Safety Reports Series

No. 88

# Safety Aspects of Nuclear Power Plants in Human Induced External Events: Margin Assessment

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.

# SAFETY ASPECTS OF NUCLEAR POWER PLANTS IN HUMAN INDUCED EXTERNAL EVENTS: MARGIN ASSESSMENT

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''.

SAFETY REPORTS SERIES No. 88

# SAFETY ASPECTS OF NUCLEAR POWER PLANTS IN HUMAN INDUCED EXTERNAL EVENTS: MARGIN ASSESSMENT

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2017

# COPYRIGHT NOTICE



Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books



Printed by the IAEA in Austria
March 2017
STI/PUB/1723

**IAEA Library Cataloguing in Publication Data**

Names: International Atomic Energy Agency.
Title: Safety aspects of nuclear power plants in human induced external events : margin assessment / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2017. | Series: IAEA safety reports series, ISSN 1020–6450 ; no. 88 | Includes bibliographical references.
Identifiers: IAEAL 16-01068 | ISBN 978–92–0–111415–0 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Safety regulations. | Nuclear power plants — Management. | Nuclear power plants — Design and construction — Safety measures.
Classification: UDC 621.039.58 | STI/PUB/1723

# FOREWORD

Many human actions pose challenges to the safe operation of a nuclear installation, such as a nuclear power plant. These challenges may arise from activities human beings undertake as a part of routine life. The challenges arising from intentional and accidental events need to be evaluated given the current design robustness of the installation and the vulnerability of the location of such events.

This publication is the third of three Safety Reports on the safety assessment of nuclear facilities subjected to extreme human induced external events. These publications address the assessment of nuclear installations subjected to accidental or unintentional human actions. They provide the general framework for approaches to obtaining the overall plant performance with regard to the fundamental safety functions from the performance of individual components. It includes safety assessments, the characterization and quantification of loadings, and appropriate analysis techniques and material properties for capacity assessments. This publication explores established methodologies in the light of recent advances in the understanding of material behaviour under such extreme loading conditions and computational techniques that can incorporate such behaviour in the analytical modelling.

These three Safety Reports were developed using funding from Member States voluntarily contributing to, and participating in, the extrabudgetary programme of the External Events Safety Section (EESS-EBP). Established in 2007, the EESS-EBP has developed technical documents considered a priority for Member States, given the current experience with severe external events globally. The aim of the programme is to provide technical inputs to current and future IAEA safety standards. The EESS-EBP implements these activities by assimilating the latest technical issues and practical methodologies in Member States, and disseminates the information through technical publications, sharing them in the working groups, and by participating in global conferences and forums.

The work of all the contributors to the drafting and review of this publication is greatly appreciated. In particular, the IAEA gratefully acknowledges the contributions of M.K. Ravindra (United States of America) to the drafting of this publication, and of A. Blahoianu and N. Orbovic (Canada) to its review. The IAEA officers responsible for this publication were A. Altinyollar and F. Beltran of the Division of Nuclear Installation Safety.

*EDITORIAL NOTE*

*Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.*

*This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.*

*Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.*

*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 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

A nuclear power plant needs to operate safely during and after an external event, satisfying IAEA Safety Standards Series No. SF-1, Fundamental Safety Principles [1]. IAEA Safety Standards Series No. NS-R-3 (Rev. 1), Site Evaluation for Nuclear Installations [2], addresses the evaluation of a nuclear power plant site and the assessment of site hazards due to human induced external events. In addition, IAEA Safety Standards Series No. NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants [3], describes the guidance for meeting these requirements. Requirements and guidelines for safety in the design against human induced external events are dealt with in IAEA Safety Standards Series Nos SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [4], and NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants [5], respectively. However, with the increase in safety concerns with regard to nuclear power plants, the need to assess safety against events not considered during siting or design has become apparent, and existing IAEA publications are not necessarily adequate for handling the specific issues arising in this case.

There is general agreement among experts that the current practice for nuclear facility design provides such a level of 'safety margin' and robustness that some events not explicitly considered at the design stage may be accommodated by the nuclear facilities in their current configuration without significant radiological consequences. This is believed to be true for nuclear facilities in general and nuclear power plants specifically. Quantification of this 'safety margin' might be required for some events which could not be screened out in a safety evaluation process.

Experience suggests that the 'margin assessment' method is an effective tool to assess the overall safety of a nuclear power plant against a hazard, by evaluating its capacity to safely withstand the impact of the beyond design basis event. At some nuclear power plants, certain hazards may not have been considered in the design basis. In the case of new plants, the margin assessment evaluates the capability of the plant for safe operation beyond design basis. For an existing plant, such assessment is prompted by one or more of the following:

(a) The perception of a greater hazard on the site than is considered in the design basis;

(b) Regulatory requirements, such as periodic safety reviews, to ensure that the plant has adequate margins against all credible human induced external events;
(c) The lack of design attributes to withstand applicable human induced external events;
(d) New technical findings, such as the vulnerability of some structures, systems and components (SSCs), and other feedback and experience from real incidents.

A margin assessment programme evaluates the current capability of the plant (i.e. the plant 'as is') to withstand human induced external events and to identify any necessary upgrades or changes in operating procedures. Currently, there is not an IAEA safety standard which covers the subject of margin assessment of nuclear power plants against human induced events similar to IAEA Safety Standards Series No. NS-G-2.13, Evaluation of Seismic Safety for Existing Nuclear Installations [6]. The purpose of this Safety Report is to bridge this gap; this publication is prepared in the spirit of the IAEA safety standards and can be considered as a methodology or approach to implement their intent.

This publication is the third in a series of three Safety Reports that has been produced to describe, generally and specifically, the approaches to addressing human induced external events with a focus on nuclear power plants. The three reports provide guidance to support the quantitative evaluation of the engineering safety of facilities subjected to accidental or postulated human induced external events. In addition to this Safety Report, they include:

(a) Safety Aspects of Nuclear Power Plants in Human Induced External Events: General Considerations, Safety Reports Series No. 86 [7];
(b) Safety Aspects of Nuclear Power Plants in Human Induced External Events: Assessment of Structures, Safety Reports Series No. 87 [8].

The first report in the series provides the general framework and includes a roadmap on how to perform the design and the evaluation of the protection against human induced external events. The Safety Report concentrates on an overall view of the methodology and on the important considerations for its application to existing and new nuclear power plants. Topics covered include elements of the design and evaluation approach, developed in five phases:

— Phase 1: Event identification;
— Phase 2: Hazard evaluation and load characterization;
— Phase 3: Design and evaluation approaches to SSCs;

— Phase 4: Plant performance assessment and acceptance criteria;
— Phase 5: Operator response.

The second report in the series addresses phases 2 and 3 of the general framework. It provides detailed guidelines for the safety assessment of nuclear power plant structures against mechanical impacts, explosions and fire hazards caused by human induced external events. The report covers the characterization of loading, the assessment of structural integrity using both simplified methods and more elaborated methodologies, and the assessment of induced vibration. Acceptance criteria are given in the report for different failure modes: overall stability, overall bending and shear, local failure modes and induced vibrations. In addition, since many of the human induced external events may result in a fire, the process of analysing the fire consequences is also given. Approaches to assessing the barrier fire performance and the fire performance of SSCs are also given.

This publication is the third in the series. It addresses phases 1 and 4 of the general framework. This Safety Report describes the procedures for assessing the safety margins of nuclear power plants against human induced external events. Both postulated and accidental hazards are considered. This publication focuses on plant and systems performance evaluations. A tiered approach to margin assessment is provided. The first tier consists of a deterministic procedure in which, for each scenario, the existence of at least one undamaged success path[1] to comply with the fundamental safety function is investigated. This procedure can be extended to calculate probability measures such as the conditional core damage probability (CCDP) and the conditional probability of loss of spent fuel pool cooling and spent fuel damage, given the scenario. In the most elaborated stage, probabilistic safety assessment (PSA) techniques are introduced, giving consideration to the probabilistic aspects of the hazards and of SSC capacity (fragility). Event tree and fault tree models are used to compute usual PSA metrics, such as core damage frequency, large early release frequency, and frequency of loss of spent fuel pool cooling and spent fuel damage.

In summary, these three publications in the Safety Reports Series provide methodologies that can be used in the evaluation of the SSC capacity of nuclear power plants subjected to extreme human induced external events and in the assessment of the resulting safety margin of the facilities. The three publications may be useful to nuclear facility owners, operators and regulators who need an understanding of the safety issues in relation to human induced events. They contain descriptions of internationally accepted methods applied by the

[1] A success path is a set of systems and associated components that can be used to bring the plant to a stable hot or cold shutdown condition and to maintain this condition for a specified period of time.

engineering community and some examples that may be useful in the evaluation of the need for plant upgrading. Many references are also provided for more detailed guidance, and the publications rely on many IAEA safety standards and relevant technical publications.

The three Safety Reports have a common thread and are closely related to each other. Together, they provide an approach to the assessment against extreme human induced external events fully consistent with the methods used for evaluation of nuclear facilities subjected to extreme natural events, such as earthquakes and floods.

## 1.2. OBJECTIVE

The objective of this Safety Report is to provide detailed methodology and procedures for assessing the safety margins of nuclear power plants against human induced events of either the postulated type or accidental type. The margin is assessed for given hazards using both probabilistic and deterministic approaches. The margin is quantified with best estimate or conservative values, such as the high confidence of low probability of failure (HCLPF) value. While the emphasis of this publication is on margin assessment, risk metrics such as core damage frequency and frequency of loss of integrity of the spent fuel pool could be calculated for external hazards of an accidental type.

## 1.3. SCOPE

In this Safety Report, the margin assessment procedures for human induced events of accidental origin or postulated type are presented. While this Safety Report provides detailed methodology and procedures for assessing the safety margins against human induced external events at both existing and new nuclear power plants, it does not provide margin acceptance criteria. That is, the margin is assessed based on the criteria given in Ref. [7] and the structural acceptance criteria given in Ref. [8]. However, no indication on whether or not the margin is acceptable is provided in this publication. The acceptability of the margin depends on the safety goals established by the Member State.

The hazards covered in this Safety Report are aircraft crashes, explosions and fires. This publication covers the overall process for the margin assessment. It addresses the different tasks of margin assessment, such as: accident sequence analysis; systems analysis; in-plant evaluations; evaluation of SSC capacity; and margin assessment (deterministic and probabilistic method) of the systems

and plant. It also describes the approach to identifying critical components and systems for upgrading.

The evaluation of hazards (i.e. the calculation of the frequency of occurrence) due to human induced external events does not fall under the scope of this Safety Report. It is considered that the hazard evaluation has been conducted and the hazard parameters that are necessary for margin assessment are available.

The methodology described here is principally developed for nuclear power plants. However, information provided may be useful for the margin assessment of other nuclear installations. Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

## 1.4. STRUCTURE

Section 2 discusses the general considerations and introduces the approach and concepts of margin assessment. The composition of the margin assessment team is outlined. Section 3 describes the procedure for the assessment of the margin against human induced events. Depending on the application, the margin could be a best estimate margin or conservative margin for each affected SSC. The plant margin could similarly be stated using deterministic evaluation — the success path approach — or probabilistic evaluation using the PSA approach. Section 4 describes the review of plant design and plant walkdown, also known as in-plant evaluation. This is a key component of the overall workflow described in Section 3. Margin assessment for different hazards is described in Section 5, using the hazards from aircraft crashes and explosions as examples. Section 6 discusses the different strategies for enhancing the margins.

Annex I outlines an example of reference parameters for loading effects. Annex II illustrates the application of PSA methods to an aircraft crash. Annex III demonstrates how a simplified PSA method could be used in the evaluation of explosion induced pressure loading. Annex IV describes how accident management could help to mitigate an accident from a human induced external event.

# 2. GENERAL CONSIDERATIONS

## 2.1. CONCEPTS

### 2.1.1. Margin

The term margin in the context of this Safety Report is the level of a hazard that compromises the safety of a nuclear power plant. Here, the compromising of safety means that the plant is rendered incapable of achieving safety objectives under the impact of the hazard. Margin and capacity are often used synonymously in reference to the capability of a plant or its component to perform its intended function when subjected to the effects of a hazard. In this publication, however, capacity refers to the margin of a component performing the safety functions, whereas margin refers to the plant capacity to withstand the hazard.

The objective of margin assessment of a nuclear power plant against a human induced external event is to determine the level of the hazard resulting from a human induced external event at which the safety objectives of the plant would be compromised; that is, the plant will cease to perform the basic safety functions (see Section 2.2). The margin assessment process also covers the work of identifying the weak points and areas of improvement for engineering the upgrades to ensure that the safety of the plant is in line with current requirements.

Margin or capacity could be quantified as a best estimate value or a conservative value (e.g. the HCLPF value), depending on the selected hazard level. The best estimate plant margin is calculated using the best estimate capacities of relevant SSCs. The best estimate (mean or median) capacity of the SSCs is derived from realistic models (i.e. load characterization, failure modes and material properties) for a postulated hazard. The HCLPF value of the plant margin is defined as the 1% probability of failure value on the mean plant level fragility curve developed in terms of a reference parameter using the event tree and fault tree model of the plant. This value is defined as equivalent to a high confidence (95%) of low probability of failure (5%).

