plant, the plant region and the design basis against external events.
- Understand how the vulnerability assessment activities have been developed and how the main results and conclusions were reached.

Documents typically needed are itemized in Section A-2.1.2.

A.2.4.2.2 Pre-walkdown meeting

After the review of the documents, a meeting with the counterpart is scheduled. The purpose of the meeting includes:

- Gather information not covered in the documentation submitted for review. Review of additional supporting documents.

- Clarify with the counterpart the key points of the vulnerability assessment.
- Questions & Answers.
- Define plant walkdown scope and walkdown preparation.
- Preliminary assessment by the review team. Identification of obvious omissions or mistakes in the use of the methodology, if any.

This 'meeting' may be understood as a 'gathering' of the review team and the counterpart team, where separate 'meetings' can be run in parallel addressing different areas of the review.

Ideally, this meeting is held just before the plant walkdown associated with the review.

A.2.4.2.3 Walk down

A plant walkdown is an essential part of the independent review. It is during the walkdown where the review team can actually validate the technical decisions made by the counterpart.

The scope of the walkdown is to be defined by the review team, since it depends on the specific hazards applicable to the plant. The scope will likely include the following:

- General configuration of the site vicinity area (less than 5 km radius): roads, railroads, industrial facilities, general topography, vegetation, etc.
- On-site exterior areas: general layout of the site, drainage systems, fire protection systems, control room air intakes, external surfaces of buildings, systems and components located out of the buildings, cooling towers, water intake structures, pump houses, switchyards, etc.
- Sample of the selected structures, systems and components (Selected SSC List) located inside the buildings.
- Key 'weak links' identified during the vulnerability assessment.

It is anticipated that the whole review team will participate in the walkdown, together with a representative of the counterpart and the required plant operations staff.

A.2.4.2.4 Post-walk down meeting

After the walkdown, the review team will basically have all the information required to finish the review. The review team will have developed its own idea about the plant and its vulnerabilities, to be compared with the results contained in the documentation supporting the vulnerability assessment. The review team will be also able to judge about the performance of the fundamental safety functions, as reported in the documentation. In a meeting after the walkdown, these preliminary conclusions will be communicated and discussed with to the counterpart.

During this meeting, the points that were raised during the walkdown and require clarification or additional information will be solved. Requests for additional information will be made, if necessary.

As before, this 'meeting' may be understood as a 'gathering' of the review team and the counterpart team, where separate 'meetings' can be run in parallel addressing different areas of the review.

Ideally, this meeting is held just after the plant walkdown.

A.2.4.2.5 Independent review report

Preparation of the independent review report is the final activity of the review. After the post-walkdown meeting, the review team will need to prepare the final version of the report and to discuss it internally, before sending it to the counterpart.

The suggested contents of the independent review report are given in the following section.

A.2.4.3. Reporting and documenting

A.2.4.3.1 Working notes

The working notes are the 'field notes' of the individual reviewers. The working notes typically contain the reviewer's comments, references to reviewed documents, interview notes, pictures, sketches, references to the IAEA publications, etc.

Typically, each reviewer develops his/her working notes all over the review process; adding information on a daily basis and following his/her own practice.

A.2.4.3.2 Daily reports

Daily reports provide a convenient way for recording the review team activities during the pre- and post-walkdown meetings with the counterpart and during the plant walkdown.

Primary information gathered by each reviewer is summarized in the form of these daily reports, and presented to the rest of the review team during daily team meetings. A new daily report is prepared each day by each reviewer, based on the working notes of the reviewer.

Daily reports are intended to be brief, itemized summaries. Typical contents of these daily reports are:

- General data: reviewer, review area, date.
- Identification of the counterpart staff, if applicable
- Summary of facts, concerns, good points, performance, gathered information, etc.
- Other remarks

A.2.4.3.3 Independent review report

This report is the main outcome of the review. It will usually consist of a main report with a number of appendixes covering specific activities, such as the meetings, the plant walkdown and any other ad-hoc developments.

A typical table of contents will include the following items:

(1) Introduction. Purpose and scope of the review.

(2) Review team members and qualifications.

(3) Description of the review:
   - Reviewed documents
   - Meetings with the counterpart
   - Plant walkdown
   - Documentation produced as a result of the review

(4) Results of the review in the different areas:

   Area A: Team composition

   Area B: Selection of applicable hazards

   Area C: Selection of the safety significant components

   Area D: Plant capacity assessment against applicable hazards

   Area E: Performance of fundamental safety functions

Area F: Risk estimates

Area G: Management system and documentation

(5) Overall assessment: conclusions and recommendations

Appendixes:

Summary of Pre-walkdown meeting
Walkdown report
Summary of Post-walkdown meeting
Specific analyses, if any

A.3 TECHNICAL GUIDANCE FOR CONDUCTING INDEPENDENT REVIEW

A.3.1. AREA A: TEAM COMPOSITION

A.3.1.1. Expectation

The composition of the team performing the vulnerability assessment and the personnel qualification meet the conditions defined in Section 9 of the present report.

A.3.1.2. Example of documents for the review

The composition and qualifications of the team performing the vulnerability assessment have to be given in the main report describing the assessment (see Section 8).

Additional documents can be used to demonstrate the qualifications and relevant experience of the key personnel, such as résumés, seminar attendance certificates, lists of professional publications, etc.

A.3.1.3. Evaluation

The review will focus on the following:

- Adequate capability and experience of the team as a whole in all areas required in Section 9 of the present report;
- Relevant participation of the plant's operations personnel;
- Adequate size of the team, given the type and number of applicable hazards and the specific plant/site configuration.

A.3.2. AREA B: SELECTION OF APPLICABLE HAZARDS

A.3.2.1. Expectation

The comprehensive list of hazards given in Section 2 of the present report has been used to define all potential external hazards.

A preliminary screening using the five criteria given in Section 2.3.2 has been used to eliminate from further consideration hazards that cannot have safety consequences in the site under study. Screening has been based on site specific information and a site walkdown.

Preliminary screening has been refined by using bounding analyses. Hazards whose worst-case scenarios will not have safety consequences have been screened out. In those cases, consequences have been computed using demonstrably conservative assumptions.

All credible combinations of not screened-out hazards have been identified, according to the criteria given in Section 2.2.

A.3.2.2. Example of documents for the review

The selection of applicable hazards and hazard combinations has to be contained in the main report describing the assessment (see Section 8), including the conclusions of the site walkdown used to confirm the selection.

Site specific configuration and near-regional data, which are the bases for the selection, are normally in the updated Safety Analysis Report and supporting documents.

A.3.2.3. Evaluation

The review will focus on the following:

- Updated site and near-regional data have been used, especially for human-induced hazards;
- Sensible application of preliminary screening criteria;
- Conservative assumptions are made for the bounding analyses, if any;
- Hazard selection has been validated by a site walkdown;
- All credible combinations of hazards have been identified and combinations are consistent with experience in other plants;
- Inconsistencies with plant design bases against external hazards, if any, have been identified and they are reported.

The review team needs to be aware that for some human activities, data can be completely obsolete after relatively short periods of time. This is the case, for example, of air routes (airways), the maximum size of hazardous material containers transported along roads or railways, chemicals stored in nearby industrial facilities, etc.

The review team needs to make sure that the counterpart has looked for instances where the currently available evidence might be in contradiction with the hazard strength considered in the design basis external events. It could happen, for example, that a design basis external event claim to have a return period much longer than the actual periodicity of the events recorded in the site or in the region.

A.3.3. AREA C: SELECTION OF THE SAFETY SIGNIFICANT COMPONENTS

A.3.3.1. Expectation

For each selected hazard, a Selected SSC List has been compiled. Alternatively, an enveloping list of SSCs, valid for all the selected hazards and credible hazard combinations is given.

The selected SSCs are enough to develop the fundamental safety functions defined in Section 3.1, under the initial plant conditions given for each applicable hazard in Table 2.

The selected SSCs include not only frontal systems, but also any required support system and all the structures providing shelter or support.

The selected SSCs include not only active components, but also passive components; that is, components which perform their intended functions without changing state.
The items in Selected SSC List correspond to individual physical items which can be located and inspected during a plant walkdown. For this purpose the list includes the necessary information, such

as: identification (plant tag), general description (e.g. horizontal pump, HVAC duct, auxiliary building) and location (room, building, area).

The required functionality or intended function is given for each item in the Selected SSC List.

A.3.3.2. Example of documents for the review

The process for selection of the safety significant components and the Selected SSC List has to be given in the main report describing the assessment (see Section 8).

Additional documents may be required for the review. Depending on the method used for the selection of SSCs, those documents may include:

- System description manuals;
- Piping and Instrumentation Diagrams;
- One-line Diagrams;
- Wiring and Schematic diagrams;
- Internal Events Level 1 PSA documentation (e.g. lists of initiating events, description of event trees, fault tree models, modelling assumptions, etc.);
- Plant operation procedures.

A.3.3.3. Evaluation

The review will focus on the following:

- Completeness of the Selected SSC List: all equipment, distribution subsystems and structures necessary to the performance of the fundamental safety functions have to be included;
- The way the fundamental safety functions are performed is consistent with plant procedures and with 'reasonable' expectations for operator actions;
- Required operator actions utilize only SSCs included in the list;
- Any exclusion of safety class SSCs from the list is justified;
- The items in list correspond to physical components, not to idealizations or to modelling assumptions (e.g. grouping) inherited from PSA models;
- The number of items in the list is consistent with experience from other similar plants.

The review team needs to make sure that the Selected SSCs are enough to perform the fundamental safety functions for the initial plant conditions applicable to each of the selected hazards.

A.3.4. AREA D: PLANT CAPACITY ASSESSMENT AGAINST APPLICABLE HAZARDS

A.3.4.1. Expectation

For each applicable hazard, the hazard strength threshold beyond which the fundamental safety functions could be jeopardized is determined.

The 'weak links' for each hazard are identified; that is, the SCCs that would likely fail first, given that the threshold is exceeded.

For each applicable hazard:

(1) A reference hazard strength has been defined;

(2) The 'as-is' condition of the plant has been used in the assessment;

(3) The plant response to the reference event has been computed (demand on SSCs);

(4) Demonstrably rugged or robust SSCs have been screened out from detailed capacity assessments;

(5) A plant walkdown has been performed to confirm screening and to identify potential spatial interaction issues;

(6) Detailed capacity calculations have been performed for screened-in SSCs;

(7) Plant level high confidence capacity has been computed from individual SSC capacities;

(8) 'Weak links' have been identified from individual SSC capacities.

For each credible hazard combination, the results for the individual hazards are checked for validity when the other hazards materialize simultaneously. That is, it is checked if the strength threshold obtained for a hazard still applies when the strength threshold for the other combined hazards is reached.

A.3.4.2. Example of documents for the review

The computation of the plant-level capacity for all selected hazards and the resulting 'weak links' have to be given in the main report describing the assessment (see Section 8).

Since the analysis for some of the hazards can be relatively involved, it is likely that the main report only provides a summary of the work performed and refers to a set of second level documents for the details. The second level documents typically include:

- Computations performed to obtain the plant response for the reference hazard strength (demand on the SSCs);
- Simple conservative capacity calculations, intended to confirm screening out of rugged SSCs;
- Capacity walk down documentation;
- Detailed capacity/fragility calculations;
- Plant-level capacity determination.

The review team may want to review a sample of these documents, including the capacity calculations performed for the identified 'weak links'.

A.3.4.3. Evaluation

Each hazard has its own specificities and its capacity assessment will likely need to be reviewed by a member of the team with some experience in capacity assessment against the hazard. For the most common hazards, Section 5 provides the main guidelines for the capacity assessments and reference documents for more detailed guidance. For hazards not included in Section 5, the general approach described in Section 4 is to be followed.

In general, the review will focus on the following:

- Plant and site configuration, together with other parameters used in the capacity assessment (e.g. material properties) correspond to the 'as-is' condition of the plant;
- The reference strength for the hazard has been defined larger than the design level strength;
- The reference hazard scenario is defined at a small exceedance probability (e.g. 16 % exceedance probability). That is, the parameters defining the reference event (loading

function, aircraft mass, response spectrum), which are conditional on the occurrence of the event, are defined at a small exceedance probability;
- Plant response to the reference event is computed using best estimate procedures, that is, with no conservative bias (median centred response);
- Material strength parameters and strength equations have a large exceedance probability (design-like strengths and equations);
- Simplified capacity calculations performed for screening purposes are based on conservative assumptions;
- Screening out of rugged components has been confirmed by a plant walkdown covering nearly all SSCs in the Selected SSC List, except for SSCs in a severe radiological environment;
- Plant housekeeping issues and 'easy-fixes' identified during the walkdown are reasonable and will be addressed by the plant so that they don't need to be considered for the capacity calculations;
- Potential spatial systems interaction have been investigated and introduced into the assessment;
- Detailed capacity/fragility calculations have been performed according to engineering good practice;
- Detailed capacity/fragility calculations give 'high confidence' capacity values (HCLPF), according to the guidance given in Sections 4 and 5;
- Identified weak links are consistent with reported previous experience in similar plants;
- Potential 'cliff-edge' effects have been investigated and reported, if applicable;
- When using the semi-probabilistic approach, plant-level capacity has been obtained using Boolean equations consistent with the way the Selected SSC List was developed.

A.3.5. AREA E: PERFORMANCE OF FUNDAMENTAL SAFETY FUNCTIONS

A.3.5.1. Expectation

For each applicable hazard, the response of the plant after the assumed failure of the 'weak links' identified in the previous activities has been investigated.

The time sequence of events following the failure of the 'weak links' has been determined up to reaching fuel damage. The SSCs governing the time sequence have been identified (i.e., any increase in the time-to-failure in those components would result in an increase in the time-to-fuel-damage).

The 'as-is' condition of the plant, current plant procedures, operations staff availability and the likely site conditions after the extreme event have been taken into account, including the possibility of using portable equipment stored on site.

A.3.5.2. Example of documents for the review

The assessment of performance of fundamental safety functions after failure of the 'weak links' has to be given in the main report describing the assessment (documentation requirements are given in Section 8).

Additional documents may be required for the review, including:

- System description manuals;
- Piping and Instrumentation Diagrams;
- One-line Diagrams;

- Wiring and Schematic diagrams;
- Technical specifications of key equipment;
- Plant operation procedures;
- Portable equipment stored on site, including location, technical specifications, procedures for deployment and use, etc.;
- Operations staff normally available on-site.

A.3.5.3. Evaluation

The review will focus on the following:

- Realistic conditions of the plant, site and near-regional area, after occurrence of the extreme event, have been taken into account;
- Time sequence of events is consistent with the current technical specification for systems and key equipment;
- Time sequence of events is consistent with plant procedures and with 'reasonable' expectations for operator actions;
- Time sequence of events is consistent with available experience for similar plants;
- When SSCs not included in the Selected SSC List developed for the plant capacity assessment (Section 3) are given credit in the time sequence, the functionality required to meet the intended function is demonstrated. That is, it is shown that after the extreme event, the SSCs are able to perform the required functions;
- SSCs for which an increase in the time-to-failure would lead to an increase in the time-to-fuel-damage, are highlighted and their role in the sequence is clearly explained and justified;
- Potential interaction between different units located at the site has been considered, whenever the interaction is possible (e.g. through shared systems).

A.3.6. AREA F: RISK ESTIMATES

A.3.6.1. Expectation

This part of the vulnerability assessment might have not been performed, since it is dependent on the availability of hazard assessments for the applicable hazards.

For those hazards with available hazard curves, the hazard curves have been obtained according to generally accepted practices.

For those hazards with available hazard curves, a mean plant-level fragility curve has been obtained using the plant-level high confidence capacity against the hazard obtained before.

Convolution of the mean plant level fragility with the mean hazard curve has provided the mean risk corresponding to the hazard (annual frequency of safety significant failure due to the hazard).

A.3.6.2. Example of documents for the review

The results of the available hazard assessments, the computation of the plant-level fragilities corresponding to the different hazards and the resulting risk estimates have to be given in the main report describing the assessment (see Section 8).

Additional documents may be required for the review, including:

- Documentation supporting the available hazard assessments;

A.3.6.3. Evaluation

The review will focus on the following:

- Hazard assessments have been performed using current generally accepted practices and updated sources of information;
- The hazard strength parameter used to define the hazard curves is the same used to define the plant-level fragility;
- The standard deviation values $ß_C$ used to develop the plant-level fragility curve are justified;
- The convolution of mean hazard and mean fragility has been performed with enough numerical accuracy.

It is important to note that in this area of review, the hazard curves will normally be considered as an input to the vulnerability assessment. Hence, the review team will only check that the curves have been obtained using generally accepted practices, as described in Section 7.2, and that the curves don't have evident inconsistencies or flaws. It is not the intent of this independent review to perform a detailed review of the hazard assessments, since for that purpose a very specialized team will normally be necessary for each of the most relevant hazards (earthquake, flood, tsunami, etc.).