The plant margin can also be evaluated using the deterministic approach of ‘success path’. The success path is a set of systems and associated components that can be used to bring the plant to a stable hot or cold shutdown condition and to maintain this condition for a specified period of time (e.g. at least 72 hours). Similarly, a success path for the integrity of the spent fuel pool and ultimate heat sink could be developed. The HCLPF value of the plant margin is considered to be equal to the lowest HCLPF capacity of the components on the success path.

### 2.1.2. Impact of human induced external events

The basic steps in the evaluation of human induced external events are:

— Event identification;
— Hazard evaluation and load characterization;
— Design and evaluation approaches to SSCs;
— Plant performance assessment and acceptance criteria.

In the first steps, once the relevant hazards have been identified, the impact (loading) on the nuclear power plant resulting from each hazard has to be defined. NS-G-3.1 [3] describes the human induced external events that need to be considered in site evaluation for nuclear power plants. Table I of NS-G-3.1 [3] lists the sources and associated initiating events. The sources could be stationary (e.g. an oil refinery) or mobile (e.g. railway trains and wagons near the plant). The initiating events associated with each hazard are identified. These could be an impact of projectiles, explosions, fires and chemical releases.

Table II of NS-G-3.1 [3] describes the evolution of events and their impacts (loads) on the nuclear power plant. For example, explosion (deflagration or detonation) could result in the following [3]:

— Explosion pressure waves;
— Projectiles;
— Smoke, gas and dust produced in the explosion drifting towards the plant;
— Associated flames and fires.

Aircraft as well as other types of vehicle crash could also result in projectiles (missiles) and fire.

Table III of NS-G-3.1 [3] lists the parameters that could be used to characterize each loading case. For example, the pressure wave is characterized by the local pressure at the plant as a function of time. The projectile is characterized by the mass, velocity, shape, size and type of material. Maximum heat flux and duration are used to characterize the impact of heat. Also listed are the consequences of the impact. A projectile could have the following consequences:

— Perforation, penetration, spalling and scabbing of concrete structural elements;
— Disruption of systems and components;
— Collapse of parts of the structure;
— False signals in the equipment, induced by vibration.

A single reference value for the parameter could efficiently be used to calculate the capacity and fragility of the SSCs (i.e. the maximum value of the overpressure is used instead of the entire time history in the case of a pressure wave due to an explosion). This is similar to the use of peak ground acceleration to represent the ground motion spectrum of an earthquake. For the projectile, the geometrical and mechanical properties such as the mass, shape, size and type of material are defined. The velocity is used as the reference parameter. For heat, the maximum thermal flux could be used as the reference parameter, although the consequence of this impact depends on the duration of the heat and the firefighting activities, which are modelled in the PSA. Annex I provides examples of reference parameters of the loading effects caused by these hazards.

### 2.1.3. Margin assessment

The concept of margin assessment of a nuclear power plant against any hazard comes from the area of evaluation of plant capability to withstand beyond design basis earthquakes. Nuclear power plants are complicated systems, and the margin can be provided by multiple combinations of SSCs performing their intended functions. The optimum combination for a given hazard might not be apparent at first sight. The concept is illustrated in the following example, in which the margin approach has been applied and, for extreme events, a safe shutdown path without redundancy has been identified. Furthermore, the emergency power element of the safe shutdown path comprises Train A. Diesel Generator A is housed in its dedicated diesel generator building (DGB-A), isolated and separated from other diesel generator buildings on-site. An aircraft crashes into the nuclear power plant, impacting DGB-A. The evaluation of DGB-A and its components within, demonstrates very low capacity (median or HCLPF) values for an aircraft crash and consequently would dictate the plant median capacity or HCLPF capacity. If redundancy were introduced into the safe shutdown path, it may be shown that the effective footprint of the aircraft crash could not reasonably be assumed to disable both trains simultaneously. Thereby, with a reintroduction of the postulated event specifics, the initial evaluation may be revisited and a more realistic plant capacity may be established.

## 2.2. SAFETY OBJECTIVES

Margin assessment of a nuclear power plant against the hazards due to human induced events is aimed at assessing the capability of the plant to withstand the impact of the hazards in performing the following safety functions:

(a) Shutting down the reactor safely;
(b) Maintaining shutdown condition;
(c) Removing long term decay heat;
(d) Containing radioactive material;
(e) Preventing or mitigating the consequences of the event.

In addition, margin assessment is to be extended to cover the spent fuel pool and ultimate heat sink. In the case of the spent fuel pool, safety functions (c) and (d) are relevant to margin assessment. The margin assessment of ultimate heat sink needs to be carried out with reference to its structural integrity and continued functionality. For the spent fuel pool, both fuel damage and loss of liner integrity need to be examined.

## 2.3. PLANT OPERATING STATES AND ASSUMPTIONS

Margin assessment against human induced events needs to consider all operating states of the plant (i.e. full power, low power and shutdown condition). The plant should be capable of being brought to, and maintained in, a safe shutdown condition for as long as the recovery actions are required following the occurrence of a human induced event. While evaluating the margin, the following assumptions are made:

(a) Internally generated loss of coolant accident (LOCA) and high energy line breaks are not postulated concurrent with the human induced external event.
(b) Simultaneous off-site and plant generated power loss occurs for at least 24 hours, if applicable to the human induced event.
(c) The loss of make-up water capacity from off-site sources occurs for at least 24 hours.
(d) Other independent external events such as fires, flooding and tornadoes are not postulated to occur simultaneously.

## 2.4. APPLICATION TO EXISTING AND NEW NUCLEAR POWER PLANTS

The methods described in this Safety Report are applicable to both existing and new nuclear power plants. In the case of existing plants, the margin against human induced events comes from the inherent robustness of design and plant response to the events, which greatly depend on operational procedures, personnel training and emergency preparedness.

For new plants, the designer has additional options. For instance, certain buildings (e.g. the containment and spent fuel pool building) could be strengthened to provide acceptable margins, or the plant layout could be improved to maximize the benefit of redundancy and separation.

In the following, the difference in the application to existing and new plants is explained. The capacity of the plant needs to be assessed for scenarios with three different levels of event magnitude: tiers one, two and three. Under the tier one scenario, the new plant is required to perform as required for a general design basis event. Following a tier one scenario, the plant is to be the same structurally and functionally as before.

Under the tier two scenario, a safe shutdown path is required that comprises at least one means of:

— Reactor shutdown;
— Fuel cooling;
— Retention of radioactive material from the reactor.

Structural integrity needs to be sufficient to protect important safety systems. If a deterministic approach is pursued, two such success paths are to be identified where practicable.

For tier three, there is at least one means to ensure the reactor shutdown and core cooling. Degradation of the containment barrier may allow the release of radioactive material. However, the degradation needs to be limited, with the goal that the dose acceptance criteria are not exceeded. In these cases, the response may require on-site and off-site emergency measures.

In the context of Refs [7, 8], tier two and tier three scenarios are termed design extension external events: DEE 1 and DEE 2, respectively. This is consistent with the terminology used by some Member States [9].

For existing facilities which are not designed against human induced external events, the acceptance criteria for tier one will probably not be met. The analysis needs to focus on tier two and tier three scenarios. Special attention is to be paid to tier three scenarios, as they define the ultimate limit state of the plant for human induced external events and therefore appropriate on-site and off-site emergency measures may be necessary.

In the analysis of the plant under human induced external events, special focus is on the assessment of the behaviour of non-redundant systems, such as the containment system. The scenarios need to cover a direct impact on the containment building (e.g. an aircraft crash). It should be noted that there is a difference in the assessment of the capacity of the containment structure for existing and new plants. For example, in the case of an aircraft crash:

(a) For new plants, a general design approach to an aircraft crash has two steps: define the containment wall thickness for the local behaviour under aircraft engine impact and verify the structural adequacy with a given loading function due to the fuselage impact for global behaviour.
(b) For the structures in existing plants in most cases, the first step can already result in a failure. In this case, the assessment of global and local effects cannot be uncoupled. Taking into account the level of uncertainties in this type of analysis, sensitivity studies need to be performed independently, with at least two independent models. If the bounding case of sensitivity studies shows that the aircraft will perforate the containment building, a conservative analysis needs to be performed to define necessary on-site and off-site emergency measures.

The margin assessment would provide insights on the inherent strength and weakness of the plant, which need to be addressed to enhance safety.

## 2.5. COMPOSITION OF MARGIN ASSESSMENT TEAM

The margin assessment team consists of nuclear power plant staff and consultants with the required expertise. The tasks and responsibilities of the team leader and members are as follows:

(a) The team leader needs to have the authority, supervisory skills, appropriate engineering background and thorough understanding of security information control necessary to supervise the activities and to ensure the security and integrity of the process. The team leader is to be nominated by the plant management. The team leader supervises the field activities, engineering evaluations and security requirements. The plant management and team leader select other team members.
(b) Engineering safety experts (expert plant staff and, if necessary, consultants with the required expertise) comprise the margin assessment team focused on engineering safety aspects. The engineering disciplines that are to be represented include PSA systems, hazard analysis, civil, structural,

mechanical, electrical, fire protection, and instrumentation and control. All engineering disciplines are considered in each evaluation to ensure completeness.

(c) Plant operations personnel are an essential component of the team, and their expertise needs to be available throughout the plant walkdown activities.

# 3. PROCEDURE FOR MARGIN ASSESSMENT AGAINST HUMAN INDUCED EVENTS

## 3.1. PROCESS FOR MARGIN ASSESSMENT

The flow chart for the margin assessment of nuclear power plant against human induced events is depicted in Fig. 1. The left hand side of this figure shows the deterministic branch; the right hand side shows the probabilistic branch. Depending on the specific needs of the Member State, the deterministic branch, the probabilistic branch or both could be employed. The tasks pertaining to these two branches are first briefly described. In subsequent sections, the major tasks are discussed in detail.

The first task is the identification of human induced events that need to be considered (e.g. aircraft crashes, explosions, projectiles and transport accidents). It is then assessed whether the hazard is of accidental origin or postulated type. In the case the hazard is accidental in origin, the frequency of occurrence of the hazard is derived and is used in the quantification process, at the end of the assessment. In the case of a postulated hazard, the frequency of occurrence is only implicitly considered.

In the deterministic branch, margin assessment is conducted for a set of hazard magnitude scenarios. These scenarios may be selected by the analyst or prescribed by the regulator of the Member State. Following this branch, the chosen scenario is described in terms of relevant hazard parameters. For example, the aircraft impact hazard could be described by total mass and stiffness of the aircraft, engine mass, amount of fuel, velocity, angle and location of impact. Alternatively, the forcing function for the postulated aircraft impact could also be specified by the regulator.

The next task is the characterization of the appropriate load effects (e.g. impact, overpressure and temperature) to characterize each hazard. Selection of the reference parameter (e.g. peak of the pressure–time history, missile velocity and mass of the fuel) for each load effect is made in the next step. These reference parameters could explicitly define the loading, as suggested, or be more

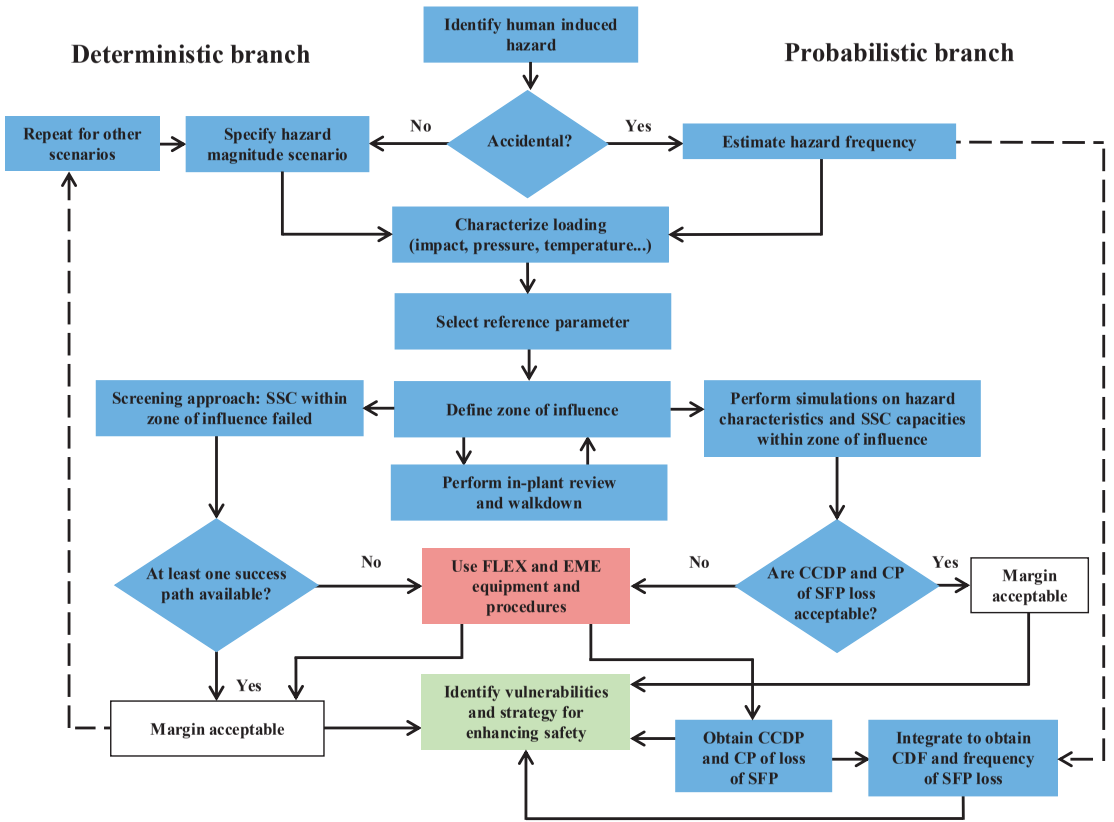



*FIG. 1. Margin assessment flow chart.*

**Note:** CCDP — conditional core damage probability; CP — conditional probability; EME — emergency management equipment; FLEX — diverse and flexible coping strategies; SFP — spent fuel pool; SSC — structure, system and component.

general, such as type of aircraft and operating conditions (e.g. velocity, fuel load and angle of impact), for communication to the decision maker (i.e. the owner or regulator).