A.3.7. AREA G: MANAGEMENT SYSTEM AND DOCUMENTATION

A.3.7.1. Expectation

Project documentation meets the requirements given in Section 8 of this document.

The assessment has been performed under a Management System complying with an international standard (e.g. ISO 9001).

Project documentation has been controlled. There is an updated list of project documents, documents are identified uniquely, and traceability of the different revisions of the same document has been maintained. Project documents are accessible for review and references cited along the documents are available.

An internal review process has been followed during the development of the project. The author and the reviewer of each document are different persons and they are clearly identified. The reviewer has adequate qualifications. Records to justify that the review has taken place are kept.

A.3.7.2. Example of documents for the review

Documents that may be required for the review include:

- Management System procedures and certificates of compliance with the relevant standards produced by an external organization;
- List of project documents;
  Records that justify the review process of a particular sample of documents;

A.3.7.3. Evaluation

The review will focus on the following:

- The documentation covers all information requested in Section 8 of this document;
- There is a clear hierarchy in which the project documents fit, from the top level report to the second and subsequent levels of supporting documents;

- The workflow is clearly reflected in the hierarchy and documents are readable and complete;
- Cited references are available;
- There exist records which justify that the internal review process has been implemented and traceability has been maintained.

APPENDIX B: SELF-ASSESSMENT QUESTIONNAIRE

B.1. INTRODUCTION

B.1.1. PREAMBLE

This appendix provides an aid to the application of the vulnerability assessment methodology described in the present report. The aid has the format of a series of questions which covers the key points needed to have a valid assessment. It is actually a self-assessment questionnaire intended to highlight the key points and to check the correct application of the methodology.

In a sense, the questionnaire provides an alternative reading of the methodology. Instead of focusing on the development details (how-to), it focuses on the intended outcome (what) and the requirements that have to be met. Hence, the questionnaire will prevent missing important issues or caveats.

The intended users of this appendix are the members of the team performing the assessment, especially those responsible for team coordination and internal review.

The questionnaire can be useful for preparation of the external independent review (Appendix A).

This appendix can also be helpful to further understand the methodology described in the main body of the report, since it provides an alternative reading of the main ingredients.

B.1.2. PURPOSE OF THE QUESTIONNAIRE

The purpose of the self-assessment questionnaire given in this appendix is to check the completeness of the vulnerability assessment performed according to this document, and the fulfilment of the main requisites.

B.1.3. SCOPE OF THE QUESTIONNAIRE

The questionnaire covers all areas of activity within the vulnerability assessment, namely:

- Team composition and personnel qualifications
- Selection of applicable hazards
- Selection of the safety significant components
- Plant capacity assessment for the selected hazards
- Performance of the fundamental safety functions
- Risk estimates
- Management system and documentation

The questions represent a minimum set of questions for the self-assessment process. They may not be considered as a comprehensive set of questions, covering every detail; rather, they are intended to call the attention of the development team about the key aspects of the methodology, and to start a reflection on how these aspects have been taken into account.

B.1.4. STRUCTURE OF THE APPENDIX

The rest of the Appendix comprises two additional sections.

Section B-2 provides a description of the questionnaire and indications on how to use it.

Section B-3 contains the questionnaire itself. The questionnaire is structured into seven different sections, corresponding to the areas of activity within the vulnerability assessment.

B.2. USE OF THE QUESTIONNAIRE

B.2.1. FORMAT OF THE QUESTIONNAIRE

The self-assessment questionnaire is given in Section B-3. Each question is contained in a single subsection of the section. The question is formulated using a short sentence, which summarizes the point under review.

The background and the intent of the question are given as a 'Commentary' to the question, which is included in the same subsection. Additionally, the commentary includes some guidance on how the question could be answered.

B.2.2. HOW TO ANSWER EACH QUESTION

The set of questions are intended to be a tour covering the key points of the vulnerability assessment methodology. Each question calls the attention to an important point of the methodology. To answer the question, a reflection about how this important point has been addressed will be needed.

This is the main goal of the questionnaire, namely, to provoke the reflection and, from this reflection, to find out if the intent of the methodology has been met.

After gathering the information and after the necessary considerations, the answer to the questions have tobe factual, that is, based on actual project documents and actual project activities. If any important point of the methodology is found to be missing, this has to be highlighted.

B.2.2. DOCUMENTATION

The self-assessment can be considered as an internal review. The answers to the questionnaire will normally be gathered in an internal review report.

It is suggested that the internal report follows the structure of the questionnaire given in Section B-3, grouping the questions into areas, and adding a final section to gather the conclusions of the review. This final section has to highlight those aspects which do not meet the intent of the vulnerability assessment methodology, if any was found.

B.3. QUESTIONNAIRE

B.3.1. AREA A: TEAM COMPOSITION

B.3.1.1. Adequate size and capabilities

Question:

Is the team performing the vulnerability assessment able to carry out this assignment?

Commentary:

The team have to meet the requirements given in Section 9, and be able to develop the project in a reasonable time. For a typical plant, a reasonable time is about 18 months. This time can be much longer when the development team lacks adequate training and experience.

The answer to this question requires going to Section 9 and checking that the requirements given there are met for the specific conditions of the plant and the expected applicable hazards.

The team is multidisciplinary, requiring systems engineers, operations personnel and capability engineers. Since the languages of these disciplines are very different, the team requires some members able to understand all these languages and, therefore, facilitate internal communication.

Engineering judgement plays a key role in the application of the methodology. Hence, the team have to include experienced engineers, able to make use of judgement in order to make the assessment as much cost-effective as possible. Project decisions based on judgement will be validated by the independent review (Appendix A).

The ideal background for the team members is having training and experience in seismic margin assessments or in the safety assessment of existing facilities against any other external hazard.

For a typical plant, for which an internal event Level 1 PSA is available, and with about half a dozen external hazards to be studied in detail, a development team consisting of ten people may be adequate. Such a team would have a steering committee, with three experienced engineers, supported by two systems engineers, one operations staff and four capability engineers (mechanical, structural).

B.3.1.2. Participation of plant's personnel

Question:

Does the interaction of the team with plant's personnel cover all necessary issues?

Commentary:

The vulnerability assessment has to be performed for the 'as-is' condition of the plant, that is, for the as-built, as-maintained and as-operated conditions. Interaction with plant's personnel is essential for identifying those conditions. It is not uncommon that the updates of the documents defining the plant configuration are released significantly after the actual changes are introduced in the plant.

In addition, the selection of safety significant components (Section 3) needs to correspond to the likely actions taken by trained operators under the assumed plant initial conditions (Table 2). Hence, the selection of the components has to be checked by plant's personnel, therefore avoiding the use of 'smart' alignment of systems that would never be used in practice.

In the same way, interaction with plant personnel is required to validate the time sequence of events after failure of the 'weak links' against the applicable hazards.
Hence, during the vulnerability assessment, a continuous interaction of the team with the appropriate plant's staff is required and the appropriate persons within the team have to be identified.

The answer to this question has to be based on the amount of interaction of the team with plant designated staff. Key checkpoints are as follows:

- Identification of documents that better define the 'as-is' condition of the plant;
- Validation of the Selected SSC List(s) (Section 3);
- Validation of the time sequences after the 'weak links' fail (Section 6).

B.3.2. AREA B: SELECTION OF APPLICABLE HAZARDS

B.3.2.1. Updated site and near-regional data

Question:

Is the information used for selecting the applicable hazards up to date?

Commentary:

The site and regional data used for the selection of applicable hazards needs to be reasonably up-to-date. As an average, the data is expected be updated every ten years. Data older than ten years have to be considered to be suspicious of being obsolete.

The answer to this question has to be based on a review of the sources of data used for the identification of applicable hazards, and the dates at which the data were produced. When the sources are older than 10 years, then a justification of the validity of the data will be needed.

B.3.2.2. Sensible application of preliminary screening criteria

Question:

Is preliminary screening of hazards based on adequate application of the screening criteria?

Commentary:

Preliminary screening of hazards is based on the use of five qualitative criteria. Meeting at least one of the criteria provides the basis for screening out a hazard.

Since the screened-out hazards will be eliminated from any further consideration, the application of the criteria has to be far from being controversial. It needs to be based on facts. Speculative reasoning about whether or not a criterion is met has to be avoided. When a hazard is screened out, it has to be obvious that at least one of the criteria is met.

The answer to this question has to be based on the review of the criteria used for eliminating the screened out hazards. The reviewer is to make sure that at least one criterion was met, based on factual information and arguments that can hardly be challenged.

B.3.2.3. Conservatism in the bounding analyses

Question:

Are bounding analyses based on demonstrably conservative assumptions?

Commentary:

Bounding analysis used to show that a particular hazard cannot have relevant safety consequences at a site are intended to be simple calculations based on conservative assumptions. The analyses have to be simple to understand, simple to check and they has to use assumptions whose conservatism is simple to demonstrate.

When those three conditions cannot be met, that is, when for instance very complicated analyses are needed, it is likely that the hazard cannot be screened out at this level.

As with the preliminary screening, the goal is to have clear arguments, in this case based on simple calculations, to justify the elimination of a hazard from any further consideration.

The answer to this question needs to be based on the review of the bounding analyses used to screen out hazards. The reviewer is to make sure that the analyses are simple, based on assumptions that are easily shown to be conservative, and that calculations are correct.

B.3.2.4. Identification of all credible combinations of hazards

Question:
Have all credible combinations of hazards been considered?

Commentary:

Table 1 provides a comprehensive list of potential hazards. However, some of these hazards can materialize simultaneously, since they could have a common physical origin. This is the case, for example, of the earthquake hazard and the tsunami hazard.

It is unusual that the events coming out from these hazards occur exactly at the same time, since the time scales of the phenomena are normally different. For example, the seismic waves will normally reach the site earlier that the tsunami waves, so that the ground shaking will be over when the tsunami arrives.

In any case, credible combinations of hazards have to be considered, since the ability of the plant to respond to the second hazard could have been affected by the first hazard.

The answer to this question needs to be based on the conditions given in Section 2.2 for identifying hazard combinations, and their application to the set of hazards remaining for further study after the preliminary screening and the bounding analyses.

B.3.2.5. Potential inconsistencies with plant design bases

Question:

Are the plant design bases consistent with the updated information about applicable hazards?

Commentary:

It could happen that plant design bases for external events were established a long period of time ago, based on the information and the state of practice at that time.

In performing the assessment, the updated information could show that the design bases are not consistent with recently observed events. For example, maximum recorded gust wind speeds could have been close to the design values in several years during the last decade, whereas the design gust wind speed is supposed to have a return period of 100 years.

This kind of inconsistencies will not affect the vulnerability assessment, since the assessment is intended to find the 'weak links' in the 'as-is' condition of the plant. A lower design basis will result in a lower plant-level capacity against a particular hazard, if the design against other hazards does not provide additional margin.

However, even though they do not affect the assessment, these findings are very valuable and needs to be reported.

The answer to this question needs to be based on the comparison of the plant design bases with the updated information about the applicable hazards.

B.3.3. AREA C: SELECTION OF THE SAFETY SIGNIFICANT COMPONENTS

B.3.3.1. Completeness of the Selected SSC List(s)

Question:

Does the Selected SSC List include all required structures, systems and components?

Commentary:

The Selected SSC List has to include all equipment, distribution subsystems and structures necessary to the performance of the fundamental safety functions under the initial conditions given in Table 2 for each selected hazard. The list needs to include not only active components, but also passive components; that is, components which perform their intended functions without changing state.

The initial conditions given in Table 2 correspond to low-medium severity scenarios typically already taken into account in the design or in subsequent safety assessments. Hence, the Selected SSC List will likely include all safety classified systems, structures and components, with some exceptions.

If the success path approach is used (Section 3.2), the Selected SSC List will not include those safety SSCs that are not credited for the selected path. However, when two alternative success paths are required, then very few safety systems, structures and components will be left out of the list.

The answer to this question needs to be based on the identification of frontal systems included in the list and on the verification that the fundamental safety functions can be accomplished by these systems. Then, the presence of the support systems in the list has to be checked, together with the structures shielding or supporting all the systems and components.

B.3.3.2. Consistency with plant procedures and 'reasonable' operator actions

Question:

Is the Selected SSC List consistent with plant operation procedures?

Commentary:

The list has to include the systems that a trained operator, following plant procedures, will use to maintain the fundamental safety functions in case of the initial conditions given in Table 2 for each selected hazard. The Selected SSC List has not to be based on 'smart' or complicated alignment of plant systems that, even if possible, would never be used in practice.

The answer to this question needs to be based on a review of plant operation procedures corresponding to the initial plant conditions given in Table 2. Frontal systems and required support systems corresponding to the given initial conditions need to have been included in the list.

B.3.3.3. Inclusion of safety class SSCs

Question:

Are the exclusions from the list of safety class SSCs justified?

Commentary:

This question is complementary to question in Section B-3.3.1. The idea is that the Selected SSC List will normally include most of safety class structures, systems and components. The exclusion of some

safety class SSCs is possible, based on the diversity of systems available to accomplish the same safety function. However, the exclusion can also be the result of a mistake during the systems analysis.

The answer to this question has to be based on the identification of all plant safety systems, a review of the intended functions of the excluded systems, and the confirmation that, for the given plant initial conditions, these functions are covered by other safety systems already taken into account in the preparation of the list.

B.3.3.4. Items in the Selected SSC List(s) correspond to physical components

Question:

Are the items in the Selected SSC List physical entities?

Commentary:

The resulting Selected SSC List needs to contain only individual physical items, which could be located and inspected in the plant. Hence, any grouping or idealization of components have to have been unfolded into individual physical components.

This question is a warning against directly including in the list items that come from PSA modelling idealizations, with no direct correspondence to physical plant items. PSA modellers sometimes use idealizations of SSCs which cannot be easily associated to physical equipment in the plant (e.g. group of HVAC dampers considered a single PSA model item or contacts of the same relay modelled as separate items). Those idealized PSA items are not usable in the capacity assessments.

The answer to this question needs to be based on a review of the Selected SSC List, to check that it complies with the requirements given in Section 3.4.

B.3.3.5. Number of SSC in the list(s) is consistent with experience

Question:

Is the number of items in the Selected SSC List(s) consistent with experience?

Commentary:

According to the experience of capacity assessment against external hazards, for a typical Light Water Reactor plant, the number of items in the Selected SSC List is in the order of hundreds and usually less that one thousand.

Obviously, the number of items depends on how the SSCs are organized within the list. The estimate for the number of items given in the previous paragraph is based on the following practices:

- Different sub-components of the same equipment item are grouped into a single item, as far as the relevant failure modes can be studied considering the overall item. This is sometimes called the ‘rule-of-the-box’.
- Manual valves and manual dampers are not included as separate items, but considered part of the pipe or duct in which they are mounted. The same applies to valves or dampers equipped with an actuator but do not need to be actuated for accomplishing the fundamental safety functions.
- Distribution subsystems (piping, HVAC ducts, cable trays and conduits) are listed by plant areas, and supports are not listed separately.
- Each structurally independent building or civil structure is considered a single item.

A list with an extra number of items will not affect the final results of the vulnerability assessment: the same weak links will eventually be identified. However, the extra number of items will result in an additional expenditure of time and resources.

On the other hand, when the list is significantly smaller than in other similar plants, it is possible that the list is missing important items. In this case, the quality of the vulnerability assessment will be affected, since some of the weak links could have been missed.

The answer to this question needs to be based on a review of the Selected SSC List, to check that the criteria for organizing the items are similar to those given above. In this case, for seismic hazard, any list with less than 250 items will need to be investigated in detail for missing components. For a typical plant and using again the seismic hazard, any list with more than 1500 items and built following the practices above, will probably be including items not strictly required for performing the fundamental safety functions.

B.3.4. AREA D: PLANT CAPACITY ASSESSMENT AGAINST APPLICABLE HAZARDS

B.3.4.1. 'As-is' configuration has been used

Question:

Does the capacity assessment correspond to the 'as-is' condition of the plant?

Commentary:

The capacity assessment against applicable hazards has to be performed for the 'as-built', 'as-maintained' configuration of the plant. This refers not only to the physical, geometrical configuration, but also to the properties of the materials used for capacity calculations. In addition, good maintenance practices allow less conservative assumptions to be made when assessing capacities.

Hence, the most updated documentation has to be used for the capacity assessment and, the correspondence of the documentation with the actual plant condition needs to be checked during the plant walkdown and reported in the walkdown documents.

In addition, significant degradation (e.g. corrosion, concrete cracking, etc.) found during the walkdown has to be recorded and taken into account in the capacity calculations.

The answer to this question needs to be based on a review of the references used as input data to the capacity assessment, which has to be updated documents, and on verification that the correspondence with actual plant condition has been checked during the plant walkdowns.