The zone of influence consisting of direct damage, damage from debris, fire and smoke is developed for each postulated hazard scenario based on the plant layout, using the analytical and numerical methods as well as the empirical equations given in Ref. [8]. Depending on the postulated scenario, the resistance capacity of structural barriers (i.e. walls, roofs and doors) may be evaluated using the as-built material properties instead of nominal properties such as concrete strength and yield strength of steel. In the screening approach, the SSCs within this zone are assumed to be damaged and could result in initiating some accidents. In addition, the SSCs in the zone of influence are assumed to not be available to perform the safety functions of safe shutdown, prevention of core damage and large early release, and spent fuel pool cooling. For this scenario, the analyst will search for one or more success paths using the SSCs that are outside the zone of influence. The random unavailability of these SSCs and the human error probabilities appropriate for the scenario are considered in this evaluation. The internal event PSA, event tree and fault tree model appropriately modified for the external hazard are used in this search for success paths.

The zone of influence is confirmed through an in-plant review and walkdown. In-plant evaluation is a key step, which is described in detail in Section 4. The objectives of the in-plant evaluation are plant familiarization, preliminary assessment of SSCs inside the zone of influence and the status of SSCs outside the zone of influence, and identification of straightforward solutions. This task includes design review, as-is information review and plant walkdown. In addition to straightforward solutions, the important deliverables of in-plant evaluation are the following:

(a) The identification of SSC items requiring further investigation and their grouping;
(b) The finalization of accident sequences and success paths.

If a success path cannot be found with available equipment within the plant (i.e. SSCs outside the zone of influence), there is a need to use emergency management equipment (e.g. diverse and flexible coping strategies (FLEX) and emergency management equipment guidance (EMEG)) which can be secured on-site or off-site. If a success path is identified for the given hazard using this additional equipment, it is concluded that an acceptable margin has been achieved (i.e. there is HCLPF for the given hazard). This process is repeated for other scenarios (e.g. impact locations) considered credible by the analyst.

An extension of this screening procedure could be to calculate probability measures such as the CCDP and the conditional probability of loss of spent fuel pool cooling and spent fuel damage, given the scenario. The internal event PSA event tree and fault tree models are used in this quantification. The plant owner or the regulatory authority of the Member State could then assess whether these conditional probabilities meet the relevant acceptance criteria.

In the probabilistic branch, the tasks are aimed at estimating the CCDP and the conditional probability of spent fuel pool damage for external hazards of both accidental and postulated types. For the accidental hazard, the frequencies of core damage and spent fuel damage are estimated.

In a PSA based approach, the probabilistic aspects of the external hazard are considered. For example, for an aircraft crash, factors such as the impact location, the impact angle and the amount of fuel could be treated as uncertain, and probability distributions could be assigned to them. Similarly, the capacity of SSCs to resist the impact effects (i.e. load, missile, heat and smoke) is also probabilistic. Therefore, the zone of influence is generally random.

A simulation procedure is followed to define the set of scenarios to be evaluated. The above event tree and fault tree model is modified by adding the SSCs in the zone of influence with their conditional probabilities (i.e. fragilities) and random failure rates (i.e. unavailabilities). The quantification of this model results in conditional probabilities of, for example, core damage, loss of spent fuel pool cooling and spent fuel damage. As a by-product of this approach, the margins of success paths or plant margin in terms of traditional HCLPF capacity could be derived. Once again, if a success path cannot be found with available equipment within the plant, there is a need to use emergency management equipment (e.g. FLEX and EMEG), which can be secured on-site or off-site. It is important that such a use consider the impact of the hazard on the equipment (since the zone of influence is random and not deterministic) and the reliability of emergency management equipment and procedures.

Finally, for accidental external hazards, the frequency of occurrence of the hazard is evaluated and used in the quantification of the event tree and fault tree model to obtain the PSA metrics such as core damage frequency, large early release frequency, and frequency of loss of spent fuel pool cooling and spent fuel damage. During this task, and based on the outcome of the margin assessment, the analyst will identify any vulnerabilities that could be overcome through design and administrative actions. The strategies for enhancing the safety against the hazard would be developed in this task.

## 3.2. ZONE OF INFLUENCE

Section 3.1 provides a high level discussion of the possibility of screening some scenarios from further detailed analysis. The following is an extension of that discussion, including some conceptual tools that may aid in excluding some scenarios from further analysis, as the consequences are deemed to be sufficiently low or success paths can be shown to remain intact. These concepts, when applied, could also serve to identify some safety concerns that are clearly vulnerabilities, without requiring extensive analysis.

In the case of an aircraft crash, the first issue that national authorities need to address is which scenario is to be assessed. This requires definitions of, for example, the types of aircraft, velocities, altitudes and payloads (including the amount of fuel and the existence of passengers and cargo) which are to be used in the analysis. For example, with regard to accidental aircraft crash scenarios, Germany has required designs to deterministically protect against a Phantom or similar, fast military jet crashing into the nuclear power plant site. In contrast, France has ruled out accidental commercial and military crashes based on probabilistic considerations, but it requires consideration of general aviation crashes (Learjet 23 and Cessna 210).

These decisions require taking into account current and predicted air traffic for the country or region. It may involve setting two levels: one for best estimate survival and another (possibly more unreasonably burdensome) for best estimate consequences. Having developed national criteria which may be defined down to a list of site specific approach directions, a case can be made to perform a high level worst case analysis.

Methodologies for analysis of impact, debris, fire and smoke are described in Ref. [8]. These analyses make use of the results of the extensive work that have been performed on the few cases of aircraft impacts on engineered structures (i.e. buildings). The Pentagon Building Performance Report [10] and the World Trade Center Building Performance Study [11] provide useful guidance that may be applied to the nuclear facility case. In Ref. [10], the results of the detailed study assessing the impact indicated that the damage was initially confined to a roughly triangular shape, extending along the direction of the approach. The damage swath was approximately 23–24 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 shown to extend beyond the initial zone of impact. Fire damage, due to burning of the jet fuel and to secondary fires caused by the ignition of on-site combustibles, extended into the areas unaffected by the impact, until contained by the building fire suppression systems.

Hence, the zone of influence concept can applied to nuclear installations for the purpose of preliminary screening. By imposing the damage and debris triangles on a scaled representation of a nuclear plant, aligned along the determined approach paths, an approximation of the areas of damage likely to occur to the relevant building can be determined. The footprint of the fire and smoke damage can be obtained by extending the zone of influence until it is met by a fire barrier that has not been damaged by the initial impact or subsequent debris. In Ref. [12], the zone of influence is referred to as the "damage footprint", and damage rules are described for developing the damage footprint for the physical damage to buildings by aircraft impact, by debris and by fire and smoke.

The expectation is that this concept may provide reasonable initial estimates of the damage caused by an aircraft crash on a nuclear facility based on the evidence from past events. Clearly, this methodology could not be directly applied to certain structures within a nuclear facility. 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, this concept could serve to focus the evaluation on those SSCs critical to the plant achieving safe shutdown, simultaneously eliminating those SSCs that are highly likely to fail in the crash.

Implementation of this concept could result in a visual representation similar to that in Fig. 2 for an aircraft crash in one direction (several diverse directions may be assessed as probable and each would need to be considered).

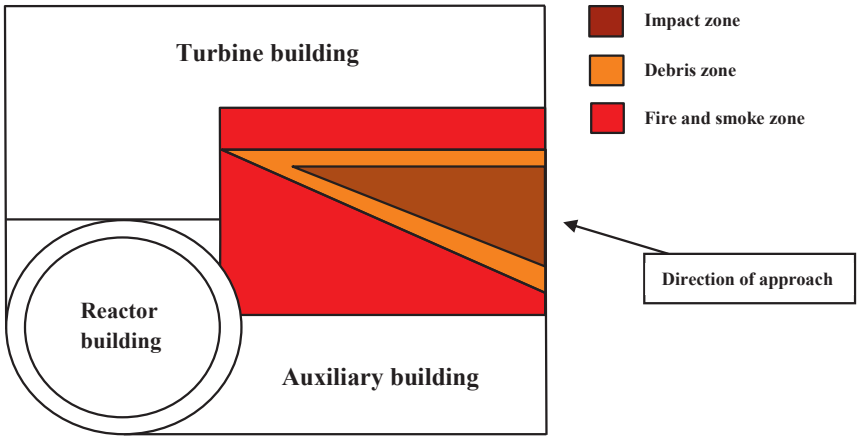



*FIG. 2. Simplified schematic of a nuclear power plant indicating the three zones of influence following an aircraft crash.*

Assuming a loss of all SSCs contained within the zone of influence, and using the defined success criteria (i.e. the redundancy and survivability requirements), an estimation of the effect of the aircraft crash on the plant could be obtained. The safe shutdown path equipment list with redundancy can be used to determine whether there are systems required to achieve the safety objectives (see Section 2.2) remaining outside the zone of influence [12]. It should be noted, however, that the safe shutdown path equipment list will greatly depend on the scenario.

In the following example, the emergency cooling system is assumed to be 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 cooling system may be relied on to maintain the basic cooling requirements for removal of decay heat. The aircraft is considered to be approaching from the north and the south directions for evaluation by the zone of influence approach. For the case of approaching from the north, and using the zone of influence concept, the emergency cooling system is assumed to be unavailable. Based on reasonable assurances, however, the maintenance cooling will survive the impact, debris and fire, thus ensuring that basic cooling functions are maintained. The opposite would be true for the approach from the south.

Caution is to be taken, however, if this methodology is to be used to exclude scenarios from further consideration. Owing to the significant uncertainty associated with this method, there needs to be a high degree of certainty that the essential safety functions are maintained. Furthermore, for open areas such as a turbine building, the zoning might be an underestimate, while for a cellular structure with many interior walls, such as a control building, the effects might be more restricted. Detailed consideration therefore needs to be given to postulated affected buildings and plant, and the methodology is to be applied by a multidisciplinary, experienced team in this domain.

The zone of influence methodology may serve to identify clear vulnerabilities. For example, some nuclear power plants may locate the primary and secondary control rooms in 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 an alternative direction, there would be a good possibility that both control rooms may be lost simultaneously, or that the access to the secondary control room may be impeded owing to the severe fires expected.

The zone of influence depends on the hazard scenario and the structural barriers. The above discussion has focused on an aircraft crash. In the case of an explosion, the analyst needs to consider all structures in the plant exposed to pressure loading, missiles and fire in developing the zone of influence. A particular structure containing SSCs of importance may withstand the hazard,

but an adjoining structure may fail owing to the hazard and collapse on the first structure. The potential for such interactions needs to be examined in the in-plant review. In summary, the zone of influence is constructed for each scenario as follows:

(a) 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 through impact or by a missile, it is assumed that the SSCs housed within the building are no longer functional.
(b) When the barrier is damaged by the missile or if the missile (aircraft) itself is damaged, resulting in additional missiles, the debris created by these events needs to be assessed, and the area over which the debris spreads is to be evaluated. The SSCs within this debris zone are also assumed not to be functional.
(c) If there is fuel available in the form of jet fuel of the impacting aircraft or because of damage to yard tanks with a flammable inventory (e.g. diesel fuel oil tanks), the fire zone is to be evaluated based on the structural damage due to the impact, the amount of fuel, the presence or absence of fire barriers, and emergency fire mitigation measures. The propagation of structural damage due to the fire needs to be assessed. Reference [8] has detailed procedures for this evaluation.
(d) The SSCs within this fire and smoke zone are assumed not to be functional.

The influence zone for each scenario (i.e. postulated or probabilistic) depends on the plant layout, impact location, hazard type and magnitude, presence of barriers and equipment or structures damaged by the impact, pressure or missiles. Several plausible scenarios need to be studied to cover the variations in these parameters.

## 3.3. PLANT SYSTEMS ANALYSIS

Plant systems analysis begins with the selection of the location (with respect to the plant) of the human induced external event. For example, the impact location of aircraft determines the accident sequences to be evaluated. If the aircraft strikes the station switchyard, it could result in the initiating event of loss of off-site power. A strike on the containment may result in a LOCA or radioactive release if the containment is breached. A strike on the spent fuel storage building may result in spent fuel pool failure. The analyst needs to consider a realistic set of impact locations to assess the impact on the plant. For a probabilistic analysis, the relative likelihood of impact locations is to be considered; for a deterministic

analysis, the analyst needs to examine a set of impact locations to envelope the impact effects.

The first step in the plant systems analysis is the identification of a set of initiating events, which may be generated from the human induced external event and could lead to core damage or large early release. The initiating event is the outcome of an external event that would challenge the plant's ability to perform safety functions. For example, the external hazard could be an aircraft crash and the initiating event caused by the aircraft crash could be loss of off-site power or a small LOCA. The frequency, or fragility, for the initiating event is ideally to be evaluated mechanistically, which is not often feasible, especially for postulated events. The practical approach is to assign the frequency or fragility based on experience and expert judgement.

A major element of plant systems analysis is defining the overall nuclear plant performance criteria when subjected to the extreme loading environment generated from the human induced external event. For example, for a nuclear plant subjected to an event not considered in the design, the overall performance criteria may be defined to be hot or cold shutdown for 24 hours after the event occurs. The further assumption is that additional aid from outside the plant boundary can be effectively mobilized within the 24 hour period [4].

The response of the plant to initiating events that require the operation of safety systems to prevent an accident is analysed by accident sequence analysis. This is normally done by constructing an event tree for each initiating event, which models the success or failure of the safety systems, support systems and human actions in carrying out the safety functions. The impact of potential internal flood and fire induced by the external events is modelled in the event trees. The end points of the accident sequence models will correspond either to a safe, stable state where all required safety functions have been performed successfully or to failure.

When the success path approach is used, a tiered approach may be implemented. For less severe events, multiple success paths based on full system redundancy and engineering capacity based on design criteria may be required. For more extreme events, a single safe shutdown path may be deemed to be adequate and very realistic engineering capacity.

The systems, both primary and supporting, that are required to perform the plant safety functions are identified in the accident sequence analysis. Performance of these systems is analysed with 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 the failure of components.

The individual component of a system appearing in an accident sequence or success path is identified as a basic event in a fault tree. The collection of

such components in the fault trees is known as the selected equipment list (SEL). Development of the SEL, which includes the spent fuel pool and ultimate heat sink, is one of the outcomes of the fault tree analysis. SSCs that comprise the accident sequences or success paths are required to function during or after the event. For each item of the SEL, the functional requirements to achieve the system performance are specified. The loadings or demands are physical, such as impact forces, heat, humidity, shock vibrations and spectra, and blast pressures. Hence, failure modes corresponding to these loadings are evaluated. The impact of the following needs to be incorporated in the plant systems analysis:

— Internal fire and flood induced by external hazards;
— Hazardous material release;
— Smothering;
— Dependencies including common cause failure;
— Specific procedures for operator actions in the case of human induced events;
— Human errors.

The three major derivatives of the plant systems analysis are: the event trees modelling accident sequence analysis and success paths; the fault trees of the primary and support systems; and the SEL.

## 3.4. ESTIMATION OF COMPONENT CAPACITY AND FRAGILITY

For the relevant SEL item such as buildings, the fragility (i.e. the median capacity and uncertainty) and the HCLPF capacity are calculated. Fragility is defined as the conditional probability of SSC failure for a given value of the hazard reference parameter (e.g. aircraft velocity and blast pressure). The widely used method of estimating fragilities of structures and equipment based on seismic fragility analysis can be adapted for the fragility evaluation of SSCs under human induced events [13]. The capacity is then expressed in terms of median value and logarithmic standard deviations $\beta_R$ and $\beta_U$, which reflect the randomness in capacity and uncertainty in the median capacity, respectively. For simplicity, the logarithmic standard deviation $\beta_c$, defined as the composite variability, is often used.

Using the log-normal model for the fragility, the two parameters — median capacity and $\beta_c$ — are sufficient to develop a best estimate or mean fragility as a function of the hazard reference parameter. A conservative value of the SSC capacity could be defined, borrowing from the seismic PSA literature [13], as the HCLPF capacity: it is the value at which the mean conditional probability

of failure is 1%. The HCLPF capacity is expressed as median capacity times $e^{-2.33\beta_c}$. For a limited set of examples of fragility calculations for the human induced external events, see annexes II and III of Ref. [14]. Evaluation of the SSC capacity or fragility relies to a large extent on the combined expertise and experience of the engineering safety personnel carrying out the evaluation [15]. Engineering analyses based on as-is conditions and design and test data are conducted to evaluate SSC fragility under the identified failure mode. The loading or demand environments for the SSCs associated with the hazard scenarios are described as in table 1 of Ref. [15] and the supporting data. These loadings or demands are physical, such as impact forces, heat, humidity, blast pressure and vibration. The failure modes to be evaluated pertain directly to these loadings. Capacity evaluations are needed for structures and exposed equipment (i.e. tanks and transformers). For input to deterministic margin assessment, the median capacity, or HCLPF capacity, is to be estimated. For input to probabilistic margin assessment, the median and $\beta_c$ are to be estimated. It is to be pointed out that evaluations of SSC fragility exposed to the human induced external events have not been conducted extensively as part of the PSA of nuclear power plants.

Several considerations are important when performing these evaluations. Engineering safety personnel take credit for the inherent robustness in the nuclear plant due to its design basis for normal operating conditions and design basis accidents. In addition, demonstrated robustness of the plant for design extension events may also be credited (see Section 2.4). These DEE 1 and DEE 2 may be internally or externally initiated. The latter category includes external events of natural origin, such as earthquakes, extreme winds and extreme floods. These external events have also been assessed under the severe accident policy for operating nuclear power plants in some Member States.

Capacity evaluations may also be performed to determine the HCLPF of SSC components when subjected to the hazard scenario. Examples are discussed in Section 5. Guidance on the engineering evaluation of various modes of extreme events can also be found in numerous IAEA and other publications. In particular, NS-G-3.1 [3] addresses the hazards of aircraft crashes, external fires, explosions, hazardous materials and floods, provides a list of references on technical evaluation approaches and introduces the concept of HCLPF for explosion risks.

The steps in the SSC capacity evaluation include the following [15]:

(1) Plant familiarization, many aspects of which are accomplished during the determination of the SEL and the determination of the loading environment of SSCs: Additional familiarization with plant specific documents for the SSCs of interest is performed during this step.

(2) In-office and in-plant evaluations of items of the SEL: In-plant evaluations refer to the walkdowns discussed in Section 4. In-office evaluations refer to the assembling of design and qualification data for the specific items of the SEL. Calculations are to be made as necessary to determine the loading environment and the failure capacity of the items.
(3) Confirmation of assumptions made in all phases of the evaluation during the plant walkdown.
(4) Documentation.

## 3.5. DETERMINISTIC EVALUATION OF THE PLANT MARGIN

The plant margin is deterministically assessed using success paths. A success path is a minimum set of systems and operator actions required to bring the plant to a safe and stable condition and to maintain this condition for a specified time. A success path typically does not comprise all safety systems [16]. Success paths need to be compatible with plant operations. In general, several possible success paths may exist. The approach is to select the success paths for which it is easiest to demonstrate adequate margins or capacity when subjected to extreme loads. In addition, the success paths have to take into consideration plant operator training and established procedures while recognizing that, for some event scenarios, the damage to the plant may be so extensive that existing plant training and procedures may be neither applicable nor adequate. For such events, specific procedures for operator actions are to be developed at the completion of the assessment.

The success paths that are chosen will depend on how 'success' is defined. Depending on the performance criteria, success may refer only to safe shutdown and removal of residual heat. This is commonly called the 'safe shutdown path'. The performance criteria define both what is meant by success (safe shutdown alone or with additional requirements) and the number of success paths required. A tiered approach can be used for defining the success paths and the acceptance criteria for SSC performance.

For example, tier one would apply to human induced events where evaluation criteria may be similar to design basis considerations: that is, full system redundancy (adherence to single failure criteria and redundant paths) and SSC performance behaviour limits at design levels. Two examples of such an event are the impact of a light aircraft on-site and an explosion at some distance from the plant. In these cases, it is feasible to restart the facility after inspections have been performed. The design basis event may or may not cover such events, depending on national practices.

Tier two (DEE 1) would apply to events where redundancy of safe shutdown paths (i.e. the means to control the reactor, cool the fuel and contain the release of radioactive material) would still need to be demonstrated, even with reduced functionality, but adequate for shutdown, structural integrity and leaktightness. Examples in this category include impacts by commercial and business aircraft. In such cases, structure and system acceptance criteria may be relaxed, taking into account the post yield behaviour of the materials.

Tier three (DEE 2) would apply to very large events, for example the impact of a large aircraft or large explosions off the site. In these cases, the response would include on-site and off-site emergency measures. In all such cases, reactor shutdown needs to be ensured, even though redundancy would not be required. Structural integrity is to be maintained, but limited leaktightness degradation might allow the release of radioactive material, as long as dose acceptance criteria are not exceeded. In such cases, structure and system acceptance criteria may be significantly relaxed, taking into account the ultimate capacity of the components.

Each of these cases leads to a different safe shutdown path or paths. For a less severe event, the safe shutdown path may encompass all, or a portion, of the safe shutdown path for a catastrophic event. Each safe shutdown path or success path comprises a subset of plant systems, including safety systems, support systems, containment and other structures, and operator actions, whose operability and survivability are sufficient to safely shut down the plant and to maintain it in a safe shutdown condition for the period specified.

A human induced event could result in one of the following initiating events: a transient, small LOCA or a large LOCA. There could also be combinations of initiating events to be considered: loss of off-site power and a small LOCA. For each initiating event, the progression of 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 (or cutsets) for each accident sequence is obtained. Alternatively, the success paths could be developed from these event trees and fault trees.

In the deterministic approach, the SSCs within the zone of influence are assumed not to be functional. Evaluation is aimed at verifying whether one or more success paths are available to bring the plant to safe shutdown or to prevent a loss of integrity of the spent fuel pool and ultimate heat sink. The SSCs needed to accomplish these success paths are assumed not to be impacted by the postulated hazard. Their success (availability) needs to be demonstrated to be highly reliable. If the success paths are demonstrated to be available, the plant is considered to have an adequate margin against the postulated external

hazard. If a success path cannot be found with available equipment within the plant (i.e. SSCs outside the zone of influence), there is a need to use emergency management equipment (e.g. FLEX and EMEG) which can be secured on-site or off-site. If a success path is identified using this additional equipment, it is concluded that an acceptable margin has been achieved (for further details on accident management for external hazards, see Annex IV).

An extension of this deterministic success path procedure could be to calculate some probability measures such as the CCDP and the conditional probability of loss of spent fuel pool cooling and spent fuel damage, given the scenario. The SSCs within the zone of influence are assumed not to be functional. The SSCs and emergency procedures are modelled in the event tree, and fault trees are appropriately modified from the internal event PSA. The plant owner or the regulatory authority of the Member State could then assess whether these conditional probabilities meet the relevant acceptance criteria.

## 3.6. PROBABILISTIC EVALUATION OF THE PLANT MARGIN

### 3.6.1. General

The procedure for evaluation of the plant margin using a probabilistic method is similar to the accident sequence analysis performed in PSAs. In a PSA based approach, the probabilistic aspects of the external hazard are considered. For example, for an aircraft crash, factors such as the impact location, the impact angle and the amount of fuel, among other things, could be treated as uncertain, and probability distributions could be assigned to them. Similarly, the capacity of SSCs to resist the impact effects (i.e. load, missile, heat and smoke) is also probabilistic. Therefore, the zone of influence is generally random.

A simulation procedure is followed to define the set of scenarios to be evaluated. The event tree and fault tree model in Section 3.5 is modified by adding the SSCs in the zone of influence with their conditional probabilities (i.e. fragilities) and random failure rates (i.e. unavailabilities). The quantification of this model results in conditional probabilities of core damage, loss of spent fuel pool cooling and spent fuel damage. As a by-product of this approach, the plant margin in terms of traditional HCLPF capacity could be derived. Once again, if an acceptable margin cannot be established with available equipment within the plant, there is a need to use emergency management equipment (e.g. FLEX and EMEG), which can be secured on-site or off-site. It is important that such a use consider the impact of the hazard on the equipment (since the zone of influence is random and not deterministic) and the reliability of emergency management equipment and procedures.

The plant level or accident sequence level fragility is obtained by combining the component fragilities and random failure rates in the quantification process. The plant level fragility could be the CCDP and the conditional probability of loss of spent fuel pool cooling. The plant margin defined in terms of the HCLPF value is derived in terms of the reference parameter at which the probability of failure is equal to 1%; similarly, the plant margin defined in terms of the median value is the reference parameter at which the probability of failure is less than or equal to 50%.

For accidental external hazards, the frequency of occurrence of the hazard is evaluated and used in the quantification of the event tree and fault tree model to obtain the PSA metrics such as core damage frequency, large early release frequency, and frequency of loss of spent fuel pool cooling and spent fuel damage.

### 3.6.2. Safety assessment using simplified event trees

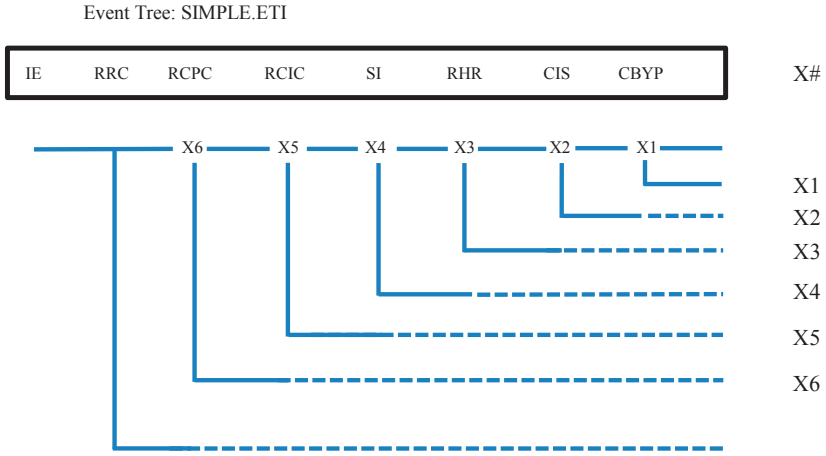
A simplified event tree approach was introduced for quick estimation of large early release frequencies without the need to perform a detailed Level 2 PSA [17]. In many cases, this simplified method can be used for the assessment of the protection of an existing nuclear installation against extreme external events once the main characteristics of the critical scenarios to be investigated are defined.