B.3.4.2. Reference strength of the applicable hazard(s) exceeds design level

Question:

Have the reference hazard strengths been set at adequate levels?

Commentary:

The reference event for each selected hazard is a working tool. If a deterministic approach is followed, SSC preliminary (conservative) capacities are compared with the demand corresponding to the reference event and those SSC with a capacity larger than this demand are screened out from further assessment. Detailed capacity calculations are performed only for screened-in SSCs.

If a semi-probabilistic approach is followed, the reference event is used to compute the plant's response, which is required to relate the 'free field' event with the demand at the location of the SSCs.

When the response might be severely non-linear and the final plant-level capacity is significantly different from the reference event, then the capacity calculations might need to be re-done.

The reference event may be either selected by the analyst or prescribed by the Regulator of the Member State. Ideally, the reference hazard strength has to be set slightly above the expected plant-level capacity.

For plants which have been designed for a particular hazard, it is usually reasonable to set the reference event above 1.25-1.50 times the design hazard strength.

The answer to this question needs to be based on a review of the selected reference event(s) and a comparison with the design basis events or with plant-level capacities reported to similar plants.

B.3.4.3. Rules of CDFM method are met

Question:

If CDFM method has been used for computing HCLPF capacities, are the rules of CDFM met?

Commentary:

This question refers to the case in which CDFM method has been used. The use of other methods is not precluded.

HCLPF capacity of a SSC is conventionally defined as the hazard strength which results in 1% probability of failure in the SSC.

The CDFM method was developed for efficient computation of HCLPF capacities in seismic safety assessments. The rules for application of the method are given in Table 3.

CDFM rules for computing HCLPF capacity are based on the values of uncertainties in computing plant response and in assessing component strength normally found in seismic evaluations. When using a log-normal fragility model, this corresponds to β_R = 0.2-0.4 and β_S = 0.2-0.5, respectively.

In the present report, it is assumed that the CDFM method will provide acceptable HCLPF capacity results for other hazards different from the seismic hazard. This is believed to be conservative, except for hazards in which the response calculation (i.e., the demand on the SSCs derived from the reference event) has associated uncertainties much larger than in the seismic case. This could be the case, for example, when the effects of very large aircraft impact are considered. In those cases, the analyst will need to adapt published fragility results to his/her specific analyses.

The answer to this question needs to be based on a review of the capacity calculation criteria used for simple and for detailed analyses. The criteria have to meet the requirements given in Table 3. For capacity calculations in which the CDFM method has not been considered applicable, specific rules to compute HCLPF capacity has to have been used.

B.3.4.4. Conservative assumptions have been used for simplified capacity calculations

Question:

Are simplified calculations used for screening-out SSCs demonstrably conservative?

Commentary:

Typically, once the demand on the SSCs is known from the plant response analysis, a large number of simplified capacity calculations are performed, trying to bound the capacity of the SSC above the level

from which it can be assumed that the SSC will not be a weak link. Capacity is checked for all relevant failure modes and the relevant failure modes are identified based on experience and judgement.

Since the SSCs shown to be robust enough will be screened out from further assessment, it is important that the bases for the capacity calculations at this stage are conservative and that the calculations themselves are simple and easy to verify. Otherwise, relevant weak SSCs could be screened out at this level. Therefore, the simplified capacity analyses have to be simple to understand, simple to check and they have to use assumptions whose conservatism is simple to demonstrate.

The answer to this question needs to be based on the review of the analyses used to screen out SSCs. The reviewer is to make sure that the analyses are simple, based on assumptions that are easily shown to be conservative and that calculations are correct.

B.3.4.5. Plant walkdown has been used to confirm screening of rugged SSCs

Question:

Has the screening-out of robust SSCs been confirmed by a plant walkdown?

Commentary:

Once the conservative capacity calculations have been carried out, the screening out of rugged components have to be confirmed during a plant walkdown.

The answer to this question needs to be based on a review of the screened out SSCs, to make sure that the walkdown confirmed the following points:

- Correspondence between documents used as input and actual configuration of the SSC.
- Absence of significant degradation (e.g. corrosion, loss of material, cracking, etc.).
- Absence of spatial systems interaction with other SSCs located nearby, whose failure could cause the failure of the SSC.

When any of these conditions is not met, the capacity calculations are invalidated and they have to be revised according to the new information.

B.3.4.6. Commitment to implement 'easy-fixes' and housekeeping issues

Question:

Is there a commitment to implement 'easy-fixes' and address housekeeping issues?

Commentary:

After the plant walkdown, it is fairly common that the capacity engineers have compiled a list of simple-to-do actions that, if addressed, can be used to screen-out a number of SSCs from further assessment.

Normally, the vulnerability assessment proceeds under the assumption that those actions are going to be implemented. However, this assumption has to be validated by a commitment made by the plant to implement those actions. Otherwise, the vulnerability assessment could produce optimistic results.

The answer to this question has to be based on a review of the 'easy-fixes' and housekeeping issues identified during the capacity walkdown, and the verification that any issue for which there is no commitment by the plant has been carried on to the detailed capacity calculations.

B.3.4.7. Spatial systems interaction has been considered

Question:

Has spatial systems interaction been considered within the capacity assessment?

Commentary:

Spatial systems interaction is an essential issue within the capacity assessment (Section 4.4.4.2). Interaction could be the governing failure mode for an SSC, but this issue can only be addressed during the plant walkdown.

The possible interaction issues vary from one hazard to the other, even though the nature of them can almost always be classified into three categories:

- Failure and falling
- Proximity
- Spray and flooding

The answer to this question needs to be based on the review of the capacity walkdown procedures and documentation. The procedures have to include the need for investigation of the possible interactions, giving guidance on what to look for during the walkdown and what may be significant interactions. Walkdown documentation has to have reported on the presence or absence of interaction issues.

B.3.4.8. Detailed capacity/fragility calculations according to current state of practice

Question:

Have the detailed capacity calculations been performed according to good practice?

Commentary:

Detailed calculations have to produce HCLPF capacity values for use in the following phase of the vulnerability assessment. The calculations have to correspond to the all failure modes identified after the capacity walkdown. The philosophy of the CDFM method would normally be applied to compute the HCLPF capacity for mechanical/structural failure modes.

At this stage, the calculations might be relatively sophisticated, since the SSCs reaching this stage are likely to be the weak links against the considered hazard. No specific rules can be given, since the kind and scope of the calculations can be very different from one case to the other.

The answer to this question needs to be based on the detailed review of the calculations. They have to have been performed according to good practice. The accuracy of the results have to be checked and they have to be consistent with previous experience.

B.3.4.9. Potential 'cliff-edge' effects have been investigated

Question:

Have potential 'cliff-edge' effects been taken into consideration?

Commentary:

The potential for a 'cliff edge' effect have to be suspected when any of the following conditions takes place:

- A significant number of individual weak links have a similar capacity;
- There is a weak link that corresponds to a generalized failure mode, affecting many SSCs at the same time. Examples of generalized failure modes are widespread soil failures, the overtopping of a flood protection barrier, or structural failure of a safety related building.

After performing the detailed capacity calculations, the analyst will have a ranking of SSC capacities. SSCs with the lowest capacities will provide the weak links against the selected hazards.

The answer to this question needs to be based on the review of the ranking of SSC capacities to find out if there is a threshold hazard strength beyond which a widespread failure of SSCs could be expected.

B.3.4.10. Plant-level capacity has been obtained

Question:

Has the plant-level capacity been obtained for each applicable hazard?

Commentary:

Plant-level high confidence (HCLPF) capacity against applicable hazards is the main result of the vulnerability assessment. These capacities provide the hazard strength under which no safety important consequences are to be expected.

When a deterministic approach has been followed, the plant-level HCLPF capacity is conservatively assumed to be the HCLPF capacity of the weakest SSC in the Selected SSC List.

When a semi-probabilistic approach is used, individual HCLPF capacities are propagated through the Boolean expressions until obtaining the plant-level HCLPFs.

The answer to this question needs to be based on the review of how the plant-level capacities have been computed for each hazard, how they are related with the individual SSC capacities and how they are reported in the project documentation.

B.3.5. AREA E: PERFORMANCE OF FUNDAMENTAL SAFETY FUNCTIONS

B.3.5.1. Realistic conditions after extreme event have been considered

Question:

Has the assessment taken into consideration the site conditions after the extreme event?
Commentary:

The assessment of performance of the fundamental safety functions, after the weak links fail, has to consider the foreseen site and near-region conditions caused by the extreme events. This includes potential site devastation, difficulties for access to some plant areas, potential loss of emergency lightening, stress of operators, lack of personnel, etc.

The time progression of events after the weak links fail needs to be determined bearing in mind that the conditions will be far from normal operation conditions. The plant walkdown will help identify what the expected conditions would look like.

Before starting this part of the vulnerability assessment, the expected site and near-regional conditions have to be identified for each applicable hazard and taken as input data for this last part of the assessment.

The answer to this question needs to be based on the review of the expected conditions for each hazard and on their bases, normally taken from the capacity walkdown documentation.

B.3.5.2. Time sequence of events consistent with procedures and technical specifications

Question:

Is the time sequence of events consistent with plant procedures, available resources and technical specifications?

Commentary:

After failure of the weak links in the Selected SSC List, a chain of failures will start, eventually leading to fuel damage. A sequential and progressive loss of the remaining systems is postulated, once their operation is no longer possible according to the 'as-is' condition of the plant (e.g. batteries depleted, tanks emptied, reservoirs depleted, etc.).

If the failure of the weak links does not lead to fuel damage, then those weak links need to have not been included in the Selected SSC List, since they were not actually required to provide the fundamental safety functions.

There are two key results coming out from the identified sequence of events:

- The time at which the failure of the systems takes place;
- The individual SSCs governing the failure of the systems.

Both results depend on the technical specifications of the SSCs and on the plant procedures related with their operation and maintenance. For instance, the time at which a set of batteries run out depends on the technical characteristics of the battery cells and on the loads connected to the batteries according to the plant procedures.

The answer to this question needs to be based on the review of the time sequences defined for each applicable hazard and the verification that the given times are in accordance with technical specification and operation procedures. These checks have to be performed not only for SSCs identified as governing the times, but also for the SSCs that are found to be not governing.

B.3.5.3. Credit only to SSCs with capacity larger than plant-level capacity

Question:

Has credit been given only to the SSCs whose capacity is larger than the plant-level capacity?

Commentary:

In assessing the performance of the fundamental safety functions after the weak links fail, the analyst could give credit to systems and components not included in the Selected SSC List, as far as they are available on site (e.g. movable equipment).

However, in that case, the analyst has to demonstrate that the functionality required to meet the intended function is available. That is, the analyst will need to show that the extreme event has not damaged the credited SSC and that, after the extreme event, the credited SSCs will able to perform the required functions.

The answer to this question needs to be based on the review of SSC not included in the Selected SSC List, which are nevertheless credited for the performance of the fundamental safety functions. The high confidence capacity (HCLPF capacity) of these components, given the actual configuration,

qualification and on-site storage conditions, has to be shown to be larger than the plant-level capacity. The plant-level capacity is given by the weak links identified in the previous stages of the assessment.

B.3.5.4. SSCs governing time-to-fuel-damage are identified

Question:

Have the SSCs governing the time-to-fuel-damage been identified for all applicable hazards?

Commentary:

As mentioned above, a key result of the assessment is the set of SSCs that govern the time sequences. In a sense, these are the 'weak links' from a functional point of view, since an increase in the time-to-failure in any of these SSCs would lead to an increase in the time-to-fuel-damage for each particular hazard.

These SSCs have to be highlighted and their role in the sequence is to be clearly explained and justified.

The answer to this question needs to be based on the review of the sequences identified for each applicable hazard. The reviewer has to make sure that sequences are complete, that all governing SSCs are identified and that their role is justified.

B.3.5.5. Potential interaction between different units has been considered

Question:

Have the interactions between co-located units been taken into account?

Commentary:

At some multi-unit sites, after the weak links fail, there exists the possibility of one unit inducing functional failures in other adjacent unit. This is the case, for example, of two units sharing systems or buildings.

In those cases, the consequences in one unit derived from the failure of weak links in other unit needs to be part of the assessment of performance of fundamental safety functions.

Note that experience shows that co-located units are never identical from an external hazard point of view, even in the case of supposedly 'twin' units. As a consequence, the weak links at one unit can be different or can have different HCLPF capacities from the weak links in the other units. Hence, failures in the co-located units will not take place for exactly the same hazard strength and they could correspond to different SSCs.

The answer to this question needs to be based on the analysis of the physical connections between different units and on the assessment of the consequences of the failure of the weak links in each unit on the performance of the safety functions in the other units.

B.3.6. AREA F: RISK ESTIMATES

B.3.6.1. Hazard assessments performed using accepted practices

Question:

Have the hazards been assessed using current state-of-practice procedures?

Commentary:

Hazard assessment procedures are constantly evolving as a result of scientific development and substantial improvement of technologies for Earth monitoring and for recording natural events.

Thus, in some cases, hazard assessments carried out only 20 years ago could be completely obsolete in the light of the current state-of-practice and they might be missing important phenomena.

In the case of external events, the uncertainty in risk estimates comes mainly from the hazard assessment, not from the plant capacity (fragility) assessment. Acceptable risk estimates require the best possible hazard assessments. Otherwise, risk estimates could have such a large level of uncertainty that their use would be misleading.

The answer to this question needs to be based on the review of the basis for the available hazard assessments and on the comparison with the current state-of-practice.

B.3.6.2. Uncertainty in plant-level fragility curve is justified

Question:

Has the uncertainty in plant-level fragility been reasonably estimated?

Commentary:

When a log-normal model is used for plant-level fragility, the mean fragility curve required for computing a mean risk estimate is defined by a plant-level HCLPF capacity and a logarithmic standard deviation $ß_C$. The latter is an overall measure of uncertainty, which combines aleatoric and epistemic uncertainties.

When the semi-probabilistic approach has been followed, Boolean equations can be used to propagate component mean fragilities up to the plant-level fragility. In that case, uncertainty at the plant level comes out the combined uncertainties at the component level fragilities.

When the deterministic approach has been followed, only the plant-level HCLPF capacity will be available and the corresponding uncertainty parameter $ß_C$ will need to be estimated. Since the mean fragility curve will be anchored to the HCLPF capacity value, the larger the $ß_C$ parameter the lower will be the mean risk estimate. In a seismic assessment, $ß_C$ can hardly be less than 0.25-0.30, when all sources of uncertainty are considered [49].

When assessing risk against external events, in the current state of the technology, usually most of the uncertainty comes from the hazard assessment, not from the capacity assessment. Hence, in general, risk metrics will be relatively insensitive to uncertainty in capacity determination, as far as the capacity is obtained using common practice procedures.

The answer to this question needs to be based on the review of the plant-level mean fragility curves for the applicable hazards. Assuming a log-normal model, the $ß_C$ parameter can be obtained from the HCLPF capacity (1% conditional probability of failure) and the median value (50% conditional probability of failure). When the mean fragility has been anchored to the HCLPF capacity, then any $ß_C$

parameter lower than 0.25-0.30 will be considered to be conservative. Values above this threshold will need to be justified.

B.3.6.3. Hazard-fragility convolution carried out with enough accuracy

Question:

Has the convolution of mean hazard and mean fragility been performed with enough accuracy?

Commentary:
Convolution of mean hazard and mean fragility to obtain the mean risk estimate is performed numerically (Section 7.4). The results can strongly depend on the discretization of the hazard curves and on the accuracy of the numerical integration.

The answer to this question needs to be based on a verification of the final results, usually by assessing the sensitivity to the discretization and the number of points used for computing the integrals.

B.3.7. AREA G: MANAGEMENT SYSTEM AND DOCUMENTATION

B.3.7.1. Required documentation has been produced

Question:

Does the project documentation accurately describe the process and the results?

Commentary:

Minimum requirements for project documentation are given in Section 8.

Ideally, the documents will cover all project activities and a hierarchy will have been established at each activity, from the more general (summary) document to the documents giving the details.

The answer to this question needs to be based on a review of the documents produced by the project team and on the verification that they comply with the minimum requirements given in Section 8.

B.3.7.2. Documentation is controlled and cited references are available

Question:

Are project documents controlled and cited references available?

Commentary:

Normally, the project will be developed under a Management System complying with an international quality standard. The Management System will include requirements for documentation control.

Minimum documentation control is provided by a list of project documents in which each document is identified, with title, internal code, date, author, reviewer and current status.

An important aspect, which facilitates the review, is the availability of the references cited in the project documents.

The answer to this question needs to be based on the verification that the Management System requirements regarding documentation are met.

B.3.7.3. Internal review has been carried out

Question:

Has the project gone through internal review?

Commentary:

Normally, the project will be developed under a Management System complying with an international quality standard. The Management System will include requirements for internal review.