The approach requires the assessment of safe shutdown paths involving the following safety functions:

— Reactor reactivity control;
— Reactor coolant pressure control;
— Reactor coolant inventory control;
— Decay heat removal.

These basic safety functions are arranged in sequence to form a simplified event tree. In the case of a loss of reactor coolant inventory control, a safety injection function will also be required and it is to be added to the event tree. To assess the impact on the environment, it is also useful to add the containment isolation function (containment of radioactive material) and question the possibility of a containment bypass.

Once this information is given, a general simplified event tree modelling the availability of the corresponding safety functions can be developed, which is then used for a simplified quantitative analysis of each scenario. Such a general event tree is shown in Fig. 3. This event tree includes the top events listed in Table 1.




**Note:** IE — initiating event. Top events are described in Table 1.

*FIG. 3. Simplified event tree.*

Based on the identified external event scenarios, a quantitative assessment on the availability of the functions represented in the simplified event tree is carried out. The assessment can be performed by:

(a) Using information on the load characteristics and on the capacity of the structures of interest (thus housing safe shutdown equipment) by developing failure probabilities;
(b) Using bounding assumptions on the consequences of the scenario, for example based on the zone of influence described above, setting certain system functions located in the zone of influence as guaranteed failed;
(c) Using structured expert judgement of the members in the assessment team;
(d) Using simplified approaches (scaling or calibration tables) for quantification.

This method implements several levels of simplification and approximation. First, the plant system behaviour is simplified to be represented by a limited number of systems that respond to the aforementioned success paths. Second, screening and enveloping of event scenario consequences are introduced to reduce the quantitative effort. Third, expert opinion is relied upon to develop failure likelihoods of systems in some instances. Such expert opinion is most valuable at the extremes of the fragility function assessment (i.e. guaranteed to fail or guaranteed to succeed). In the intermediate range, guidelines on expert opinion interpretation are required. Annex III contains an example of implementation of the simplified event tree approach to explosion hazards.

TABLE 1. TOP EVENTS FOR A SIMPLIFIED EVENT TREE

| Top event | Description | Related systems (BWR) | Related systems (PWR) |
|---|---|---|---|
| RRC | Reactor reactivity control | Reactor trip system<br>Alternate rod insertion<br>Standby liquid control system | Reactor trip system<br>Reactor power limitation system<br>Boron injection system |
| RCPC | Reactor coolant pressure control | Steam line safety and relief valves | Pressurizer safety and relief valves |
| RCIC | Reactor coolant inventory control | Integrity of reactor coolant piping | Integrity of reactor coolant piping |
| SI | Safety injection | Isolated core cooling<br>HPCS<br>LPCS | High pressure safety injection<br>Low pressure safety injection |
| RHR | Residual heat removal | RHR function of low pressure injection (LPCS), including corresponding cooling water trains | RHR operation in recirculation and sump recirculation mode<br>Secondary side heat removal |
| CIS | Containment isolation | Containment isolation system and its supports | Containment isolation system and its supports |
| CBYP | Containment bypass | Piping connected to the reactor coolant system outside the containment | Piping connected to the reactor coolant system outside the containment |

**Note:** BWR — boiling water reactor; HPCS — high pressure core spray; LPCS — low pressure core spray; PWR — pressurized water reactor.

# 4. IN-PLANT EVALUATION

## 4.1. GENERAL

As stated in Section 3, in-plant evaluation is a key step in the process for margin assessment (see Fig. 1). The following provides a more detailed description of the activities included within this step.

The objectives of the in-plant evaluation are plant familiarization, preliminary assessment and identification of straightforward solutions, if any. The major components of this task are the following:

(1) To evaluate the feasibility of hazard affecting the structures for each hazard. The result is a list of viable locations for aircraft impact (building-by-building and yard) and explosive pressure, among other things. The list is transmitted to analysts implementing the evaluation procedures in Ref. [7]. The layout of the plant and the topography of the surrounding area need to be reviewed as part of this activity.
(2) To receive results from analyses defining consequences of hazard scenarios, including zones of influence (footprints) for aircraft crashes, explosions and fires (direct or indirect), according to Ref. [7].
(3) To receive a preliminary list of SSCs.
(4) To review designs.
(5) To review as-is information of the nuclear power plant.
(6) To develop preliminary proposed screening rules.
(7) To perform plant walkdowns.

The plant walkdown will focus on several modes of failure:

— Direct exposure to hazard effects (mechanical: collapse, perforation and deflection; heat; and others);
— Fire;
— Indirect exposure to hazard effects, for example: scabbing and spalling of concrete structures, and penetration of all structures; fire related issues, such as firefighting (water and foam) and smoke; falling missiles and debris (e.g. the aircraft fuselage, engines and landing gear); and other systems interaction issues;
— Vibration due to impact and impulse.

The walkdowns performed within the seismic PSA and fire PSA are useful if the documentation is made available after they have been performed.

Activities (1) and (2) are defined in Ref. [7] (phases 1 and 2 of the safety evaluation). The output is the extreme environment matrix and the associated matrixes defining each hazard scenario. Activities (4)–(7) are described in Sections 4.2 and 4.3.

The important deliverables of in-plant evaluation are the following:

(a) Screening out of SEL items (verification of in-office assessment and additional screening in-plant) (see Sections 4.3.2 and 4.3.3);
(b) Straightforward solutions, for example installation of fire doors, reinforcing accesses (air intakes and windows) and sealing penetrations in underground chases;
(c) Identification of items in the SEL requiring further investigation and their grouping;
(d) Finalization of accident sequences and success paths.

## 4.2. REVIEW OF PLANT STATUS

### 4.2.1. Review of design

Activity (4) is:

(a) To review identified accident sequences or success paths and the relevant SSCs;
(b) To confirm the required functions of the SSCs during and after the event;
(c) To confirm the demand environments to which the SSCs are subjected for each event scenario;
(d) To identify or confirm failure modes of concern as a function of the event;
(e) To identify robust SSCs (robustness includes direct and indirect effects) that may be excluded from further consideration.

### 4.2.2. Review of as-is information

In Activity (5), the correspondence of design information reviewed in the previous activity with current conditions of the plant needs to be verified, including plant systems.

## 4.3. PLANT WALKDOWN[2]

In-plant evaluation is based on walkdowns. The plant walkdown activities are completed in three principal steps: walkdown preparation; the preliminary screening walkdown, also known as walk-by (Activity (6)); and the more detailed walkdown (Activity (7)). Certain special topics, such as co-located facilities on the site and the potential of spatial interactions, are examined in Section 4.4.

### 4.3.1. Walkdown preparation

Plant walkdown preparation includes the following activities:

(a) Plant familiarization:
  (i) General plant documentation needs to be assembled, including safety analysis reports, system descriptions, piping and instrumentation diagrams, 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.
  (ii) Plant access requirements have to be met, including radiation protection, safety practices and security practices (adherence to the 'as low as reasonably achievable' principle is required).

(b) Plant documents on safe shutdown paths and the SSCs are to be consulted or created, and the environmental demand on each item in the SSC, including physical and security demands, needs to be defined.

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

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

(e) An in-plant walkdown plan is to be developed indicating the number of teams and their composition. 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. Table 8 of Ref. [15] illustrates a format that can

[2] This section is based on appendix II of Ref. [15].

be used for the SSC database (safe shutdown equipment list, SSEL). The columns of this table are as follows:

(i) *SSC No.* is a unique numerical identifier for the SSC, which may contain location, system or other information.
(ii) *SSC name* contains descriptive information on the SSC (e.g. the auxiliary building and diesel generator number).
(iii) *SSC ID No.* is a plant specific identifier.
(iv) *Description* briefly describes the SSC.
(v) *Hazard scenario No.* is an identifier linked to a master list of scenarios to be evaluated.
(vi) *Location* refers to a series of location identifiers to aid in planning the in-plant walkdown and evaluating the consequences of the hazard.
(vii) *Physical loading conditions* are identifiers of the type of loading condition 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. the impact plus fire).
— *Impact* refers to 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 the scabbing of concrete and vibration induced loadings.
— *Explosion/blast effects* to be considered can be direct or indirect. Direct impact effects are blast pressures; indirect blast effects are conditions such as vibration induced loadings.
— *Heat/fire* refers to heat from a fire or direct flame effects on the SSC.
— *Smothering* and related conditions 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 needs to be evaluated.
— *Flooding* from internal or external sources may need to be evaluated.

Table 9 of Ref. [15] 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 SSC under consideration is entered into the forms; the remainder of the table is filled out upon completion of the walkdown and evaluations. Documentation of the evaluation then comprises these summaries and the detailed evaluations.

Table 9 is based on the data sheets used for SSC evaluations for seismic and other external events. For the seismic evaluation case, unique data sheets exist for each of 22 equipment categories. 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, were the basis for developing similar worksheets for the current evaluation [of human induced events]. The data to be collected and evaluated may need to be modified to take into account non-vibrational modes of failure, that is, environmental conditions such as heat, humidity and direct impact."

### 4.3.2. Preliminary screening walkdown

The preliminary screening walkdown needs to achieve the following objectives:

(1) Determine the location and accessibility of each SSC item in the plant;
(2) Identify any other SSCs needed for safe shutdown, hazard prevention or consequence mitigation, which then need to be added to the SSC database;
(3) Review and validate the screening of SSCs with respect to capacity considerations (direct and indirect effects);
(4) Identify potential straightforward solutions;
(5) Group all the components located within or on larger items of equipment;
(6) Group components at the same location, particularly in the same vital area, for evaluation of spatially common environments;
(7) Evaluate whether SSC capacity is adequate for the specified event(s);
(8) Document conclusions.

The preliminary screening walkdown examines accessible SSCs. There are three alternative disposition categories for each item on the SSC database:

(a) Disposition Category 1: For SSCs in this category, capacity is clearly less than the demand and a modification is required.
(b) Disposition Category 2: For SSCs in this category, capacity is uncertain, and further evaluation is needed to determine whether a modification is required.
(c) Disposition Category 3: For SSCs in this category, capacity is clearly greater than the demand, and the SSC is adequate for the specified event.

The preliminary screening walkdown is to be fully documented. The main result of the preliminary walkdown is the identification of SEL items that are

clearly robust. These SSCs 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.

### 4.3.3. Detailed screening walkdown

The detailed screening walkdown is to be performed for all SSCs whose capacity for the defined scenarios 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 screening walkdown. At this stage, walkdown engineers evaluate these SSCs in more detail and judge whether or not the component requires further analysis or modification.
(2) SSCs in the second category are those for which plant modifications are clearly warranted. In these cases, the walkdown engineers suggest that the modifications be implemented.

The detailed screening walkdown needs to be thoroughly documented. It is advisable to supplement the documentation with photographic and/or video records. Table 8 of Ref. [15] is an acceptable form of summary documentation for the entire SEL. The SSC evaluations may be documented using the form given in table 9 of Ref. [15], with supporting material attached.

## 4.4. SPECIAL TOPICS OF IN-PLANT EVALUATION

### 4.4.1. Type and number of collateral 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 human induced external events. The evaluation needs to take all on-site facilities into consideration, including any interdependence of their safety systems. Such consideration includes consequence evaluation of environmental discharges that are cumulative for all facilities on the site.

### 4.4.2. Spatial interactions

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

#### *4.4.2.1. Falling*

Falling is the structural integrity failure of a non-safety or safety related item that could hit and damage a safety related item. For the interaction to be a threat to an SEL item, the impact has to contain considerable energy and the target has to 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 needs 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 a falling interaction. Masonry walls are generally located close enough to the safety related equipment that their failure could lead to equipment damage.

#### *4.4.2.2. 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). The most common examples of proximity interaction are fires and explosions. These interactions are discussed for human induced events of the postulated type in Ref. [15].

#### *4.4.2.3. Spray and flood*

Spray and flood can result from the failure of piping, systems and vessels that are not properly supported or anchored. Inadvertent spray hazards to SEL 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 has to evaluate the vulnerability of all SEL components to spray.

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 are potential sources of flooding. The walkdown team, with the assistance of plant personnel, has to assess the potential consequences of a flood source failure and the ability of floor drainage systems to mitigate the consequences of such a failure.

### 4.5. PLANT WALKDOWN TEAM

Plant walkdown team consists of members of the operator's staff, consultants with the required expertise and, potentially, regulators. For a description of the team composition, member qualifications and responsibilities, see Section 2.5.