The expectation is that an internal review process has been followed during the development of the project, with the following main attributes:

- The author and the reviewer of each document are different persons and they are clearly identified;
- The reviewer has adequate qualifications;
- Records to justify that the review has taken place are kept.

The answer to this question needs to be based on the verification that the Management System requirements regarding internal review are met.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Action Plan on Nuclear Safety, Vienna (2011)

[2] EUROPEAN NUCLEAR SAFETY REGULATORS GROUP, Stress Tests Performed on European Nuclear Power Plants as a Follow-up to Fukushima Accident: Overview and Conclusions, Presented to ENSREG by the Peer Review Board, April (2012).

[3] EUROPEAN NUCLEAR SAFETY REGULATORS GROUP, Stress Tests Performed on European Nuclear Power Plants as a Follow-up to the Fukushima Accident: Compilation of Recommendations and Suggestions from the Review of the European Stress Tests, Draft prepared by the Peer Review Board for ENSREG, July, (2012).

[4] U.S. NUCLEAR REGULATORY COMMISSION, Near-Term Report and Recommendations for Agency Actions Following the Events in Japan, SECY-11-0093, Washington DC, July 12, (2011).

[5] U.S. NUCLEAR REGULATORY COMMISSION, Request for Information Pursuant to Title 10 of the Code of Federal Regulations 50.54(f) Regarding Recommendations 2.1, 2.3 and 9.3, of the Near-Term Task Force Review of Insights from the Fukushima Dai-Ichi Accident, Letter to all power reactor licensees and holders of construction permits in active or deferred status, with enclosures, Washington DC, March 12, (2012).

[6] G. CHAI, Improvement Measures for NPPs in China in Light of Fukushima Accident, in Protection against Extreme Earthquakes and Tsunamis in the Light of the Fukushima Daiichi Nuclear Power Plant, Vienna, 4-7 September (2012).

[7] CANADIAN NUCLEAR SAFETY COMMISSION, CNSC Integrated Action Plan on the Lessons Learned from the Fukushima Daiichi Nuclear Accident, Ottawa, August 2013.

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Report on Protection against Extreme Earthquakes and Tsunamis in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, International Experts Meeting, 4-7 September 2012, Vienna, (2012).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Report on Evaluation of Nuclear Power Plant Design Safety in the Aftermath of the Fukushima Daiichi Accident, Technical Meeting, 26-29 August 2013, Vienna, (2013).

[10] CONVENTION ON NUCLEAR SAFETY, Final Summary Report, in *2nd Extraordinary Meeting of the Contracting Parties to the Convention on Nuclear Safety*, Vienna, 27-31 August (2012).

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

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.15, IAEA, Vienna (2009).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary - Terminology Used in Nuclear Safety and Radiation Protection, IAEA, Vienna (2007).

[14] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Safety of New NPP Designs, WENRA, Reactor Harmonisation Working Group, March (2013).

[15] U.S. NUCLEAR REGULATORY COMMISSION, PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, Washington DC, January (1983).

[16] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sa-2009, New York (2009).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No.4, Technical Guidance, Vienna (2007).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Aspects of Nuclear Power Plants against Human Induced External Events: Margin Assessment, Safety Reports Series No. 86, Vienna (2017).

[19] ELECTRIC POWER RESEARCH INSTITUTE, A Methodology for Assessment of Nuclear Power Plant Seismic Margin, Report EPRI NP-6041-SL, Rev. 1, Palo Alto, California (1991).

[20] U.S. NUCLEAR REGULATORY COMMISSION, An Approach to the Quatification of Seismic Margins in Nuclear Power Plants, Report NUREG/CR-4334, Washington DC (1985).

[21] 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 DC June (1991).

[22] U.S. NUCLEAR REGULATORY COMMISSION, Generic Issue 199 (GI-199) - Implications of Updated Probabilistic Seismic Hazard Estimates in Central and Eastern United States on Existing Plants - Safety/Risk Assessment, ML1000270639, Washington, DC (2010).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3 (Rev. 1), IAEA, Vienna (2016).

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-9, IAEA, Vienna (2010).

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Geotechnical Aspects of Site Evaluation and Foundations for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-3.6, IAEA, Vienna (2004).

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, WORLD METEOROLOGICAL ORGANIZATION, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-18, IAEA, Vienna (2011).

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Volcanic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-21, IAEA, Vienna (2012).

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-3.1, IAEA, Vienna (2002).

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

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

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Extreme External Events in the Design and Assessment of Nuclear Power Plants, IAEA TECDOC-1341, Vienna (2003).

[32] U.S. NUCLEAR REGULATORY COMMISSION, Evaluation of External Hazads to Nuclear Power Plants in the United States, NUREG/CR-5042, Washington DC, December (1987).

[33] U.S. NUCLEAR REGULATORY COMMISSION, Evaluation of External Hazards to Nuclear Power Plants in the United States - Seismic Hazard, NUREG/CR-5042, Supplement 1, Washington DC, April (1988).

[34] U.S. NUCLEAR REGULATORY COMMISSION, Evaluation of External Hazards to Nuclear Power Plants in the United States - Other External Events, NUREG/CR-5042, Supplement 2, Washington DC, February (1989).

[35] U.S. DEPARTMENT OF ENERGY, Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities, DOE-STD-1020-94, Washington DC, April (1994).

[36] LAWRENCE LIVERMORE NATIONAL LABORATORY, Design and Evaluation Guidelines for Department of Energy Facilities Subjected to Natural Phenomena Hazards, UCRL-15910, Lawrence Livermore National Laboratory, Livermore, California, June (1990).

[37] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, WENRA Reactor Safety Reference Levels, WENRA, January (2008).

[38] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, WENRA Safety Reference Levels for Existing Reactors / Update in Relation to Lessons Learned from TEPCO Fukushima Dai-Ichi Accident, Draft document, WENRA, 20 November 2013.

[39] NUCLEAR ENERGY AGENCY, Probabilistic Safety Analysis (PSA) of Other External Events than Earthquake, NEA/CSNI/R(2009)4, Organisation for Economic Co-operation and Development, Paris, March (2009).

[40] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Extreme Earthquakes and Tsunamis in the Light of the Accident at the Fukushima Dai-ichi Nuclear Power Plant, International Experts Meeting, 4-7 September, Vienna, September (2012).

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

[42] U.S. NUCLEAR REGULATORY COMMISSION, Guidance on Performing a Seismic Margin Assessment in Response to the March 2012 Request for Information Letter, Report JLD-ISG-2012-04, Interim Staff Guidance, Washington DC, (2012).

[43] SQUG, Generic Implementation Procedure (GIP) for seismic verification of nuclear plant equipment, Rev. 3A, Seismic Qualification Utility Group, December (2001).

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

[45] R. P. KENNEDY, Overview of Methods for Seismic PRA and Margins Methods Including Recent Innovations, in *Proceedings of the OECD Nuclear Energy Agency Workshop on Seismic Risk*, Tokyo, August 10-12, (1999).

[46] R. P. KENNEDY and M. K. RAVINDRA, Seismic fragilities for nuclear power plant risk studies, *Nuclear Engineering and Design,* vol. 79, no. 1, pp. 47-68, (1984).

[47] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Evaluation of Exisiting Nuclear Power Plants, IAEA Safety Reports Series No. 28, Vienna (2003), revision under preparation.

[48] ELECTRIC POWER RESEARCH INSTITUTE, Seismic Probabilistic Risk Assessment Implementation Guide, Report EPRI 1002989, Palo Alto, California (2003).

[49] U.S. NUCLEAR REGULATORY COMMISSION, Interim Staff Guidance on Implementation of a Probabilistic Risk Assessment-Based Seismic Margin Analysis for New Reactors, DC-COL-ISG-020, US NRC, Washington DC (2010).

[50] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of External Flooding (excluding Tsunami) and High Wind Hazards in Site Evaluation for Nuclear Installations Safety Report SeriesVienna (under preparation).

[51] INTERNATIONAL ATOMIC ENERGY AGENCY, External Hazard Considerations for Single and Multi-unit Probabilistic Safety Assessment, Safety Report Series Vienna (under preparation),.

[52] E. SIMIU, R. SCANLAN, Wind Effects on Structures, John Wiley, New York (1996).

[53] 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).

[54] 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 (in preparation).

[55] BULATOM, Risk Assessment and Development of Protection Capacity for Critical Infrastructures due to Aircraft Attack, RISK PROTEC CI, Results of a European R&D Project, edited by F.O. Henkel and M. Kostov, Sofia (2014).

[56] KESSLER, G., et al, The Risks of Nuclear Energy Technology - Safety Concepts of Light Water Reactors, Berlin: Springer, (2014).

[57] AMERICAN SOCIETY OF CIVIL ENGINEERS, The Pentagon Building Performance Report, ASCE, Reston VA (2003).

[58] FEDERAL EMERGENCY MANAGEMENT AGENCY, World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations, Second Printing, FEMA 403, New York (2002).

[59] NUCLEAR ENERGY INSTITUTE, Methodology for Performing Aircraft Impact Assessment for New Plant Designs, Rev. 8P, Rep. NEI 07-13, prepared by ERIN Engineering & Research, Inc., Washington DC (2011).

[60] U.S. DEPARTMENT OF ENERGY, Accident Analysis for Aircraft Crash in Hazardous Facilities," Report DOE-STD-3014-2006, Washington DC (2006).

[61] CANADIAN NUCLEAR SAFETY COMMISSION, Physical Design, Design of Reactor Facilities: Nuclear Power Plants, REGDOC-2.5.2,Ottawa, May 2014

[62] ELECTRIC POWER RESEARCH INSTITUTE, Methodology for Developing Seismic Fragilities, Rep. EPRI TR-103959, Palo Alto, CA (1994).

[63] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems for Nuclear Power Plants, IAEA Safety Standards Series SSG-34, Vienna (2016).

[64] INTERNATIONAL ATOMIC ENERGY AGENCY, Desing Provisions for Withstanding Station Blackout at Nuclear Power Plants, IAEA TECDOC Series No. 1770, Vienna (2015).

[65] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004).

[66] G. ATKINSON, Seismological considerations for the analysis of soil structure interaction, in *Workshop on Soil Structure Interaction (SSI) Knowledge and Effect on the Seismic Assessment of NPPs Structures and Components, Report NEA/CSNI/R(2011)6, OECD/NEA*, Ottawa (2010).

[67] L. ANDERSON, Interim Assessment of Surface Faulting Potential at Lauro Dam - Cachuma Project, Technical Memorandum D8330-99-011, U.S. Bureau of Reclamation, Denver (1999).

[68] INTERNATIONAL ATOMIC ENERGY AGENCY, Ground Motion Simulation based on Fault Rupture Modeling for Seismic Hazard Assessment in Site Evaluation for Nuclear Installations, Safety Report Series No. 85 , IAEA, Vienna (2015).

[69] L. TWISDALE, Tornado Missile Simulation and Design Methodology, Report EPRI NP-2005, Electric Power Research Institute, Palo Alto CA, 1981.

[70] O'CONNOR, J.E., ATWATER, B.F., COHN, T.A., CRONIN, T.M., KEITH, M.K., SMITH, C.G., MASON, R.R., Assessing Inundation Hazards to Nuclear Power Plant Sites Using Geologically Extended Histories of Riverine Floods, Tsunamis, and Storm Surges, U.S. Geological Survey, Scientific Investigation Report 2014-5207, Reston VA (2014).

[71] U.S. NUCLEAR REGULATORY COMMISSION, Design-basis Tornado and Tornado Missiles for Nuclear Power Plants, Regulatory Guide 1.76, Washington DC (2007).

[72] A. BOISSONNADE, Q. HOSSAIN, J. KIMBALL, R. MENSING, J. SAVY, Development of a Probabilistic Tornado Wind Hazard Model for the Continental United States, Report UCRL-ID-140922-VOL-1, Lawrence Livermore National Laboratory, Livermore CA (2000).

[73] INTERNATIONAL ATOMIC ENERGY AGENCY, Tsunami and Seiche Hazard Assessment in Site Evaluation for Nuclear Installations, Safety Report Series, IAEA, Vienna (in preparation).

[74] S. HIRSCHBERG, G. SPIEKERMAN, R. DONES, Severe Accidents in the Energy Sector, Report Nr. 98-16, Paul Scherrer Institute for the Swiss Federal Office of Energy, Villigen (1998).

[75] D. HARTFORD, G. BAECHER, Risk and Uncertainty in Dam Safety, London: Thomas Telford (2004).

[76] J. TATALOVICH, Comparison of Failure Modes from Risk Assessment and Historical Data for Bureau of Reclamation Dams, Report DSO-98-01, Dam Safety Office, U.S. Bureau of Reclamation, Denver (1998).

[77] S. BENUCCI, M. PONTIGGIA, G. UGUCCIONI, Explosion load calculation for building design: risk-based versus consequence-based approach, Chemical Engineering Transactions, vol. 26, pp. 153-158, (2012).

[78] J. MARX and K. WERTS, The use of overpressure exceedance curves in building siting, in *2011 Spring Meeting & 7th Global Congress on Process Safety*, Chicago IL (2011).

[79] INTERNATIONAL ATOMIC ENERGY AGENCY, Extreme External Events in the Design and Assessment of Nuclear Power Plants, TECDOC-1341, Vienna (2003).

[80] INTERNATIONAL ATOMIC ENERGY AGENCY, Volcanic Hazard Assessments for Nuclear Installations: Methods and Examples in Site Evaluation, TECDOC No. 1795, IAEA, Vienna (2016).

[81] A. VOLENTIK, C. CONNOR, L. CONNOR, C. BONADONNA, Aspects of volcanic hazard assessment for the Bataan nuclear power plant, Luzon Peninsula, Philipinnes, in *Volcanic and Tectonic Hazard Assessment for Nuclear Facilities*, Cambridge, Cambridge University Press, (2009), 229-256 pp.

[82] R. P. KENNEDY, Performance-goal based (risk informed) approach for establishing the SSE site specific response spectrum for nuclear power plants, Nuclear Engineering and Design, vol. 241, (2011) 648-656pp.

[83] INTERNATIONAL ATOMIC ENERGY AGENCY, Format and Content of the Safety Analysis Report for Nuclear Power Plants, IAEA Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004).

ANNEX I: DEFINITION OF EXTERNAL HAZARDS

Hazards and associated phenomena are described in the same order as they appear in Table 1

Earthquake [1]

For most existing nuclear facilities, the primary seismic hazard is earthquake ground shaking. Shaking is caused by the seismic waves reaching the site from the seismic source.

Other earthquake effects that can be devastating to facilities include differential ground motion induced by fault displacement at the site, liquefaction, and seismic-induced slope instability and ground settlement. Existing facilities located on capable fault[11] traces, adjacent to potentially unstable slopes, or on saturated, poorly compacted cohesion less soil or fill material can be severely damaged by earthquakes.

While earthquake hazards related to potential fault movement or to other gross soil movement are typically avoided or mitigated, the earthquake ground shaking hazard is unavoidable. When a structure or component is subjected to earthquake shaking, its foundation or support moves with the ground or with the structural element on which it rests. Earthquake ground shaking consists of a short duration of time-varying motion that has significant energy content in the range of natural frequencies of many structures. Thus, for flexible structures, dynamic amplification is possible such that the motions of the structure may be significantly greater than the ground shaking motion.

High winds and tornadoes [1]

The primary wind hazard is the force (pressure/suction) that wind exerts on the exposed surfaces of structures, systems and components (SCC). Pressures are proportional to the square of the wind speed.

Wind pressures on structures (buildings) can be classified as external or internal. External pressures develop as air flows over and around enclosed structures. The air particles change speed and direction, which produces a variation of pressure on the external surfaces of the structure. At sharp edges, the air particles separate from contact with the building surface, with an attendant energy loss. These particles produce large outward acting pressures near the location where the separation takes place. External pressures act outward on all surfaces of an enclosed structure, except on windward walls and on steep windward roofs. External pressures include pressures on windward walls, leeward walls, side walls and roof.

Internal pressures develop when air flows into or out of an enclosed structure through openings. Internal pressure acts either inward or outward, depending on the location of the opening and the wind direction. If air flows into the structure through an opening in the windward wall, a ‘ballooning’ effect takes place: pressure inside the building increases relative to the outside pressure. The pressure change produces additional net outward-acting pressures on all interior surfaces. Openings in any wall or roof area where the external pressures are outward acting allow air to flow from inside the structure: pressure inside the structure decreases relative to the outside pressure. The pressure change produces net inward acting pressure on all interior surfaces. Internal pressures combine with external pressures acting on a structure's surface.

With systems and components, interest focuses on net overturning or sliding forces, rather than the wind pressure distribution. The magnitude of these forces is determined by wind tunnel or full-scale tests. Also, in special cases associated with aerodynamically sensitive SSCs, vortex shedding or flutter may need to be considered. Typical wind sensitive SSCs include stacks, poles, cooling towers, utility

[11] A *capable fault* is a fault that has a significant potential for displacement at or near the ground surface.

bridges, and relatively light-weight structures with large smooth surfaces (e.g. roof structures made using steel trusses, purlins and light roof panels).

Gusts of wind produce dynamic pressures on SSCs. Gust effects depend on the gust size relative to SSC size and gust frequency relative to the natural frequency of the SSC. Except for tall, slender structure, the gust frequencies and the structure frequencies of vibration are sufficiently different that resonance effects are small. The size (spatial extent) of a gust relative to the size of the SSC contributes to the magnitude of the dynamic pressure. A large gust that engulfs the entire SSC has a greater dynamic effect on the SSC than a small gust that only partially covers the SSC. In any event, wind loads may be treated as quasi-static loads by including an appropriate gust response factor in calculating the magnitude of the wind pressure.

Strong winds capable of damaging SSCs in nuclear facilities can be classified as (1) straight winds, (2) hurricane winds or (3) tornado winds. Straight winds generally refer to winds in thunderstorm gust fronts or mesocyclones. Winds circulating around high or low pressure systems (mesocyclones) are rotational in a global sense, but are considered 'straight' winds at the scale of interest for this publication. Tornadoes and hurricanes both have rotating winds. The diameter of the rotating winds in a small hurricane is considerably larger than the diameter of a very large tornado. However, most tornado wind diameters are large compared to the dimensions of typical buildings or structures.

Although the three types of wind are produced by distinctly different meteorological events, research has shown that their effects on SSCs are essentially the same. Wind effects from straight winds are studied in boundary layer wind tunnels. The results of wind tunnel studies are considered reliable because they have been verified by selected full-scale measurements. Investigations of damage produced by straight winds also tend to support wind tunnel findings. Although the rotating nature of hurricane and tornado winds cannot be precisely duplicated in the wind tunnel, wind damage investigations suggest that the magnitudes and distribution of wind pressures on SSCs produced by hurricane and tornado winds are essentially identical to those produced by straight winds, if the relative wind direction is taken into account. Thus, the wind pressures on SSCs can be considered to be independent of the type of windstorm.

In addition to forces on exposed surfaces, there are two additional or secondary effects associated to strong winds: windborne missiles and atmospheric pressure change.

Strong winds pick up and transport various pieces of debris, including roof gravel, pieces of sheet metal, timber planks, plastic pipes and other objects that have high surface area to weight ratios. These objects can be carried to heights up to 60 metres in strong tornadoes. Steel pipes, posts, light-weight beam sections and open web steel joists having smaller area-to-weight ratios are transported by tornado winds, but occur less frequently and normally do not reach heights above 30 metres. Automobiles, storage tanks, and railroad cars may be rolled and tumbled by severe tornado winds. All these objects are windborne missiles which can impact SSCs in the NPP with enough energy to produce severe damage. Unprotected thin shell storage tanks are of special concern.

Atmospheric pressure change (APC) only affects sealed structures during strong tornadoes. At the centre of the tornado, the atmospheric pressure can be significantly smaller than at the radius of maximum wind. Natural porosity, openings or breach of the structure envelope permit the inside and outside pressures of an unsealed structure to equalize. However, SSCs that are purposely sealed will experience the net pressure difference caused by APC. APC, when present, acts outwardly and combines with external wind pressures. The magnitude of APC is a function of the tangential wind speed of the tornado. The rate of APC is a function of the tornado's translational speed, which can vary from 8 to 100 km/h. A rapid rate of pressure change can produce adverse effects on HVAC systems.

Flood [1]
There are a number of meteorological and hydrological phenomena that can cause flooding at a site. For each cause or source of flooding, a NPP may be exposed to one or a number of flood hazards. In most cases, the principal hazard of interest is submergence or inundation. However, the damage

potential of a flood is increased if there are impact or dynamic forces, hydrostatic forces, water-borne debris, etc.

Table I-1 lists the various possible sources or causes of flooding and the particular effects they produce. From the table, it is apparent that many of the causes of flooding may be interrelated. For example, flooding on a river can occur due to dam or levee failure or to run-off of intense precipitation in the watershed. The consequences on the site can be very similar.

In most cases, flood hazards are characterized in terms of the depth of flooding that occurs on site. Depth of inundation is the single most relevant measure of flood severity. However, the degree of damage that is caused by flooding depends on the causes. For example, coastal sites can experience significant damage due to wave action alone, even if the site is not completely inundated by a storm surge. Similarly, high velocity flood waters on a river add substantially to the potential for loss of life and the extent of structural damage. In many cases, other effects - such as wave action, sedimentation, and debris flow - can compound the damage caused just by inundation.

TABLE I-1. DIFFERENT CAUSES FOR FLOOD AND THEIR EFFECTS (ADAPTED FROM REF [1])

Hazard	Cause(s)	Effect(s) on site
Flood	Regional precipitation run-off, snow melt	Inundation Dynamic loads Sedimentation / Debris
Flood	Local intense precipitation (storm run-off)	Inundation (ponding) Dynamic loads (flash flooding) Sedimentation / Debris
Flood	Tsunami[1], seiche[2], meteotsunami[4]	Inundation Dynamic loads Debris
Flood	Storm surge[3], high tide, wind waves	Inundation Dynamic loads
Flood	Dam failure, levee or dike failure	Inundation Dynamic loads Erosion / Sedimentation / Debris
Flood	Blockage of river (debris jams, ice jams)	Inundation Sedimentation

Notes:

1. Tsunami: Series of travelling waves of long wave length (e.g. from kilometres to hundreds of kilometres) and period (e.g. several minutes to tens of minutes, and exceptionally hours), generated by deformation or disturbances of the sea floor (or, in generic terms, underwater floor). Earthquakes, volcanic phenomena, underwater and coastal landslides, rock falls or cliff failures can generate a tsunami. All oceanic regions and sea basins of the world and even fjords and large lakes can be affected by tsunamis.
2. Seiche: Long period free oscillation of a water body, which can be excited by storm surges, variations of wind speed, earthquakes, landslides into water or other disturbances.
3. Storm surge: Abnormal rise of water surface elevation in near-shore areas of water bodies, normally induced by high winds together with an atmospheric pressure reduction that occurs in conjunction with a severe meteorological disturbance.
4. A meteotsunami is a tsunami-like phenomenon which has a meteorological origin. Meteotsunamis propagate in the water as other long period waves, and they have the same dynamics at the coast, but they are not caused by disruptions in the sea floor nor by impact events, such as landslides and meteorite strikes. Instead they are basically a form of storm surge or large amplitude seiche oscillation, caused by intense low pressure or certain wind conditions associated with tropical storms and hurricanes.

In many ways, flood hazards differ significantly from other natural phenomena. The opportunity to effectively utilize warning systems and emergency procedures to limit damage and personnel injury is significantly greater in the case of flooding than it is for seismic or extreme winds and tornadoes.
The damage to buildings and the threat to public health vary depending on the type of flood hazard. In general, structural and non-structural damage occur if a site is inundated. Depending on the dynamic intensity of on-site flooding, severe structural damage and complete destruction of some buildings can result. In many cases, structural failure may be less of a concern than the damaging effects of inundation on building contents and the possible transport of hazardous or radioactive materials.

For existing installations that are not hardened against possible on-site and in-building flooding, simply inundating the site can result in a loss of function of critical components required to maintain safety and breach of areas that contain hazardous materials.

Explosion [2]

For the purposes of the present work, explosion hazard means any chemical reaction between solids, liquids, vapours or gases which may cause a substantial rise in pressure, possibly leading to impulse loads, drag loads, fire or heat. An explosion can take the form of a deflagration, which generates moderate pressures, heat or fire; or a detonation, which generates high near field pressures (shock wave) and associated drag loading but usually without significant thermal effects.

Whether or not the ignition of a particular chemical vapour or gas causes a deflagration or a detonation in air depends primarily on the concentration of the chemical vapour or gas. At concentrations two to three times the deflagration limit, detonation can occur. The deflagration limit and therefore the associated effects are in general related to the burning velocity.

For the purposes of assessing the explosion hazard, moving clouds of explosive gases and vapours are usually considered.

Release of hazardous substances [2]

The release of hazardous substances means the release of hazardous fluids which are normally kept in closed containers but which upon release could damage items important to safety or threaten human life. Of particular concern is the threat to operators in the control room of a NPP.

Those substances include the following:

- Flammable gases and vapours which can form explosive clouds and can enter ventilation system intakes and burn or explode;
- Asphyxiant and toxic gases which can threaten human life and impair crucial safety functions;
- Corrosive and radioactive gases and liquids which can threaten human life and impair the functionality of equipment.

Extreme temperatures

Extreme temperatures refers to a meteorological event in which the outside temperature is either very low (cold) or very high (hot) during a significant period of time (e.g. typically more than 24 hours). The hazard refers also to very low (icing) or very high temperature in the water body used as ultimate heat sink.

Very low temperatures can cause freezing of water pipes, boron separation in borated waters, gelling of diesel fuel, and malfunction or blockage of outdoor equipment, such as valve actuators, level sensors and miscellaneous instrumentation and control equipment.

Extreme low outside temperature has been the root cause of many malfunctions in nuclear power plants, particularly affecting instrumentation and control systems, which on many occasions have generated spurious signals. Low temperatures have at times created moisture condensation in closed rooms, with consequent dropping of water onto electrical equipment causing short circuits and malfunctions. Low temperatures have also prevented the air ventilation system of some nuclear power plants from working properly, hindered proper operation of diesel generators where the fuel showed separation of paraffin wax, damaged the external power supply system and limited the availability of service water. Additionally, very cold weather could lead to loss of the ultimate heat sink due to ice formation (frazil ice) or blockage by transported ice floes. An indirect effect is that cold weather usually produces an increase of power supply demand, which could cause grid instabilities and, eventually, a loss of off-site power event.

Very high outside temperatures can exceed the design limits of air based cooling systems (e.g. cooling towers, fan coolers, etc.) and lead to a significant reduction of their efficiency. High temperature of the cooling water can also lead to efficiency reduction in the normal and emergency cooling systems. As for the low temperatures, very hot weather usually produces an increase of power supply demand, which could cause grid instabilities and, eventually, a loss of off-site power event.

Hence, extreme temperatures have the potential to cause both the loss of the ultimate heat sink and the off-site power.

Aircraft crash

Aircraft crash is the accidental impact of an aircraft on any zone of the NPP. It could be either a fixed wing aircraft (airplane) or a helicopter. The primary hazard of an aircraft crash is the impact itself, which includes impact of 'soft' parts (e.g. the fuselage) and of 'hard' parts (e.g. the engines). Severity of impact depends on the mass, the velocity and the attitude of the impacting aircraft. Note that flight mechanics does not allow arbitrary combinations of these parameters.

Secondary hazards of the aircraft crash are related with the possible consequences of the release of fuel, which could lead to explosion and fire.

External fire

An external fire is any fire that initiates outside the NPP boundary but which can propagate towards the site and eventually affect the NPP. Typical examples are the forest, grass or peat fires. Also included in this hazard category are the fires in hydrocarbon storage facilities or in nearby factories which work with flammable materials, such as wood, plastics or solvents. However, fires in nearby industrial facilities are usually more localized and easier to isolate.

Primary hazard of an external fire is the propagation to the site of the fire itself. Secondary hazards are generated smoke and ashes, which could force isolation of ventilation systems, and cut-off grid distribution lines, which could lead to an event of loss of off-site power.

Volcanic tephra fallout [3]

Tephra fallout refers to the fall and deposition of pyroclastic material such as ash, pumice and scoria which occur after these particles are lifted by an explosive volcanic eruption to altitudes of several kilometres to tens of kilometres. This material is transported in the atmosphere by wind. Volcanic eruptions produce widely varying volumes of tephra. On falling, pyroclasts[12] normally reach a constant velocity (so-called terminal velocity), which is determined by the size, shape and density of the falling particles, air density and air viscosity. Their distribution is governed by the velocity and direction of the wind and by the nature of the eruption column. The thickness and mass per unit area of tephra deposited generally decrease with distance from the volcano, each in a roughly exponential

[12] A *pyroclast* is a particle of any size or composition produced from a volcanic eruption.

manner. Thus, tephra fallout may occur more than 100 km from the vent and the mass per unit area may vary from less than 10 kg/m^2 far from the vent to more than 1000 kg/m^2 close to the vent. When wet, these loads may be more than double. Tephra particles can range in size from microns to decimetres and average particle size decreases with distance from the volcano. Tephra fallout is common for all types of volcanic eruption, but the most voluminous fallout is normally associated with caldera-forming eruptions and composite volcanoes.

Volcanic activity [3]

Volcanic activity hazard refers to volcanic phenomena that take place within a distance range relatively close to the volcano (e.g. typically less than 40 km). It includes the following:

- Pyroclast density currents. They include pyroclastic flows, pyroclastic surges and blasts. Pyroclastic flows are high temperature mixtures of rock fragments, volcanic gases and air that flow down slopes at high speeds (flow velocities reach 10-100 m/s). Pyroclastic surges are dilute gas–solid suspensions (clouds of volcanic ash and hot gases) that flow over the ground surface at high velocities (often exceeding 25 m/s) and are less influenced by topography than pyroclastic flows. A volcanic blast is a laterally directed pressure wave associated with ash-laden clouds.
- Lava flows. Flows of lava are driven by gravity and follow the drainage lines of the topography. Lavas are viscous, dense (approximately 2000 kg/m^3) fluids, usually with a semi-solid crust on the surface, and flow at speeds of less than 1 m/s to around 20 m/s in extreme cases. Lava flows can travel tens of kilometres from the vent and in unusual cases up to several hundred kilometres, and range in thickness from less than one metre to more than 100 m.
- Debris avalanches, landslides and slope failure. These phenomena are not necessarily related with a volcano eruption. They can be considered an especial case of slope instability. They also occur on long dormant volcanoes. Steep sided volcanic edifices, such as volcanic domes and composite volcanoes, may become unstable as a result of rock alteration, ground deformation and erosion. Partial or complete failure of the slopes can produce debris avalanches, which are flows of rock fragments, ranging in size from a few centimetres to tens of metres in diameter, and entrapped air. The mode of movement of debris avalanches is therefore similar to that of pyroclastic flows in that both phenomena are high velocity fluidized flows accelerated downslope by gravity (up to 50–70 m/s). Although not as large as debris avalanches, detachment and collapse of unstable slopes of the volcanic edifice may lead to landslides and other types of sudden slope failure, triggered by igneous intrusion, earthquake or heavy rainfall. These mass movements may have sufficient volume to dam river drainages. In some cases, the entry of debris avalanches and landslides into water bodies may generate tsunamis.
- Debris flows, lahars and floods. Volcanic debris flows and lahars are mixtures of volcanic rock fragments ranging in diameter from 10^{-6} m to 10^2 m, mixed with varying proportions of water, as well as other rocks, soil and vegetation. They range from flows containing many large boulders cascading down steep slopes to muddy currents sweeping over wide areas at the base of the volcano following river courses. Debris flows and lahars can become torrential streams, heavily loaded with suspended sand and clay particles. These flows may occur at any stage during volcanic activity, including the earliest stages of an eruption. Debris flows can occur throughout a region for decades following voluminous explosive volcanic eruptions.