## 5. MARGIN ASSESSMENT FOR DIFFERENT HAZARDS

### 5.1. GENERAL

The overall approach to margin assessment is shown in Fig. 1, in Section 3. The sequence of activities for a full assessment is as follows:

(a) For each hazard, the appropriate load effects (i.e. impact, impulse, overpressure, missiles and heat) are identified.
(b) For each load effect, the reference parameter is selected (e.g. peak of the impulse–time history, peak overpressure, velocity, cross-sectional area and crushing strength of the missile, and mass of the fuel).
(c) For the specific hazard, the SSC items, which are to be evaluated for each load effect, are identified (this includes the spent fuel pool and ultimate heat sink).
(d) Based on the in-plant review (this includes design and drawing review as well as plant walkdown), the SSC items for margin assessment are identified.
(e) For the relevant SSC items, the fragility (i.e. the median or mean capacity and uncertainty) and the HCLPF capacity (defined as the 1% probability of failure capacity on the mean fragility curve) are calculated.

(f) The accident sequences for core damage and large early release are developed. These include the failures of SSCs under the human induced external event and the random failures and unavailabilities of equipment and systems as well as human error probabilities.
(g) For each accident sequence, the accident sequence fragility is calculated using the fragilities of SSC items appearing in the sequence, the random unavailabilities and human error probabilities.
(h) The accident sequence fragilities are combined to obtain the plant level fragility for core damage and large early release.
(i) For hazards of accidental origin that can be defined probabilistically, the hazard frequency is convolved with plant level fragility to obtain the frequency of core damage and large early release. The frequencies of loss of spent fuel pool cooling and loss of ultimate heat sink are calculated.
(j) For postulated hazards, the margin is calculated as a selected probability of failure value on the plant level fragility curve. Examples are the median value (50% non-exceedance value) and HCLPF value (1% non-exceedance value).
(k) Alternatively, success paths to prevent core damage or large early release could be identified. The HCLPF values (or other specified values, e.g. best estimate) of SSC items are entered into these success paths to obtain the margin of the success paths. If two success paths are each identified for prevention of core damage or large early release, the higher of the two margins will represent the plant margin against core damage or large early release.

In the following sections, the approaches to capacity assessment of components against impact, overpressure and heat load effects are described. These are illustrated using two hazard types: aircraft crash and explosion.

## 5.2. CAPACITY ASSESSMENT OF COMPONENTS AGAINST IMPACT

### 5.2.1. Description of loading

The hazard that leads to an impact of nuclear power plant structures and components could be an aircraft or land vehicle crash, collision of a ship or missiles generated by an explosion. These would result in impact loading of the walls of barrier or building structures and in perforation, penetration, or scabbing and spalling of reinforced concrete structural walls and roofs. The parameters of such missiles are many and include the mass, velocity, missile size, angle of impact and type of material, including crushing strength. It may be convenient to

select the missile velocity as the reference parameter; other parameters are frozen for the specific missile at their mean or median values.

It is also possible that one hazard could create other loading effects on different structures in the nuclear power plant. For example, the aircraft crash could result in a direct impact on the reactor building, but the secondary missiles generated in the crash (e.g. the landing gear) could impact other buildings. The jet fuel fire could affect SSCs internal to the structure, if ingress occurs, and the yard equipment. The zone of influence needs to be defined taking into account these situations.

For the impact loading characterized by the reference parameter of missile velocity, the impact–time history could be described for evaluation of the structural barriers (i.e. walls, roof and other barriers). The velocity of secondary missiles, if any, could also be expressed as a function of this reference missile velocity.

### 5.2.2. Failure modes

The structure failure modes to be examined are those that affect the required performance of the structure: overall instability, loss of structural integrity (e.g. missile perforation and partial structure collapse), loss of leaktightness, and loss of support for systems, components and equipment within the SEL [8].

### 5.2.3. Capacity assessment

Capacity evaluation is generally limited to building structures housing the SEL and exposed large equipment such as yard tanks and substation structures. For each failure mode, the mean or median capacity and the uncertainty in the capacity are estimated using the procedures of response analysis and semi-empirical formulas described in Ref. [8]. The mean or median capacity is calculated using the best estimates for different parameters that are used to describe the loading and capacity evaluations. For conservative margin assessment, a judicious combination of conservative values of parameters needs to be used.

## 5.3. CAPACITY ASSESSMENT OF COMPONENTS AGAINST PRESSURE

### 5.3.1. Description of loading

An explosion near the plant would create a pressure wave that impinges on the nuclear power plant structures of importance to the SEL. Typical pressure–time

histories are shown in Ref. [8]. For capacity evaluation, the reference parameter of peak overpressure is used — either side-on or reflected overpressure.

### 5.3.2. Failure modes

As for impact loading, the structure failure modes to be examined are those that affect the required performance of the structure: overall instability, loss of structural integrity (e.g. missile perforation and partial structure collapse), loss of leaktightness, and loss of support for systems, components and equipment within the SEL [8].

### 5.3.3. Capacity assessment

In this case, capacity evaluation is generally limited as well to building structures housing the SEL and exposed large equipment such as yard tanks and substation structures. As in the case of impact, for each failure mode, the median capacity and the uncertainty in the capacity are estimated using the procedures of response analysis described in Ref. [8]. The median capacity is calculated using the best estimates for different parameters that are used to describe the loading and capacity evaluations. For conservative margin assessment, a judicious combination of conservative values of parameters is used.

## 5.4. CAPACITY ASSESSMENT OF COMPONENTS AGAINST HEAT LOAD

Some human induced external events (e.g. aircraft crashes and explosions) could result in a fire ball or pool fire. References [7, 8] provide guidance on the evaluation of SSCs subject to these fire load cases.

The fires may occur inside or outside the buildings. For a fire scenario outside the buildings, the analyst needs to confirm that the impact and blast impulses will not penetrate the building structures. Otherwise, it is to be conservatively assumed that an interior fire will also result. This may be due to external fire occuring near openings or open shafts of the building. The extent of fire within the building depends on the amount of fuel entering the building and the amount of combustibles within the building. It may be conservatively assumed that 100% of the fuel in an aircraft crash is disposable for an interior fire scenario if the thickness of the walls of the reinforced concrete building is less than 50 cm.

A conservative screening approach is to assume that structures, or portions thereof (e.g. compartments and interconnected corridors), are disabled when a fire occurs in the area. For example, for an aircraft crash, if penetration of the structure could occur and jet fuel could enter various portions of the structure, and ignition is assumed, a conservative assumption could be that all SSCs in the area are disabled and cannot function. This approach acts as a first level screen, which could be refined with more information about the fire (i.e. heat, duration and smoke). Additional, less conservative screening could be performed by taking into account fire detection and extinguishing capabilities, if deemed likely to function (for further details on the assessment of fire performance of SSCs, see section 5.5.2 of Ref. [8]). The data and results of the fire PSA could be used in this screening if such a fire PSA exists for the plant (for further discussion on jet fuel fires, see Section 5.6.5).

## 5.5. MARGIN ASSESSMENT

In the PSA approach, the Boolean equations for accident sequences are derived using the event tree and fault tree modelling. SSC fragilities, random unavailabilities and human error probabilities in these accident sequences are entered to calculate the accident sequence fragilities. The accident sequence fragilities are combined to obtain plant level fragility from which the plant margin is stated as the load reference parameter value at a selected non-exceedance probability (e.g. 1%), or median or best estimate.

When a deterministic success path approach is used, the margin for the success path is calculated based on the 'min–max' method, wherein the HCLPF of 'AND' failures is taken as the maximum of the component HCLPFs, and the HCLPF of 'OR' failures is taken as the minimum of the component HCLPFs.

## 5.6. AIRCRAFT CRASH

### 5.6.1. Specific hazards

Depending on the location of the airport or airways with respect to the nuclear power plant, the type and size of aircraft accidently impacting the plant is selected. It is assumed that a probabilistic analysis of the aircraft hazard for accidental crash in the vicinity has been conducted and a specific aircraft is chosen to perform the margin assessment. This margin assessment could also be part of the overall probabilistic analysis. For a postulated aircraft crash, it is expected that the competent authority of the Member State will specify the

hazard. It could be in terms of a forcing function or the type of aircraft and its impact velocity [7].

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 needs to be therefore performed not only for the maximum loads related to the whole aircraft but also for their parts impacting with the same velocity but acting on a much smaller surface. The effect of an aircraft crash on a building mainly depends on the type of aircraft, the design concept of the structure and the 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 subjected to impacts, fires and other concomitant events, the following need to be checked:

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

The stability checks are to be performed for the loads applied by the aircraft acting on the corresponding building at its upper regions, considering the local soil conditions.

The zone of influence concept is described in Section 3.2 for the purposes of preliminary screening. The concept is applied to an aircraft crash by imposing the damage and debris triangles on a scaled representation of a nuclear plant, aligned along each or all determined approach paths. An approximation of the areas of damage likely to occur to the relevant building could be obtained. 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.

Assuming a loss of all SSCs contained within the zone of influence, and using the defined success criteria (i.e. the redundancy and survivability requirements), an estimation of the effect of the aircraft crash on the plant could be obtained. Margin assessment would then determine whether successful shutdown of the nuclear power plant is feasible using the SSCs outside the zone of influence.

### 5.6.2. Local response

Local loading effects develop in three stages: missile penetration into the target; scabbing and spalling at front and rear surfaces of the target, respectively; and missile perforation of the target, when the target is not able to stop the missile. This publication uses the definition of these terms given in Ref. [8]:

(a) Penetration is the displacement of the missile into the target. It is a measure of the depth of the crater formed at the zone of impact.
(b) Spalling is the ejection of target material from the front face of the target (i.e. the face on which the missile impacts).
(c) Scabbing is the ejection of material from the back face of the target (i.e. opposite the face of impact).
(d) Perforation is when the missile fully penetrates and passes through the target.

The definitions of 'perforation velocity' and 'residual velocity' are also taken from Ref. [8]. Perforation velocity designates the initial missile velocity that is just sufficient to completely perforate the target, resulting in a residual velocity equal to zero. Residual velocity is the exit velocity of the missile, which has an initial velocity greater than the perforation velocity.

Local damage will not generally result in structural collapse. However, local effects need to be considered, since they have a potential for damaging safety related systems or components. For instance, the scabbed material or a perforating missile could potentially impact safety equipment and cause system failures.

In the context of this publication, the main local effect of interest is the perforation of a reinforced concrete wall by an aircraft engine. An aircraft engine is a compact, high density, but crushable, missile. In addition, scabbing of concrete fragments from the inside surface of the wall needs to be considered when critical equipment is located at, or near, the back surface of the impacted area. When there is no transverse reinforcement, the scabbed area can be significantly larger than the missile impact footprint area. Therefore, the cross-section of the structure can be significantly reduced, owing to the ejected concrete, and the global structural capacity could be affected. This effect needs to be considered by the analyst when assessing the global capacity.

When an impacting engine has an initial velocity in excess of the perforation velocity corresponding to a primary target wall, the damage potential of the perforating crushed engine needs to be considered. The residual velocity of the resulting missile can be estimated by assuming that the initial kinetic energy of the missile less the energy loss during the perforation process is transferred to the

crushed engine and to the volume of concrete which is scabbed. After perforation of the primary target, the exiting missile can be assumed to be a compacted semi-solid missile with a diameter approximately equal to the engine casing. Under this assumption, the local damage potential of the missile when impacting on a secondary target can be estimated by using the same empirical formulas used for the main target, but by using a reduced mass and slightly different modification factors to introduce the residual crushability of the remaining missile [12].

In case of impact on steel containment shells located behind the primary target wall, the formulas for estimating the perforation potential are based on impact tests with solid missiles hitting steel plates [18]. When using these formulas, the residual crushability of the missile is not considered.

In Ref. [8], a set of empirical formulas is given, together with their applicability ranges. The formulas provide the following:

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

The formulas provide a simplified approach to the assessment of structural integrity for local loading on nuclear plant structures. The formulas are empirically derived using missile test data, and they give the best estimate values; the variability in the test results is not explicitly stated (for detailed discussion of these and other available formulas, see Ref. [8]).

### 5.6.3. Global response

Global structural response effects correspond to the overall building behaviour as a consequence of aircraft crashes. In contrast to the local effects discussed in Section 5.6.2, the global response could lead to major structural damage, such as the collapse of large portions of walls, floors or main structural systems of the building. In addition, the impact will induce vibrations throughout the building (see Section 5.6.4).

In a general case, global structural damage is the result of excessive deformation of the main structural system. Global structural damage can be evaluated by analysis of the missile initial velocity and deformability, and the inertial, structural and dynamic characteristics of the target. The method of evaluation needs to be adapted to the availability of data and the intended level of detail. Normally, one of the following methods of evaluation can be used, as described in Ref. [8]:

(a) Force–time history analysis method: Following this approach, analyses of the missile and target are uncoupled. First, the impact force–time history is computed based on aircraft crushing strength and impulse conservation principles. In doing this, the target is assumed to be rigid. In a second step, the force–time history obtained is used in a computational model of the structure in a time history analysis. This analysis provides the internal forces and corresponding stresses in the structure under the force–time history, which are used to assess the structure's capability to maintain its integrity during the impact. The analysis also produces displacement/acceleration–time histories at the relevant locations within the structure, which can be used to assess equipment functional capability during and after the impact.

(b) Missile–target interaction analysis method: In this more elaborated approach, the analyses of the missile and target are not uncoupled. A combined computational model of both the missile and target is developed, and the dynamic response of both the missile and target is determined by running an initial velocity problem. The non-linear computational models are normally significantly larger and more complex than those used in the previous approach. This method can provide more accurate results. However, it requires more detailed mass configuration and structural system data for the definition of the missile model, which is not always available from the aircraft manufacturers.

It is to be taken into account that, in reality, those local and global impact effects take place simultaneously. Hence, large 'local' damage could have a significant influence on the global response.

### 5.6.4. Vibration effects on equipment inside the building

Even when local and global impact effects on structures are acceptable, the equipment housed by the impacted structure could fail owing to shock damage, especially near the impacted zone. Potential shock damage needs to be assessed to define a shock damage footprint. Typically, all equipment within the zone of influence of the impact is assumed to fail unless it is shown to withstand the shock loading by means of a specific evaluation. The shock damage footprint is defined by the equipment which cannot be shown to be functional after the shock.

For defining the shock damage footprint, susceptibility distances are provided in Ref. [12] for different equipment classes. However, numerical values are not given because they are considered classified information. Since shock is transmitted through structures and not open air, those distances are measured from the centre of the initial impact and along a structural path up to the affected

equipment item. This means that the shock is not transmitted across seismic gaps or other structural discontinuities between adjacent buildings.

Normally, the frequency content of the shock produced by the impact corresponds to a frequency band that is at a higher level than the frequency band corresponding to the seismic loading. Hence, seismic qualification will normally not cover the dynamic excitation produced by the shock due to impact [8].

In many cases, the fire and/or the structural damage footprint will envelope the shock damage footprint.

If detailed response analysis of the structure is performed for aircraft crashes [7], the evaluation of the equipment inside the structure is to be in terms of in-structure response spectra, which define the frequency range of interest for the equipment from an engineering point of view.

### 5.6.5. Jet fuel fire

Reference [8] discusses the fire sources, different fire scenarios such as fire ball and pool fire, and the methods for evaluating the potential fire effects. The design and size of containment structures are such that a large fire could be anticipated in the zone surrounding the containment even if the structure is not breached by the impact. The fire has the potential to affect off-site power supplies, diesel generators and other important equipment.

When assessing containment damage scenarios, the effects of such a large fire outside the containment need to be taken into consideration. In addition, an aircraft crash into the containment structure will likely lead to significant debris being dispersed across the zone being impacted. Therefore, adjacent buildings, penetrations and distribution subsystems being routed through penetrations will need to be assessed for potential damage due to falling debris. Falling debris could consist of large fragments, such as the fuselage, wing parts, engines or the landing gear.

In general, it can be assumed that external fires caused by aircraft crashes will not have a long duration. Consequently, they will not have a significant influence on the systems required to provide cooling to the reactor vessel or to the spent fuel pool. This is a reasonable assumption based on: (i) in the open air, there is a continuous supply of oxygen to support fuel combustion; and (ii) access to the fire by firefighters is normally good. The in-plant evaluation needs to assess the potential for jet fuel to penetrate underground chases that contain piping, cabling and other commodities. If no flow path exists, then the potential for the failure of commodities inside the chases may be screened out. If a flow path exists, the potential for fire and its effects on SSC items needs to be evaluated.

However, if the impact leads to perforation of the structure, it is very likely that an internal fire will result. The fire will be fed by both jet fuel and potentially by secondary combustible material stored within the structure. In this case, the damage caused by the fire can extend well beyond the area of local structural damage, since the ignition of the fuel can cause an initial fireball with overpressure effects propagating within the building and, in addition, the jet fuel can spread through open pathways, reaching other areas of the building.

The likely scenario is that, just after impact, an internal fireball develops, caused by the combustion of the dispersed jet fuel spray (mist and droplets). The fireball causes an overpressure wave, which is able to fail doors, windows and panels that are not rated for at least a pressure of 35 kPa. The overpressure wave will propagate throughout the building, through large openings such as hatches, grating and stairwells. In addition, the heating, ventilation and air-conditioning ducts in the impacted area (structural/physical damage footprint) are expected to be severely torn and crushed. Hence, the ductwork that crosses the impacted area also provides a pathway for the fireball, smoke and combustion gases to spread to adjacent rooms.

Under the overpressure, the expected failure mode of common metal fireproof doors is buckling of the door. Hence, doors that have failed under pressure cannot be closed again. As the fireball propagates through openings and failed doors, additional parts of the building are threatened.

The initial deflagration will consume a significant portion of fuel, and another important part will be coating internal structures and equipment. Thus, the amount of fuel that could accumulate in pools and flow to other areas is only a fraction of the total initial amount. However, it can easily pass through openings such as grating and blown-up doors. In theory, it is possible that the fuel passes through small openings, but this is normally not significant. According to Ref. [12], the analysis only needs to consider openings with a linear perimeter greater than 30 cm.

In contrast to external fires, it needs to be assumed that a ventilation controlled fire will burn for several hours and, as a consequence, operations staff will not be able to take manual actions in the affected areas. The methodology in Ref. [12] assumes that all SSCs are lost instantaneously in the structural/physical damage footprint and that all cabling and electrical equipment in cubicles affected by the fire are available for just five minutes.

It should be noted that a fire with a longer duration might affect building structural capacity, and partial, or global, collapse caused by structural degradation is a possibility [8].

Reference [12] has a two step process for identifying the potential new compartment connections due to overpressure and the spread of fire damage through connected compartments.

### 5.6.6. Margin assessment

In summary, the major steps for margin assessment for an aircraft crash are the following:

(1) To review the aircraft to be considered by type, size, impact angle and amount of jet fuel or the loading parameters defined.
(2) To choose the reference parameter for fragility or margin evaluation (e.g. the impact velocity).
(3) To construct the zone of influence for a specific location of impact, which comprises an impact zone, a debris zone and a fire and smoke zone (see Fig. 2, Section 3.2), and to identify the SSCs that are in this zone: Depending on the structure impacted, there may or may not be any damage or breach (e.g. the containment may withstand the aircraft impact, including engines, without damage, whereas the auxiliary building may be breached). Therefore, some SSCs may be affected by the aircraft impact, while others may be affected by secondary missiles and/or heat generated by the jet fuel fire. The empirical formulas for local behaviour and the global response procedures discussed above are used to determine whether or not the structure is damaged for this aircraft crash [8].
(4) To determine the fire and smoke zone for the amount of jet fuel available at impact: The zone is also dependent on the resistance of the structure impacted. Depending on the type of aircraft, the 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, the probabilities of failure for impact and heat are defined 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 impact or fire, whichever is more critical. A conservative approximation is to assume that all equipment, including piping and cabling, within the zone of influence is lost.
(5) To calculate the median (best estimate) aircraft velocity for breach, or instability (i.e. overturning or sliding), of the building, and to estimate the uncertainty $\beta_c$ for this velocity.
(6) To calculate the median and uncertainty $\beta_c$ for other SSCs due to secondary missiles and heat loading.
(7) To perform a systems analysis to develop the accident sequences and, with the SSC fragilities appearing in these sequences, to calculate the plant level fragility: The aircraft velocity for which the probability of failure is 1% is also to be calculated.

(8) To use, as an alternative, the systems analysis to derive success paths.
(9) To assess the SSC capacities on these success paths (in terms of reference parameters) to safely withstand the impact of aircraft, secondary missiles and heat loading: The lowest SSC capacity 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 crashes is the lowest of margins so calculated.

## 5.7. EXPLOSION

### 5.7.1. General

This category of human induced event comprises accidents involving explosive cargo carried on transport routes near the nuclear power plant (e.g. trucks, rail cars and barges carrying explosives). Probabilistic analysis procedures exist for calculating the frequency of exceeding different levels of overpressure at the nuclear power plant structures from accidents on these routes. They take into account the location of the plant from the transport route, the frequency and magnitude of explosives transported, and the frequency of accidents per unit distance along the route. For postulated explosions, the loading conditions of importance are the overpressure, missiles and fires.

NS-G-1.5 [5] and Ref. [8] discuss the different types of explosion: deflagration and detonation. Explosions of gas or vapour clouds and solid explosion are also discussed. Paragraph 6.8 of NS-G-1.5 [5] states that:

> "In general the effects of explosions which are generally of concern when analysing structural response are:
>
> — incident and reflected pressure (mainly from detonation),
> — time dependence of overpressure and drag pressure,
> — blast generated missiles,
> — blast induced ground motion (mainly from detonation),
> — heat or fire."

Paragraph 6.23 of NS-G-1.5 [5] states that:

> "There are two principal ways of determining the design basis parameters so as to protect the nuclear power plant against unacceptable damage by pressure waves from detonations:

(1) If there is a potential source in the vicinity of the plant that can produce a pressure wave..., propagation of the wave to the plant can be calculated and the resulting pressure wave and associated drag force will be the basis for the design.
(2) If there is already a design requirement to provide protection against other events (such as tornadoes), a value should be calculated for the corresponding overpressure. This value allows the calculation of safe distances between the plant and any potential source. That is, distances from the source are given at which the pressure wave is calculated not to exceed the overpressure corresponding to the design basis for the other event. This can also be done if there is a design basis for the entire plant against overpressure or if the design basis of the least protected structure, system or component important to safety is known."

NS-G-3.1 [3], NS-G-1.5 [5] and Ref. [8] provide methods to calculate the blast peak overpressure for detonation and deflagration. Annex II of NS-G-1.5 [5] also lists the median capacities and the HCLPF capacities in terms of overpressure for different types of SSC.

### 5.7.2. Specific hazard

The hazard can be specified in terms of location, type and quantity. The objective is then to determine whether the nuclear power plant can withstand the effects of an explosion with a sufficient margin. Another way is to determine what is assessed as the maximum quantity of explosion that the plant can withstand at a specific location (e.g. the plant fence). (See the discussion on safe distances in para. 6.23 of NS-G-1.5 [5] outlined in Section 5.7.1.)

### 5.7.3. Pressure loading

For a specified hazard at a fixed location or along a transport route, the resulting overpressure can be developed as a function of the quantity of explosives using the procedures given in Ref. [8]. If the overpressure exceeds the capacity of the structure, the structure is considered to have failed; if there are safety related equipment items housed within this structure, they are also deemed to have failed.

### 5.7.4. Missile

Blast generated missiles of two types are of potential concern: fragments of the explosive container itself; and missiles projected by the blast waves as they pass from the explosive source to the target. Examples of the latter are failed items in the path of the wave, such as items of equipment. These concerns are treated in the same manner as described for evaluating projectiles from an aircraft crash.

### 5.7.5. Fire

To evaluate the impact of exterior fires on the plant structures, the fires are typically 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 threat. 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. [8]. 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 fire 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.

The potential for these different effects needs to be evaluated for the given hazard scenario. Once the relevant fire scenario is determined, correlations provided in Ref. [8] can be used to determine the potential for structural failure of adjacent plant structures. In this approach, the probability of structural failure and the spread of interior fires through facility buildings can be determined.

### 5.7.6. Margin assessment

Contact and non-contact explosions are addressed in Ref. [8]. Only non-contact explosions are discussed here. In summary, the major steps for margin assessment for non-contact explosion are the following:

(1) To describe the characteristics of the explosion;
(2) To calculate the overpressure at different structures within the nuclear power plant;

(3) To assess whether each structure can safely withstand the overpressure (depending on the objective, it could be the median capacity or a conservative capacity);
(4) To determine the capability of exposed structures against the heat load if a fire is postulated;
(5) To assume structural collapse will result in the failure of all equipment, piping and cabling within the structure; partial collapse of structures is to be addressed for its impact on equipment, piping and distribution systems housed or supported therein;
(6) To assess from the success paths developed for the nuclear power plant whether a success path could be achieved without the SSCs conceded to have failed because of explosion effects (if step 6 is successful, the nuclear power plant has a margin against the specified explosion hazard, but it does not quantify this margin);
(7) To estimate the parameters of the explosion that would result in not achieving the success path (this is the margin in terms of explosive parameters).

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

# 6. STRATEGIES FOR ENHANCING SAFETY

## 6.1. GENERAL

For each human induced event, the margin assessment will result in an estimation of the expected plant margin. In the process, the SSCs and emergency procedures that contribute to the margin are identified. In some cases, it could be a low SSC capacity that dominates the plant margin. In another case, it could be the lack of redundancy created by the fact that a single event (e.g. the aircraft impact location) could breach containment and damage redundant safety trains. In another case, the inadequate emergency response (e.g. firefighting) could have exacerbated fire damage. Having identified these weak links, the nuclear power plant operator needs to explore the strategies for enhancing the margin. The strategies vary depending on whether it is an existing plant or a new plant.

Once the need for upgrading has been recognized, reasonable objectives need to be developed according to the safety criteria mentioned above. In general, upgrading measures can be of a different nature, such as system upgrading, the

strengthening of structures and barriers, operational and administrative aspects, and security. Preference is to be given to measures that are related to hardware upgrading rather than those based upon administrative measures.

Emergency measures may need to be invoked in the case of events beyond what was considered in the design. Coordination among on-site and off-site emergency teams may be required. Having identified vulnerabilities — either through preliminary screening studies or through detailed margin evaluations — the most effective methods to resolve them need to be determined.

For others, it may be shown that the nuclear power plant would survive a particular human induced external event, but with insufficient guarantees due to uncertainties in the analysis or due to low margins. Regardless of the failure case, the consequences are to be considered, for example from reduction in redundancy for cases where plant performance requires full redundancy, to direct and significant releases. In addition, the relative likelihood of both failure and the event may play a role in evaluating the upgrading priorities.

It is recognized that, for some event scenarios, the damage to the plant may be so extensive that existing plant training and procedures may be neither applicable nor adequate. For such events, specific procedures for operator actions are to be developed if the events are identified at the completion of the assessment.