- Opening of new vents. A new vent forms when magma ascends through the Earth's crust along a new pathway, leading to an eruption of lava at a new location. New volcanoes can form at locations tens of kilometres away from the sites of previous eruptions.
- Volcano generated missiles. Ejection of missiles such as blocks, bombs and other solid fragments is caused by explosions occurring within craters, domes or vents. These objects are propelled by high pressure gas and follow trajectories under gravity. The speeds of the missiles can be more than 300 m/s and the maximum horizontal distances they may travel can be up to 5 km from the origin.
- Volcanic gases and aerosols. Volcanic gases make up a significant fraction of the total mass of material emitted by volcanoes. Gases exhaled from volcanic vents, fumaroles, solfataras, mofettes and hydrothermal systems may be highly reactive and hazardous to humans and property. Although volcanic gases consist mainly of H^2O, they also include CO^2, SO^2, H^2S, CO, HC^l and HF and form low pH condensates. Gases may be discharged in large quantities either from established vents or from new fissures unrelated to established vents, or through soils on volcanoes, well before or after an eruption.
- Tsunamis, seiches, crater lake failure and glacial burst. Volcanogenic tsunamis and seiches may be generated when voluminous landslides, pyroclastic flows or debris avalanches rapidly enter the sea or large lakes, or by submarine eruption of volcanoes. Collapse of a volcano edifice triggered by volcanic eruptions or earthquakes may lead to large displacement of the slopes, which, in turn, can generate tsunamis in proximal bodies of water. This can be considered an especial case of tsunami or seiche.
- Atmospheric phenomena. Explosive eruption of a volcano can generate air pressure waves powerful enough to break windows at distances of several kilometres. Air shocks may accompany lateral volcanic blasts and thus may affect areas tens of kilometres from the volcano, depending on the interaction of the blast and the topography. In addition, lightning often accompanies many types of volcanic eruption and may involve hundreds of ground strikes. In some cases, lightning and high static charges occur up to several kilometres from the erupting volcano. Locally violent weather may accompany volcanic eruptions. Heavy rainfall may accompany the development of explosive eruption columns, as ash particles in the atmosphere cause sudden nucleation of raindrops. Heavy rainfall during tephra fallout may result in the generation of lahars. Downbursts (locally very strong winds) can occur as a result of explosive columns or the emplacement of hot lava flows. These winds may cause damage extending beyond the lava flows themselves. All these phenomena can be considered as especial causes of hazards already considered.
- Ground deformation. Some of the largest amplitude natural ground deformations ever observed has occurred on volcanoes. Prior to a volcanic eruption, ground deformation can involve rapid uplift of several metres or more. More generally, ground displacements of millimetres to centimetres may occur over broad areas in response to magma intrusion into volcanoes. Deformation typically occurs around volcanoes through syneruptive faulting or shallow intrusion of magma. Modes of deformation include uplift, subsidence and extension. For example, vertical displacements of more than 100 m were produced by the 1977 eruption of Usu volcano in Hokkaido (Japan).
- Volcanic earthquakes. Volcanic earthquakes and seismic events normally occur as a result of stress releases associated with the rise of magma towards the surface. Generally, the largest volcanic earthquakes have smaller magnitudes than the largest earthquakes of tectonic origin in a geodynamically active region. This phenomenon can be considered an especial case of a hazard already considered.

- Hydrothermal systems and groundwater anomalies. Extensive hydrothermal systems are sometimes associated with volcanoes. Hydrothermal systems create elevated near surface temperatures that can boil water and alter solid rock to clays. The presence of active hydrothermal systems or hydrothermal alteration can indicate a propensity for large mass movements, such as landslides or edifice collapse. Additionally, hydrothermal systems can produce steam explosions that are capable of ejecting rock fragments over distances of several kilometres and of forming explosion craters hundreds of metres in diameter.

Lightning [4]

Lightning is described as the static spark discharge resulting from the development of hundreds of millions of volts of electric potential between clouds or between a cloud and the earth. It can be compared to the dielectric breakdown of a huge capacitor. It is the most frequent cause of over-voltages on electrical distribution systems. The current in a lightning strike can be greater than 200000 amperes, although about 50% of all stroke currents are thought to be less than 15000 amperes. The time duration of the current flow in the majority of high-current lightning strikes may be tens to hundreds of microseconds. Non-conductors are often shattered by lightning strikes, while conductors may be burned or vaporized entirely. Transformers may explode.

Lightning has been involved in many complete and partial losses of offsite power in nuclear power plants. Lightning has also triggered serious fire accidents and spurious signals to valves, with consequent flooding and loss of off-site power. In boiling water reactor plants, lightning has produced detonation of gaseous effluents in plant vent systems (off-gas).

Slope instability

Slope instability refers to the hazard of large movements of ground material, ice or snow, typically in mountainous or hilly terrain or in artificial trenches and embankments. It includes phenomena such as avalanches, landslides, rock falls or rock slides. During these events, millions of tons of material can move in a matter of minutes, with enormous property damage and potential loss of human lives. This kind of massive movement can be triggered by a variety of causes, such as heavy rain, earthquakes, snow melt or volcanic activity.

Hail [4]

Hail is a type of ice formation in the atmosphere. Strong, rising convective air currents, as in a cumulonimbus cloud, cause intense supersaturation resulting in raindrops which are carried aloof and then freeze in the higher, cooler air. These frozen drops are what are known as hail. The hailstones may fall after reaching a certain height and descend through a region of the cloud containing super cooled water that freezes on the hailstone or leaves a coating of water. Repetitions of the ascending and descending motion results in a concentric structure of clear and opaque ice and the possible formation of very large hailstones, up to 150 mm in diameter. Soft hail is not really hail but a form of snow, consisting of pellets of closely packed ice crystals. It breaks apart upon striking a hard surface. Usually, true hail is characteristic of violent summer thunderstorms, while soft hail accompanies the less severe winter or spring storms.

Primary hazard of hail is impact of hailstones on outdoor sensitive equipment such as brittle components or small instrumentation lines. For instance, impact of big hailstones on substation ceramic insulators can lead to an event of loss of off-site power. A secondary hazard is the accumulation of hailstones in the roofs, which may overload the roof slabs.

Abrasive windstorms [4]

Abrasive windstorms refer to the dust storms or sandstorms that occur in semi-arid regions when the wind forces exceed the threshold value at which loose particles are removed from a dry surface and

become airborne. As a primary hazard, these phenomena can pose a threat to ventilation systems, degrade the ultimate heat sink or lead to a loss of off-site power event. Secondary hazards are the accumulation of sand or dust at the roofs, the reduced visibility, the abrasion of exposed surfaces and the potential malfunction of sensitive equipment located outdoors.

Extra-terrestrial activity [4]

Extra-terrestrial activity is described as natural celestial objects (such as meteors) or artificial satellites entering the earth's atmosphere from space. These bodies undergo friction heating and lose mass by ablation as they travel through the earth's atmosphere. If they are sufficiently large when begin they descent, they eventually strike the earth's surface.

Meteors vary in size from dust-like particles to asteroids several hundred miles in diameter. However, all meteors having an initial mass of less than about 50 kg are reduced to dust-like particles by the heat developed from passing through the earth's atmosphere. The entry velocity of meteors can vary from 11300 m/s (the escape velocity from the earth) to 88500 m/s (the sum of the earth's orbital velocity and the solar escape velocity). The number of meteors striking the earth each year weighing over 500 grams at impact has been estimated to be about 3500, with the majority being between 0.5 and 1.0 kg.

It has to be noted that the kinetic energy of a 1000 kg meteorite striking the earth at 11300 m/s is equivalent to the energy of about 15000 kg of a high explosive like TNT. Clearly, the damage potential to objects on the earth being struck or even being near-missed by meteorites is enormous.

Ship/Barge impact [5]

Ship/Barge impact refers to the collision of a vessel with plant's water intake or outlet structures. The primary hazard is the impact by itself, which could damage those structures and lead, for example, to the loss of service water. Secondary hazards, due to accidents even without impact with plant's structures, are the possible release of hazardous material towards the plant and/or the possibility of explosion and fires with resulting physical damage to the plant due to blast, debris and fire.

Note also that spillage of oil or corrosive fluids could affect the availability or quality of cooling water.

Collision of floating bodies [6]

This hazard considers the impact of inert bodies with plant's water intake or outlet structures. Examples of inert bodies are ice masses or floating debris during a flood event.

Recent operating experience shows a significant number of occurrences of impact related damage to water intakes and ultimate heat sink components. Ice blocks and floating debris have damaged water intakes and pump houses were flooded.

Foundation ground instability

Foundation ground instability hazard includes the collapse, subsidence or uplift of the surface of the ground due to consolidation, underlying karstic formations, caverns, expansive soils, volcanic activity or man-made features such as mines, water wells or oil wells.

Electromagnetic interference

Electromagnetic interference hazard concerns the malfunction of electrical/electronic devices due to strong electromagnetic fields produced by rapidly changing electrical currents or other causes. The source of the electromagnetic disturbance can be both on-site (e.g. high voltage switchgear) and off-site (e.g. a central telephone facility, radars, solar storms, electrical storms or the Northern Lights). Electronic devices are typically used in modern plants for I&C applications. However, strong solar

storms can induce large currents in high voltage transmission systems which, in turn, can produce severe damage in the step-up transformers of a power station.

Blockage or diversion of river

Blockage or diversion of river is defined as the accidental interruption or reduction of water flow in the river at the location of the plant, so that water level at the intake is reduced up to the point that the ultimate heat sink is lost. Blockage can be the result of a landslide, of jams caused by ice, logs, debris or volcanic material.

Biological phenomena [6]

Biological phenomena mainly affect the availability of cooling water from the ultimate heat sink and the service water system, as consequence of excessive growth of algae, mussels or clams, or clogging by exceptional quantities of fish or jellyfish.

In addition, very often malfunctions have also been recorded in ventilation systems because of clogging of filters by leaves or insects.
In some cases, attacking of instrumentation and control cables by rats and by bacteria has been recorded. Corrosion effects and accelerated ageing of steel structures exposed to the marine environment can be induced by sulphate reducing bacteria.

Such acute events have usually been found to be combined with flooding, which can cause the sudden removal of marine growth (deposited in different areas) and clogging into the water intake; and strong winds, which can cause the clogging of air intakes by leaves or insects in unusual seasonal conditions.

Depletion of a reservoir

Depletion of a reservoir is defined as the loss of the water body used as ultimate heat sink due to natural (e.g. drought) or human induced (e.g. dam break) causes .

Freezing precipitation and frost related phenomena

This hazard is connected to the hazard about extreme temperatures, discussed above.

Freezing precipitation is a precipitation that falls when the temperature on and above surfaces is below freezing. The drops become super cooled and freeze upon impact with soil or with any surface, resulting in the formation of a layer of ice.

Ice due to freezing rain, snow, rime and in-cloud icing is known to cause increases in the dead loads and the response of structures. Important effects are related to significant increases in the static and dynamic response to wind action for conductors in transmission lines. Similar but usually less pronounced effects need to be expected in steel trusses under winter conditions. In addition the formation of ice in cooling systems may affect their efficiency.

Extreme snowpack

Extreme snowpack is defined as the accumulation of snow in roofs and at grade level to the extent that it can overload the structures and complicate plant operations.

Variation of groundwater level

The hazard of variation of groundwater level is defined as the change in water pore pressures which may affect soil stability, increase forces on embedded structures or favour seepage through walls and foundation slabs.

An increase in the groundwater level in the uppermost geological formation is generally a consequence of another phenomenon. For plant sites located near a river or coastal area, a rise in the groundwater level is generally related to an increase in the water level of the surface water bodies that are hydraulically connected to the aquifer. Additional phenomena, such as a large rainfall event or the failure of a water control structure, also could cause groundwater levels to increase. Variations in groundwater levels depend on the properties of soil and rocks, primarily the permeability and porosity of geological media.

The range of yearly variations of groundwater levels may vary from centimetres to tens of metres owing, in particular, to the broad diversity of geological media. Torrential rainfall may cause quick, large amplitude increases in groundwater levels in very porous or karstified media.

Saltspray / Saltstorm

This hazard refers to the salty winds blowing from the sea during severe storms. Conductivity of air can be substantially increased and salt crystals can build-up on the insulators of power lines, transformers or breakers located outside the buildings. Resulting electrical arches or grounding can lead to short circuits, fires and loss of off-site and on-site power.

Waterspouts

Waterspouts hazard includes both tornadic waterspouts and fair weather waterspouts.

Tornadic waterspouts are tornadoes that form over water or move from land to water. They are associated with severe thunderstorms.

Fine weather waterspouts form most commonly in the summer, in fair and relatively calm weather, along the dark flat bases of a line of developing cumulus clouds. They typically move slowly, since the cloud they are attached to is typically horizontally static.

Apart from damage associated to strong winds, waterspouts may transfer large amounts of water to land from nearby water bodies, thus producing local floods.

ANNEX II: EXAMPLES OF PRELIMINARY SCREENING FOR TYPICAL SITES

Preliminary screening is site specific, since it is dependent on site characteristics and plant layout.

In order to provide guidance to the hazard analysts performing the screening for an actual nuclear installation, several typical sites representative of the worldwide nuclear fleet have been selected. For each of these sites, a generic preliminary screening has been carried out in this Annex.

According to Section 2.3.2, for screening out an external hazard from the vulnerability assessment, any one of the following qualitative criteria provides an acceptable basis:

Criterion 1: The hazard is of equal or lesser damage potential than the events for which the installation has been designed. This requires an evaluation of plant design basis in order to estimate the resistance of plant structures and systems to a particular external hazard.

Criterion 2: The hazard could not result in worse consequences than the consequences of other hazard which has not been screened out.

Criterion 3: The events associated with the hazard cannot take place close enough to the installation to affect it. This criterion must be applied taking into account the range of physically possible strengths of the events affecting the installation.

Criterion 4: The hazard is included in the definition of other hazard not screened out.

Criterion 5: The hazard corresponds to events that are slow in developing and it can be demonstrated that there is sufficient time to eliminate the source of the threat or to provide an adequate response.

Typical site A is defined by the following characteristics:

- Coastal site, either a lake or sea site.
- The primary ultimate heat sink for safety related systems is the lake or the sea.
- The local topography is basically flat, with no significant grass or forest areas.
- There are main transportation routes (roads, railroads, etc.) at less than 8 km from the site.
- There are other industrial facilities at less than 8 km distance from the site.
- The site is located at geographical latitude less than about 40º.

Preliminary screening for this site is given in Table II-1. Hazards not screened out at this stage are the following:

(1) Earthquake

(2) High winds (‘straight’ winds or tropical cyclones)

(3) Flood due to meteorological causes

(4) Flood due to long period water waves

(5) Explosion

(6) Release of hazardous substances

(7) Extreme temperatures

(8) Aircraft crash

(9) Hail (only to identify exposed SSCs vulnerable to impact by hailstones during plant walkdown)

TABLE II-1. PRELIMINARY SCREENING FOR SITE A (cont.)

Hazard	Applicable criteria*	Remarks
Earthquake	--	Earthquake hazard cannot be screened out for any site. There is evidence that earthquakes can occur at any location of the Earth's surface.
High winds ('straight' winds or tropical cyclones)	--	High winds hazard cannot be screened out for any site. Strong winds are possible due to a variety or causes (extra-tropical cyclones, local storms, hurricanes, etc.).
Flood due to meteorological causes	--	Flood due to meteorological causes cannot be screened out for this site. It could be screened out after a bounding analysis that showed enough capacity of the drainage system for local extreme precipitation and enough margins against maximum possible water height from: storm surge + high tide + wind waves.
Tornado	2	For this site, it is likely that tornado conditions are enveloped by hurricane or 'straight wind' conditions.
Flood due to long period water waves	--	For this site, the tsunami or seiche hazard cannot be screened out at this stage.
Flood due to failure of water control structures	3	There are no water control structures whose failure could affect this site.
Explosion	--	The explosion hazard from an accident in nearby facilities or transportation routes cannot be screened out at this stage. A bounding analysis has to be done in the next step.
Release of hazardous substances (toxic, asphyxiant, corrosive or radioactive)	--	The release of hazardous substances from an accident in nearby facilities or transportation routes cannot be screened out at this level. A bounding analysis has to be done in the next step.
Extreme temperatures	2, 5	The potential effects of extreme temperatures (extreme heat, extreme cold) in this plant are the loss of off-site power and the reduction of primary ultimate heat sink capacity.
	--	The loss of off-site power is already considered as a consequence of other hazards not screened out in this plant (e.g. high winds).
		The reduction of capacity of the ultimate heat sink would be a slow process, so that the operators have enough time to take adequate actions.
		However, actual temperature limits for reliable operation of outdoors safety related equipment beyond design temperature are not known in this plant. Hence, the weak links against extreme temperatures are not known and they will not be identified during the analysis of other hazards.

(*) See Section 2.3.2.

TABLE II-1. PRELIMINARY SCREENING FOR SITE A (cont.)

Hazard	Applicable criteria*	Remarks
Aircraft crash	--	At this stage, aircraft impact cannot be screened out for this plant.
External fire (forest, hydrocarbon storage, nearby factories)	3	There are no significant grass or forest areas around the site. Industrial facilities around the site do not store flammable materials in a quantity such that a fire could affect the site, given the distances at which they are located.
Volcanic tephra fallout	3, 4, 5	This hazard can be screened out, since there is no active volcano at less than 100 km from the site and the accumulation of tephra on plant structures is slow enough to take appropriate counteracting measures. Other associated phenomena, (e.g. loss of off-site power due to short circuits) are considered in other hazards.
Volcanic activity	3	This hazard can be screened out, since there is no active volcano at less than 100 km from the site.
Lightning	1, 2, 4	The primary effect of lightning is the loss of off-site power, which is already considered as a consequence of other hazards not screened out in this plant (e.g. high winds). Based on past operating experience, lightning has not affected safety related instrumentation and control systems in this plant. Safety related SSCs in this plant are protected by a lightning protection system according to the current regulation in the Member State. Redundancy and physical separation of exposed safety systems in this plant eliminates the possibility of a lightning strike affecting two safety trains.
Slope instability	3	Local topography is flat, with no slopes.
Hail	2	Potential effect of loss of off-site power is considered for other hazards not screened out (e.g. high winds). Exposure of safety related SSCs vulnerable to impact by hailstones to be checked during plant walkdown.
	--	Potential maximum accumulation of hailstones in roofs to be checked during plant walkdown.
Extra-terrestrial activity	(2), 3	Meteorite strikes, with masses over 0.5 kg, are very rare events at any point of the Earth's surface. There is wide consensus worldwide that consideration of these events is not needed within nuclear safety analyses.
Abrasive windstorms (dust storms and sandstorms)	3	Abrasive windstorms cannot occur close to this site.

(*) See Section 2.3.2.

TABLE II-1. PRELIMINARY SCREENING FOR SITE A (cont.)

Hazard	Applicable criteria*	Remarks
Ship/barge impact	3	There are no navigation channels near the site.
Collision of floating bodies	3	Shore line at the site is protected by rock riprap. Cooling water intakes are submerged.
Foundation ground instability	3	Site investigation demonstrated that no karst phenomena or underground caverns are present under the site. There are no water or oil wells that could produce subsidence at the site. Civil structures in this plant are founded on stable soft rock, with no expansion or consolidation phenomena.
Electromagnetic interference	1, 3	No sources of strong electromagnetic fields exist in the site vicinity. Design of instrumentation and control systems complies with Ref [7] regarding protection against lightning.
Blockage or diversion of river	3	This hazard does not apply to this site, since it is a coastal site.
Biological phenomena	5	The potential effect of biological phenomena in this plant is the reduction of primary ultimate heat sink capacity. For the biological species present in this zone, the reduction of capacity of the ultimate heat sink would be a slow process, so that the operators have enough time to take adequate actions.
Depletion of a reservoir	3	The loss of the water body used as ultimate heat sink in this plant is not considered to be possible.
Freezing precipitation and frost related phenomena	3	Climate in the site region is relatively mild. Freezing precipitation is a phenomenon unknown in the area.
Extreme snowpack	3	Climate in the site region is relatively mild. Snow is very rare and it melts rather quickly.
Variation of groundwater level	3	Ground water level in this site is fairly stable, since it is anchored to the water level in the water body.
Saltspray/Saltstorm	2, 3	Main plant substations are far enough from the shore line to be protected from salt-sprays. In any case, the result of salt sprays would be electrical arches or grounding, leading to short circuits, and loss of off-site power, which is already considered as a consequence of other hazards not screened out in this plant (e.g. high winds).

(*) See Section 2.3.2.

TABLE II-1. PRELIMINARY SCREENING FOR SITE A (cont.)

Hazard	Applicable criteria*	Remarks
Waterspouts	2, 4	This hazard can be considered to be enveloped by two hazards which have not been screened out: High Winds and Flood due to Meteorological Causes.

(*) See Section 2.3.2.

Typical site B is defined by the following characteristics:

- Inland river site.
- The primary ultimate heat sink for safety related systems is the river.
- The local topography is basically flat, with no significant grass or forest areas.
- There are main transportation routes (roads, railroads, etc.) at less than 8 km distance from the site.
- There are no other industrial facilities at less than 8 km distance from the site.
- The site is located at geographical latitude larger than about 40º, with continental climate.

Preliminary screening for this site is given in Table II-2. Hazards not screened out at this stage are the following:

(1) Earthquake

(2) High winds (‘straight’ winds or tropical cyclones) / Tornado

(3) Flood due to meteorological causes

(4) Flood due to failure of water control structures

(5) Explosion

(6) Release of hazardous substances

(7) Extreme temperatures

(8) Aircraft crash

(9) Hail (only to identify exposed SSCs vulnerable to impact by hailstones during plant walkdown)

(10) Collision of floating bodies (site walkdown has to confirm that intakes and pump houses will not lose their intended safety functions due to impact by large floating bodies)

(11) Extreme snowpack (only to confirm that plant procedures are in place to avoid exceeding allowable levels for roof structures)

TABLE II-2. PRELIMINARY SCREENING FOR SITE B (cont.)

Hazard	Applicable criteria*	Remarks
Earthquake	--	Earthquake hazard cannot be screened out for any site. There is evidence that earthquakes can occur at any location of the Earth's surface.
High winds ('straight' winds or tropical cyclones)	--	High winds hazard cannot be screened out for any site. Strong winds are possible due to a variety or causes (extra-tropical cyclones, local storms, hurricanes, etc.).
Flood due to meteorological causes	--	Flood due to meteorological causes cannot be screened out for this site. It could be screened out after a bounding analysis that showed enough capacity of the drainage system for local extreme precipitation and enough margins against maximum possible water height in the river.
Tornado	--	For this site, it has to be investigated whether tornado conditions are enveloped by 'straight wind' conditions. If not, an enveloping scenario can be defined for the assessment
Flood due to long period water waves	3	This phenomenon cannot affect this site.
Flood due to failure of water control structures	--	The flood due to failure of upstream dams cannot be screened out at this stage. A bounding analysis needs to be done in the next step.
Explosion	--	The explosion hazard from an accident in nearby transportation routes cannot be screened out at this stage. A bounding analysis has to be done in the next step.
Release of hazardous substances (toxic, asphyxiant, corrosive or radioactive)	--	The release of hazardous substances from an accident in nearby transportation routes cannot be screened out at this level. A bounding analysis has to be done in the next step.
Extreme temperatures	2, 5	The potential effects of extreme temperatures (extreme heat, extreme cold) in this plant are the loss of off-site power and the reduction of primary ultimate heat sink capacity.
	--	The loss of off-site power is already considered as a consequence of other hazards not screened out in this plant (e.g. high winds). The reduction of capacity of the ultimate heat sink would be a slow process, so that the operators have enough time to take adequate actions. However, actual temperature limits for reliable operation of outdoors safety related equipment beyond design temperature are not known in this plant. Hence, the weak links against extreme temperatures are not known and they will not be identified during the analysis of other hazards.

(*) See Section 2.3.2.

TABLE II-2. PRELIMINARY SCREENING FOR SITE B (cont.)

Hazard	Applicable criteria*	Remarks
Aircraft crash	--	At this stage, aircraft impact cannot be screened out for this plant.
External fire (forest, hydrocarbon storage, nearby factories)	3	There are no significant grass or forest areas around the site. There are no industrial facilities around the site.
Volcanic tephra fallout	3, 4, 5	This hazard can be screened out, since there is no active volcano at less than 100 km from the site and the accumulation of tephra on plant structures is slow enough to take appropriate counteracting measures. Other associated phenomena, (e.g. loss of off-site power due to short circuits) are considered in other hazards.
Volcanic activity	3	This hazard can be screened out, since there is no active volcano at less than 100 km from the site.
Lightning	1, 2, 4	The primary effect of lightning is the loss of off-site power, which is already considered as a consequence of other hazards not screened out in this plant (e.g. high winds). Based on past operating experience, lightning has not affected safety related instrumentation and control systems in this plant. Safety related SSCs in this plant are protected by a lightning protection system according to the current regulation in the Member State. Redundancy and physical separation of exposed safety systems in this plant eliminates the possibility of a lightning strike affecting two safety trains.
Slope instability	3	Local topography is flat, with no slopes.
Hail	2	Potential effect of loss of off-site power is considered for other hazards not screened out (e.g. high winds).
	--	Exposure of safety related SSCs vulnerable to impact by hailstones to be checked during plant walkdown. Potential maximum accumulation of hailstones in roofs to be checked during plant walkdown.
Extra-terrestrial activity	(2), 3	Meteorite strikes, with masses over 0.5 kg, are very rare events at any point of the Earth's surface. There is wide consensus worldwide that consideration of these events is not needed within nuclear safety analyses.
Abrasive windstorms (dust storms and sandstorms)	3	Abrasive windstorms cannot occur close to this site.

(*) See Section 2.3.2.

TABLE II-2. PRELIMINARY SCREENING FOR SITE B (cont.)

Hazard	Applicable criteria*	Remarks
Ship/barge impact	3	There are no navigation channels near the site.
Collision of floating bodies	--	Site walkdown has to confirm that water intakes and pump houses are protected against impact of large floating bodies.
Foundation ground instability	3	Site investigation demonstrated that no karst phenomena or underground caverns are present under the site. There are no water or oil wells that could produce subsidence at the site. Civil structures in this plant are founded on stable soil, with no expansion or consolidation phenomena.
Electromagnetic interference	1, 3	No sources of strong electromagnetic fields exist in the site vicinity. Design of instrumentation and control systems complies with Ref [7] regarding protection against lightning.
Blockage or diversion of river	3	Examination of the river course in the near-region area (25 km radius) and the analysis of historical floods, conclude that blockage or diversion of the river affecting the plant is not possible.
Biological phenomena	5	The potential effect of biological phenomena in this plant is the reduction of primary ultimate heat sink capacity. For the biological species present in the zone, the reduction of capacity of the ultimate heat sink would be a slow process, so that the operators have enough time to take adequate actions.
Depletion of a reservoir	3	The ultimate heat sink in this plant is not dependent on keeping a minimum water level in any reservoir.
Freezing precipitation and frost related phenomena	4	This hazard will be studied within the hazard of 'Extreme Temperatures', which has not been screened out.
Extreme snowpack	--	Extreme snowpack hazard cannot be screened out at this stage. A bounding analysis needs to be done in the next step to assess the allowable snowpack at roofs and to check that plant procedures are in place to avoid exceeding this level.
Variation of groundwater level	3	Ground water level in this site is fairly stable, since it is anchored to the water level in the river.
Saltspray/Saltstorm	3	This phenomenon cannot take place at this site.
Waterspouts	3	This phenomenon cannot take place at this site.

(*) See Section 2.3.2.

Typical site C is defined by the following characteristics:

- Inland site, separated from large rivers or lakes. Water is brought to the site by means of a pipeline and it is stored in ponds within the site.
- The primary ultimate heat sink for safety related systems is not directly dependent on nearby natural water bodies (e.g. forced draught cooling towers).
- The local topography includes hills and steep slopes, together with significant forest areas.
- The plant is relatively isolated, with no other industrial facilities or main ground transportation routes at less than 8 km from the site boundaries.
- The site is located at geographical latitude larger than about 40º.

Preliminary screening for this site is given in Table II-3. Hazards not screened out at this stage are the following:

(1) Earthquake

(2) High winds ('straight' winds or tropical cyclones)

(3) Flood due to meteorological causes

(4) Extreme temperatures

(5) Aircraft crash

(6) Slope instability

(7) Hail (only to identify exposed SSCs vulnerable to impact by hailstones during plant walkdown)

(8) Extreme snowpack (only to confirm that plant procedures are in place to avoid exceeding allowable levels for roof structures)

TABLE II-3. PRELIMINARY SCREENING FOR SITE C (cont.)

Hazard	Applicable criteria*	Remarks
Earthquake	--	Earthquake hazard cannot be screened out for any site. There is evidence that earthquakes can occur at any location of the Earth's surface.
High winds ('straight' winds or tropical cyclones)	--	High winds hazard cannot be screened out for any site. Strong winds are possible due to a variety or causes (extra-tropical cyclones, local storms, hurricanes, etc.).
Flood due to meteorological causes	--	Flood due to meteorological causes cannot be screened out for this site. It could be screened out after a bounding analysis that showed enough capacity of the drainage system for local extreme precipitation and run-off.
Tornado	2	Tornado is a rare phenomenon in the region. For this site, it is likely that tornado conditions are enveloped by 'straight wind' conditions.
Flood due to long period water waves	3	The phenomenon cannot affect this site.
Flood due to failure of water control structures	3	Failure of upstream dams cannot affect the site, due to plant grade elevation and distance from the river.
Explosion	3	There are no other industrial facilities or main ground transportation routes near the site, which could be the origin of an explosion external to the plant.
Release of hazardous substances (toxic, asphyxiant, corrosive or radioactive)	3	There are no other industrial facilities or main ground transportation routes near the site, which could be the origin of a release of hazardous substances.
Extreme temperatures	2, 5	The potential effects of extreme temperatures (extreme heat, extreme cold) in this plant are the loss of off-site power and the reduction of primary ultimate heat sink capacity.
	--	The loss of off-site power is already considered as a consequence of other hazards not screened out in this plant (e.g. high winds).
		The reduction of capacity of the ultimate heat sink would be a slow process, so that the operators have enough time to take adequate actions.
		However, actual temperature limits for reliable operation of outdoors safety related equipment beyond design temperature are not known in this plant. Hence, the weak links against extreme temperatures are not known and they will not be identified during the analysis of other hazards.

(*) See Section 2.3.2.

TABLE II-3. PRELIMINARY SCREENING FOR SITE C (cont.)

Hazard	Applicable criteria*	Remarks
Aircraft crash	--	At this stage, aircraft impact cannot be screened out for this plant.
External fire (forest, hydrocarbon storage, nearby factories)	1, 2, 4	Forest fires are possible around the site, but will not be able to spread on-site because of site clearing during construction and continuous surveillance of the perimeter of the plant site. Forest fires could produce a loss of off-site power. The loss of off-site power is already considered as a consequence of other hazards not screened out (e.g. high winds).
Volcanic tephra fallout	3, 4, 5	This hazard can be screened out, since there is no active volcano at less than 100 km from the site and the accumulation of tephra on plant structures is slow enough to take appropriate counteracting measures. Other associated phenomena, (e.g. loss of off-site power due to short circuits) are considered in other hazards.
Volcanic activity	3	This hazard can be screened out, since there is no active volcano at less than 100 km from the site.
Lightning	1, 2, 4	The primary effect of lightning is the loss of off-site power, which is already considered as a consequence of other hazards not screened out in this plant (e.g. high winds). Based on past operating experience, lightning has not affected safety related instrumentation and control systems in this plant. Safety related SSCs in this plant are protected by a lightning protection system according to the current regulation in the Member State. Redundancy and physical separation of exposed safety systems in this plant eliminates the possibility of a lightning strike affecting two safety trains.
Slope instability	--	At this stage, slope instability cannot be screened out for this plant.
Hail	2 -- 	Potential effect of loss of off-site power is considered for other hazards not screened out (e.g. high winds). Exposure of safety related SSCs vulnerable to impact by hailstones to be checked during plant walkdown. Potential maximum accumulation of hailstones in roofs to be checked during plant walkdown.
Extra-terrestrial activity	(2), 3	Meteorite strikes, with masses over 0.5 kg, are very rare events at any point of the Earth's surface. There is wide consensus worldwide that consideration of these events is not needed within nuclear safety analyses.
Abrasive windstorms (dust storms and sandstorms)	3	Abrasive windstorms cannot occur close to this site.

(*) See Section 2.3.2.

TABLE II-3. PRELIMINARY SCREENING FOR SITE C (cont.)

Hazard	Applicable criteria*	Remarks
Ship/barge impact	3	There are no navigation channels near the site.
Collision of floating bodies	3	There are no water bodies close to the site.
Foundation ground instability	3	Site investigation demonstrated that no karst phenomena or underground caverns are present under the site. There are no water or oil wells that could produce subsidence at the site. Civil structures in this plant are founded on stable soft rock, with no expansion or consolidation phenomena.
Electromagnetic interference	1, 3	No sources of strong electromagnetic fields exist in the site vicinity. Design of instrumentation and control systems complies with Ref [7] regarding protection against lightning.
Blockage or diversion of river	3	This hazard does not apply to this site, since necessary water is stored on site
Biological phenomena	3	This hazard does not apply to this site, since necessary water is stored on site and biocides are used.
Depletion of a reservoir	3	This hazard does not apply to this site, since necessary water is stored on site
Freezing precipitation and frost related phenomena	4	This hazard will be studied within the hazard of 'Extreme Temperatures', which has not been screened out.
Extreme snowpack	--	Extreme snowpack hazard cannot be screened out at this stage. A bounding analysis has to be done in the next step to assess the allowable snowpack at roofs and to check that plant procedures are in place to avoid exceeding this level.
Variation of groundwater level	3	Ground water level in this site is very deep and variations do not have consequences on the plant.
Saltspray/Saltstorm	3	This phenomenon cannot take place at this site.
Waterspouts	3	This phenomenon cannot take place at this site.

(*) See Section 2.3.2.

ANNEX III: COMMENTARY

The methodology for plant capacity assessment presented in this publication is, in many aspects, a generalization of methods that have been in use for seismic assessment since the 1980s. Experience in the application to hazards other than seismic is more limited. The authors would like to call the attention about the following points:

(1) Criteria for screening out robust SSCs for seismic events have been well developed over the years using a combination of earthquake experience data and test data, [8]. Comparable screening criteria have not been compiled for other external hazards. Therefore, in those cases, the screening process needs to rely on engineering judgment and requires more elaborated analyses.

(2) Plant walkdown procedures for seismic events are well developed and have been applied at many nuclear power plants worldwide, [8]. Comparable, as well established procedures for other hazards do not exist. For most hazards, the external barriers of buildings protect the equipment and systems housed inside them. If the external barriers are breached, the equipment inside are generally assumed lost. Therefore, the walkdown method and procedures have to be specially tailored to each hazard.

(3) The CDFM method for computing HCLPF capacities (Section 4.2.3) was developed for seismic events and it has been applied in the seismic margin assessment of nuclear power plants in many Member States. Even though the application to other hazards is thought to be conservative (since the variability in the demand will be normally equal or less than for seismic hazards, see Ref [9]), the suitability of the method for other hazards has not been systematically tested so far.

(4) The Hybrid Approach (Section 4.3.4) has been developed and extensively applied for seismic events. However, the generic composite variability β_c values have not been established so far for fragilities of SSCs under other external hazards. When the approach is applied to other external hazards, it has to be noted that the lower the β_c values, the more conservative will be the fragility curve.

ANNEX IV: EXAMPLE OF SELECTION OF STRUCTURES, SYSTEMS AND COMPONENTS

The methodology for plant capacity assessment presented in this publication is, in many aspects, a generalization of methods that have been in use for seismic assessment since the 1980s. Experience in the application to hazards other than seismic is more limited. The authors would like to call the attention about the following points:

(5) Criteria for screening out robust SSCs for seismic events have been well developed over the years using a combination of earthquake experience data and test data, [8]. Comparable screening criteria have not been compiled for other external hazards. Therefore, in those cases, the screening process needs to rely on engineering judgment and requires more elaborated analyses.

(6) Plant walkdown procedures for seismic events are well developed and have been applied at many nuclear power plants worldwide, [8]. Comparable, as well established procedures for other hazards do not exist. For most hazards, the external barriers of buildings protect the equipment and systems housed inside them. If the external barriers are breached, the equipment inside are generally assumed lost. Therefore, the walkdown method and procedures have to be specially tailored to each hazard.

(7) The CDFM method for computing HCLPF capacities (Section 4.2.3) was developed for seismic events and it has been applied in the seismic margin assessment of nuclear power plants in many Member States. Even though the application to other hazards is thought to be conservative (since the variability in the demand will be normally equal or less than for seismic hazards, see Ref [9]), the suitability of the method for other hazards has not been systematically tested so far.

(8) The Hybrid Approach (Section 4.3.4) has been developed and extensively applied for seismic events. However, the generic composite variability β_c values have not been established so far for fragilities of SSCs under other external hazards. When the approach is applied to other external hazards, it has to be noted that the lower the β_c values, the more conservative will be the fragility curve.

Introduction

The purpose of this annex is to illustrate the process of selection of SSCs for vulnerability assessment described in Section3 of the main body of this publication.

For this purpose, the event tree/fault tree approach (Section 3.3) is followed for a typical PWR plant. As mentioned in the main body of the publication, this approach is very efficient when a validated Internal Event Level 1 PSA is available.

In the following sections, the suggested steps for application are given, together with a brief commentary on each of them.

Plant initial conditions induced by the applicable hazard

The plant is assumed to be operating ‘at-power’ and, using Table 2 of the main body of the publication, the analyst finds out that the applicable hazard induces a ‘Loss of Off-site Power’ (LOOP) and a ‘Small Loss of Coolant Accident’ (SLOCA).

Safety functions

Under the induced plant initial conditions, fundamental safety functions need to be maintained (Section 3.1). According to this requirement, the analyst selects the following plant specific functions to be maintained:

1) Reactor sub-criticality
2) Emergency core cooling (early)
3) Emergency core cooling (late)
4) Containment isolation
5) Containment overpressure protection

Identification of frontal systems

In order to perform the functions selected in the previous step the analyst identifies the following frontal systems. Numbers indicate the associated function(s):

- Chemical and volume control system (1)
- High pressure safety injection (1) (2)
- Reactor protection system (1)
- Auxiliary feed water system (2)
- Main steam system (bleed) (2)
- Low pressure injection system (2)
- Residual heat removal system (3)
- Safety injection accumulators (2)
- Containment spray system (5)
- Containment cooling system (5)
- Containment isolation system (4)
- Combustible gas control system (5)

Identification of support systems

For the frontline systems identified in the previous step, the analyst identifies the following first order support systems:

- Condensate storage and transfer system
- Refuelling water storage system
- Component cooling water system
- Auxiliary building HVAC system
- Engineering safeguards actuation system
- AC/DC power supply system (including UPS)
- Standby AC power supply system
- Alternate AC power supply system
- Instrumentation and control system
- Accident monitoring system

The second order support systems are as follows:

- Essential service water system
- Component cooling system
- Chilled water system
- Essential chilled water system
- Control building HVAC system
- Standby AC power fuel system (diesel, gas, etc.)

Consideration of plant conditions

The 'loss of off-site power' makes some of the identified support systems unavailable. Particularly, those which are not supplied from the safety buses. As a consequence, the following support systems may also be unavailable:

- Non-essential service water system
- Non-essential component cooling system
- Chilled water system
- Non-essential compressed air system
- Non-essential HVAC system

Event trees from Internal Event Level 1 PSA

According to the assumed plant conditions, two event trees are selected from the Internal Event Level 1 PSA, corresponding to the following initiating events:

- Loss of off-site power (LOOP)
- Small LOCA (SLOCA)

The analyst verifies that the system functionalities required to mitigate these initiating events in the Internal Event PSA are the same as required in the present analysis.

With respect to the LOOP, the analyst finds out that in the Internal Event PSA the possibility of external power recovery in the short term is considered. This possibility has to be disabled for the present analysis.

With respect to the SLOCA, the analyst confirms that the required functionalities are the same.

Identification of components in frontal and support systems

Basic events in Internal Events PSA models

The analyst takes basic events from the Internal Events PSA model corresponding to the event trees identified in the previous section.

An initial list of selected SSCs is compiled by taking the plant components associated to these basic events. Basic events representing corrective or preventive maintenance and common cause failures are not considered, since they do not add additional plant components to the list.

However, basic events related with required human actions are analysed to find the components needed to provide the necessary indicators in the control room. Those components are included in the list as well.

Finally, the analyst looks into basic events modelled as 'special basic events' to check if they are associated to any components not yet included in the list. In such a case, those components are added.

From the resulting list, the analyst eliminates components belonging to systems not identified as required frontal and support systems (see above) or components which are disabled by the LOOP (see above).

Components not modelled in PSA

In this step the analyst adds the components in the frontal and support systems which have not been modelled in the Internal Events Level 1 PSA. This is normally the case of passive components, whose probability of random failure is much smaller than in the active components. This step is very important, since failure in the present vulnerability study can be not only random, but caused by the extreme event. It could happen that the plant's SSCs more vulnerable to the extreme event are passive.

Hence, in this step the analyst adds to the Selected SCC list items such as tanks, heat exchangers, structures, HVAC ducts, cable trays, piping, etc.

Grouping of SSCs for vulnerability assessment

The list resulting from the previous steps will likely contain a large number of items that, in reality are sub-components of the same physical plant component.

During the capacity assessment, most SSC failure modes corresponding to external hazards can be analysed after grouping together the different sub-components of the same equipment item into a single item. This is sometimes called the 'rule-of-the-box'. Following this rule, for example, the body, the actuator and the limit switches of a motor operated valve will appear as a single equipment item in the Selected SSC List; or all the subcomponents of a diesel generator mounted on the same skid will appear as a single item in the Selected SSC List.

In this step, the analyst goes through the list and applies the 'rule-of-the-box' to the sub-components. Examples of application are as follows:

- Electrical devices such as coils, switches, relays, protective devices, electronic boards, motor starters, etc. are associated to the electrical cabinet or panel in which they are mounted;
- Limit switches in actuated valves are associated the valve itself;
- Transformers installed inside a cabinet are associated to the cabinet;
- Appurtenances mounted on diesel engines are associated to the diesel engines;
- Passive valves and filters are associated to the pipe itself, since for most of external hazards they are less vulnerable than the pipe.

List of Selected SSCs

As a final result of this process, the analyst has a list of Selected SSCs to use in the vulnerability assessment. For each item in the list the following information is given in Table IV–1:

TABLE IV–1 SYSTEM/COMPONENT SPECIFIC INFORMATION

ID:	Plant tag or plant identification of the item
Description:	Brief description (e.g. horizontal pump, motor control centre, refuelling tank)
Location:	Location of the item (e.g. plant area, plant building, elevation, room)
System:	Identification of a system, identification of necessary support
Applicable hazard(s):	Identification of a hazard (or combination of hazards) that could challenge functionality or performance of a system/item
Intended function:	Required functionality in order to keep the fundamental safety functions (e.g. structural integrity, pressure boundary, functional, change state)
Initial qualification/protection:	Information on initial qualification for anticipated external/internal hazard(s)
Failure mode of an item:	Information on consequence if item fails, impact on safety performance
Margin assessment:	Information, whether the item has sufficient margin for identified hazard, or needs to be reinforced

REFERENCES TO THE ANNEXES

[1] U.S. DEPARTMENT OF ENERGY, Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities, DOE-STD-1020-94, Washington DC (1994).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-3.1, IAEA, Vienna (2002).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Volcanic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-21, IAEA, Vienna (2012).

[4] U.S. NUCLEAR REGULATORY COMMISSION, Evaluation of External Hazards to Nuclear Power Plants in the United States - Other External Events, NUREG/CR-5042, Supplement 2, Washington DC, February 1989.

[5] U.S. NUCLEAR REGULATORY COMMISSION, Evaluation of External Hazards to Nuclear Power Plants in the United States, NUREG/CR-5042, Washington DC (1987).

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

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

[8] ELECTRIC POWER RESEARCH INSTITUTE, A Methodology for Assessment of Nuclear Power Plant Seismic Margin, Report EPRI NP-6041-SL, Rev. 1, Palo Alto, California (1991).

[9] R. P. KENNEDY, Overview of Methods for Seismic PRA and Margins Methods Including Recent Innovations, in Proceedings of the OECD Nuclear Energy Agency Workshop on Seismic Risk, Tokyo, August 10-12, 1999.

GLOSSARY

The following definitions apply for the purposes of this TECDOC.
Further definitions are provided in the IAEA Safety Glossary:
Terminology Used in Nuclear Safety and Radiation Protection (2007 Edition),
IAEA, Vienna (2007): http://www-ns.iaea.org/standards/safety-glossary.asp

'as-is' condition: The 'as-is' condition of an installation refers to the present state and actual condition of the NPP, considering the 'as-built', 'as-operated' and 'as-maintained' state of structures, systems and components.

aleatory variability: The variability inherent in a non-deterministic (i.e., stochastic, random) phenomenon. Aleatory variability is accounted for by modelling the phenomenon in terms of a probability model. In principle, aleatory variability cannot be reduced by the accumulation of more data or additional information, but the detailed characteristics of the probability model can be improved. Sometimes aleatory variability is called 'randomness'.

design basis external event: External event explicitly taken into account in the design of a NPP, according to established criteria, such that the NPP can withstand them without exceeding authorized limits by the planned operation of safety systems or structures.

epistemic uncertainty: Uncertainty attributable to incomplete knowledge about a phenomenon that affects the ability to model it. Epistemic uncertainty is captured by considering a range of model parameters within a given expert interpretation or multiple expert interpretations, each of which is assigned an associated weight representing statistical confidence in the alternatives. In principle, epistemic uncertainty can be reduced by the accumulation of additional information associated with the phenomenon. The uncertainty in the parameters of the probability distribution of a random phenomenon is epistemic.

event: An event is any occurrence unintended by the operator of the NPP, the consequences or potential consequences of which are not negligible from the point of view of safety. An event can be considered as the materialization of a hazard.

external event: Event which is unconnected with the operation of the NPP. Typically, an 'external event' originates outside the site. However, in some cases, events originating on the site but outside the safety related buildings can be treated as external events if the characteristics of the generated effects are similar to those caused by off-site events,.

extreme external event: External event that exceeds the design basis of the existing nuclear installation.

front line system: A frontline system is a system that is capable of directly performing one of the accident mitigating functions, e.g. reactivity control, core heat removal, etc.

hazard: A natural or human-induced phenomenon that poses some risk to a NPP. Internal hazards include phenomena such as equipment failure or human failure. External hazards include phenomena such as flooding and fires external to the plant, tornadoes, earthquakes, and aircraft crashes. A particular 'hazard' materializes itself in 'events'. Typically, a 'hazard' is defined by a relationship between the strength of the hazard and the annual frequency of exceeding this strength (hazard curves).

plant-level capacity: Strength of a hazard that compromises the safety of a plant. Here, the compromising of safety means that the plant is rendered incapable of achieving safety objectives under the impact of an event having such a level of strength or higher. Further, the 'margin' and 'capacity' are often used synonymously with reference to expressing the capability of a plant or its component to perform its intended function when subjected to the

effects of a hazard. In this report, 'capacity' is referred to the margin of a component whereas 'margin' refers to the plant capacity to withstand the hazard, performing the safety functions.

vulnerability: Any of those structures, systems or components more prone to failure for a particular external hazard. Vulnerabilities are the 'less strong' items or the 'weak links' against a particular external hazard. In the context of this report, the term corresponds to a relative concept, rather than to an absolute concept (i.e., some components are more vulnerable than others). In this sense, any plant will have 'vulnerabilities', which is not intended to mean non-compliance with a safety requirement.

weak link: See 'Vulnerability'.

ABBREVIATIONS AND ACRONYMS

AC	alternate current
APC	atmospheric pressure change
AOO	anticipated operational occurrences
CDFM	conservative deterministic failure margin
EPRI	Electric Power Research Institute
FMEA	failure mode and effect analysis
HCLPF	high confidence of low probability of failure
HVAC	heating, ventilation and air conditioning
IAEA	International Atomic Energy Agency
ICOLD	International Commission on Large Dams
IPEEE	individual plant examination of external events (US-NRC program)
ISRS	in-structure response spectra
LOCA	loss of coolant accident
LOOP	loss of off-site power
LRF	large release frequency
NPP	nuclear power plant
NRC	U. S. Nuclear Regulatory Commission
NTTF	near term task force (US-NRC activity)
PMF	probable maximum flood
PSA	probabilistic safety assessment
PSHA	probabilistic seismic hazard analysis
PTHA	probabilistic tsunami hazard analysis
PWR	pressurized water reactor
RLE	review level earthquake
SBO	station black-out
SFP	spent-fuel pool
SMA	seismic margin assessment
SLOCA	small loss of coolant accident
SPSA	seismic probabilistic safety assessment
SSC	structure, system or component
UHRS	uniform hazard response spectra
US	United States of America
UPS	uninterruptible power supply
WTC	World Trade Center

CONTRIBUTORS TO DRAFTING AND REVIEW

Andel, J.	ÚJV Řež, Czech Republic
Beltran, F.	International Atomic Energy Agency
Benitez, F.	IBERDROLA Ingeniería y Construcción, Spain
Coman, O.	International Atomic Energy Agency
Dababneh, A.	RIZZO Associates, United States of America
Duchac, A.	International Atomic Energy Agency
Ferrante, F.	Nuclear Regulatory Commission, United States of America
Galan, M.	Electricité de France, France
Gupta, A.	North Carolina State University, United States of America
Haddad, J.	International Atomic Energy Agency
Jimenez, A.	Consejo de Seguridad Nuclear, Spain
Kim, M.	International Atomic Energy Agency
Labbe, P.	Electricité de France, France
Maly, J.	ÚJV Řež, Czech Republic
Morita, S.	International Atomic Energy Agency
Poveda, A.	International Atomic Energy Agency
Rizzo, P.	RIZZO Associates, United States of America
Samaddar, S.	International Atomic Energy Agency
Yllera, J.	International Atomic Energy Agency

Consultants Meetings
Vienna, Austria, 28-30 January 2015
Vienna, Austria, 9-10 June 2015

Technical Meeting
Vienna, Austria, 23 – 27 November 2015

IAEA
International Atomic Energy Agency

No. 25

ORDERING LOCALLY

In the following countries, 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.

CANADA

Renouf Publishing Co. Ltd

22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: www.renoufbooks.com

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com Web site: www.rowman.com/bernan

CZECH REPUBLIC

Suweco CZ, s.r.o.

Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: www.suweco.cz

FRANCE

Form-Edit

5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: www.form-edit.com

GERMANY

Goethe Buchhandlung Teubig GmbH

Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: www.goethebuch.de

INDIA

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: www.bookwellindia.com

ITALY

Libreria Scientifica "AEIOU"

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: www.libreriaaeiou.eu

JAPAN

Maruzen-Yushodo Co., Ltd

10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: www.maruzen.co.jp

RUSSIAN FEDERATION

Scientific and Engineering Centre for Nuclear and Radiation Safety

107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: www.secnrs.ru

UNITED STATES OF AMERICA

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

Renouf Publishing Co. Ltd

812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: www.renoufbooks.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 2600 29302 or +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/books

17-51331

International Atomic Energy Agency
Vienna
ISBN 978–92–0–108817–8
ISSN 1011–4289