## 6.2. ENHANCEMENT MEASURES

There is a spectrum of possible identified measures to enhance the safety of the plant from human induced events, taking into consideration feasibility and economic viability.

For an existing plant, these include:

— The strengthening of, or additions to, structural barriers;
— Additions to, or the relocation of, equipment and systems to reduce the exposure to, or to mitigate, the hazard loading environment;
— Enhanced emergency procedures.

For a new plant, these include:

— Additions to, or the relocation of, equipment and systems to reduce the exposure to, or to mitigate, the hazard loading environment;
— The enhanced design of structural barriers;

— The strengthening or introduction of redundancies or layout separation in the plant safety systems;
— Enhanced emergency procedures.

# REFERENCES


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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3 (Rev. 1), IAEA, Vienna (2016).

[3] 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).

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

[5] 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).

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

[7] 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).

[8] 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).

[9] CANADIAN NUCLEAR SAFETY COMMISSION, Design of Reactor Facilities: Nuclear Power Plants, CNSC REGDOC-2.5.2, CNSC, Ottawa (2014).

[10] AMERICAN SOCIETY OF CIVIL ENGINEERS, The Pentagon Building Performance Report, ASCE, Reston, VA (2003).

[11] FEDERAL EMERGENCY MANAGEMENT AGENCY, World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations, FEMA 403, FEMA, New York (2002).

[12] NUCLEAR ENERGY INSTITUTE, Methodology for Performing Aircraft Impact Assessment for New Plant Designs, NEI 07-13, Rev. 8P, NEI, Washington, DC (2011).

[13] KENNEDY, R.P., RAVINDRA, M.K., Seismic fragilities for nuclear power plant risk studies, Nucl. Eng. Des. **79** (1984) 47–68.

[14] ANDONOV, A., ILIEV, A., KOSTOV, M., "Fragility assessment of a pre-stressed concrete containment for aircraft impact" (Proc. 22nd Int. Conf. on Structural Mechanics in Reactor Technology, SMiRT 22, San Francisco, California, 2013).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).
[16] ELECTRIC POWER RESEARCH INSTITUTE, A Methodology for Assessment of Nuclear Power Plant Seismic Margin (Revision 1), NP-6041-SL, Rev. 1, EPRI, Palo Alto, CA (1991).
[17] PRATT, W.T., MUBAYI, V., CHU, T.L., MARTINEZ-GURIDI, G., LEHNER, J., An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events, Rep. NUREG/CR-6595, Rev. 1, Brookhaven National Laboratory, New York (2004).
[18] UNITED STATES DEPARTMENT OF ENERGY, Accident Analysis for Aircraft Crash in Hazardous Facilities, Rep. DOE-STD-3014-2006, USDOE, Washington, DC (2006).

## Annex I

## EXAMPLE OF REFERENCE PARAMETERS FOR LOADING EFFECTS

Each human induced external event is characterized by the appropriate load effects (i.e. impact, overpressure and temperature). A reference parameter (e.g. peak of the pressure–time history, missile velocity and mass of the fuel) is selected to represent each load effect in order to evaluate the structures, systems and components (SSCs) using deterministic or probabilistic methods. Table I–1 provides the relevant parameters to characterize the load for mechanical impacts, explosions and fires.

TABLE I–1. SUMMARY OF HAZARDS AND LOADS CAUSED BY HUMAN INDUCED EXTERNAL EVENTS

| | Hazard | | | | | |
|---|---|---|---|---|---|---|
| | Mechanical impact | | Explosion | | Fire | |
| | Hard | Soft | | | | |
| Load | Missile impact load | Missile impact load | Blast or pressure load | | Thermal load, smoke | |
| Load type | Dynamic | Dynamic | Equivalent Static | Impulsive Dynamic | Fire ball | Pool fire |
| Parameters to characterize load | Missile mass, velocity, missile cross-sectional area | Missile mass, velocity, crushing force | Pressure | Pressure transient | Fuel mass | Fuel mass, burning rate |

**Source:** See Ref. [I–1].

A specific human induced external event may have several load effects. Considering an aircraft crash, the hazard could be described by the type of aircraft, mass, shape, deformability, velocity, impact angle and amount of jet fuel. The crash may result in the soft impact of the aircraft fuselage and wings on the buildings, the hard impact of the aircraft engine, fire from the jet fuel and the impact of secondary missiles. For the load effect of the impact, an appropriate

reference parameter would be the aircraft velocity. The other variables (i.e. mass, shape, deformability, impact angle and amount of jet fuel) are taken into account in evaluating the loads on the SSCs. For margin evaluation, the aircraft velocity at which the nuclear power plant would suffer unacceptable damage is estimated using deterministic or probabilistic methods.

For example, if a standard aircraft is considered, the aircraft mass, engine mass and other geometrical properties are obtained from publicly available sources. The margin assessment would be to determine the impact velocity for which the nuclear power plant would suffer unacceptable damage (e.g. core damage or large early release). This velocity, defined as the high confidence of low probability of failure (HCLPF) value, could be calculated using either deterministic or probabilistic methods. The analyst may report this margin to be 135 m/s. If the hazard is an extreme event such as the crash of a large passenger aircraft, the analyst may report the best estimate velocity using best estimate models and parameter values.

It is shown in Ref. [I–1] that the thermal load due to fire hazard and its effect on SSCs can be described as a function of the mass of the fuel exposed to the fire. Admittedly, other factors such as the fire barrier design, type of fire scenario (i.e. a fireball or pool fire) and availability of fire protection systems contribute to the duration of the fire and the effect on SSCs. For margin assessment purposes, the reference parameter for thermal load could be taken as the mass of the fuel.

Explosions could result in blast pressure loading, blast generated missiles, blast induced ground motion and thermal loading. In the case of a distant blast, the main loading condition is the overpressure caused by the incoming pressure wave on a structure increased by wave refraction. The magnitude of the pressure wave depends on the energy or trinitrotoluene equivalent of the explosive as well as the distance from the source to the structure. As shown in Ref. [I–1], the peak side-on overpressure, $Ps_0$, is the key parameter that describes the incident pressure wave due to the blast. For margin assessment purposes, the reference parameter for load effect due to explosions could be taken as the peak side-on overpressure.

## REFERENCE

[I–1] 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).

## Annex II

## APPLICATION OF PSA METHODS TO AN AIRCRAFT CRASH

### II–1. OVERVIEW

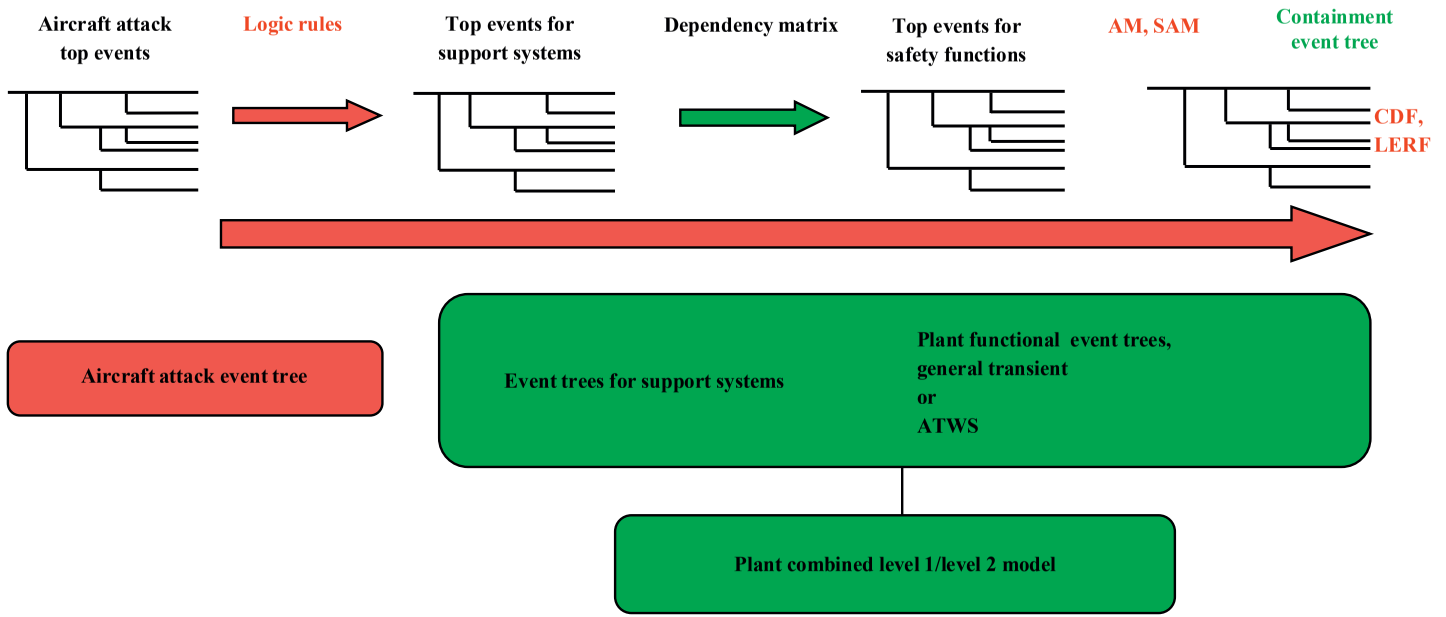
Figure II–1 shows the adaptation of an existing probabilistic safety assessment (PSA) model to the safety assessment of postulated events. The original model was developed based on the linked event tree approach, using specialized software for random internal and external events [II–1]. The model was adapted for the analysis of the consequences of aircraft crash scenarios on nuclear power plants, similar to the events of 11 September 2001, which was performed in Switzerland [II–2].

The parts of the model shown in green were available before the start of the analysis of the aircraft crash scenario. The parts shown in red had to be adjusted or newly developed. As Fig. II–1 demonstrates, the dependency between support functions and frontline safety systems had been available before the analysis. This also includes implicitly the complete definition of all possible safety shutdown paths, a human reliability model for the essential operator actions, some models for accident management and, to a certain extent, for severe accident management actions.

The task for the new analysis could be thus reduced to perform a hazard scenario specific event sequence analysis, which included:

(a) Analysis and evaluation of possible functional impacts of the aircraft crash based on:
   — Detailed analysis of possible crash scenarios;
   — Detailed analysis and classification of possible impactors (types of aircraft, engines and main structural characteristics);
   — Development of impact load, deflagration load and fire heat load characteristics;
   — Accident sequence classification based on possible functional impacts and definition of critical failure modes.

(b) Extended structural analysis for important buildings and structures for the evaluation of load capacities:
   — Assessment of the effects of the scenarios analysed on operator actions, accident management and severe accident management actions (preventive and mitigating actions);
   — Evaluation of failure probabilities for structures and




**Note:** AM — accident management; ATWS — anticipated transient without scram; CDF — core damage frequency; LEFR — large early release frequency; SAM — severe accident management.

*FIG. II–1. Example of the adaptation of an existing plant specific PSA model for the assessment of malevolent events: aircraft attack.*

equipment relevant to the scenario;
— Adjustment of human error failure probabilities for operator actions and accident management actions (preventive and mitigative actions).

(c) The development of modifications to the existing plant logic model describing the possible functional impacts by a corresponding set of logic rules.

(d) Quantification of the model and sensitivity analysis.

## II–2. ANALYSIS AND EVALUATION OF FUNCTIONAL IMPACTS

The first step in this analysis was to define and evaluate site specific aircraft crash scenarios. This included a detailed analysis of possible impactors:

— Types of aircraft and their structural characteristics;
— Types and characteristics of aircraft engine and other hard parts.

The evaluation of crash scenarios included:

— Analysis of the events of 11 September 2001 scenarios;
— Structured interviews with experienced airline flight captains on possible crash scenarios and realistic impact velocities;
— Site specific, full scope plant simulator exercises for the simulation of the crash scenarios.

Data distributions for site specific realistic impact velocities (normal distributions), crash angles and hit accuracy were derived from interviews and flight simulations. Based on the analysis, it was decided to perform an enveloping analysis, covering all types of commercial aircraft and their engines. For this purpose, five classes of commercial aircraft were defined, for which representative types of aircraft were selected for detailed analysis. For the analysis of engines, seven different classes were developed, which were analysed in the attack scenarios. Tables II–1 and II–2 show typical characteristics of aircraft and aircraft engines used in the analysis.

TABLE II–1. CLASSIFICATION OF REPRESENTATIVE COMMERCIAL AIRCRAFT

| Class | Type | Maximum take-off mass (kg) | Average mass to length relation (kg/m) | Maximum fuel load (L) | Relative frequency of occurrence (for the class in 2000) (%) |
|---|---|---|---|---|---|
| Turboprops | SAAB 2000 | 22 800 | 843.5 | ca. 5 000 | 29.95 |
| Regional jets | FOKKER 100 | 44 450 | 1 250.3 | 13 040 | 7.07 |
| Short distance commercials | A 320 | 77 700 | 2 066.5 | 23 860 | 37.02 |
| Medium distance commercials | A 310 | 150 000 | 3 082.6 | 68 100 | 7.97 |
| Long distance commercials | B747-400 | 396 890 | 5 616.8 | 216 980 | 17.99 |

TABLE II–2. CLASSIFICATION OF REPRESENTATIVE AIRCRAFT ENGINES

| Class | Type | Mass (kg) | Fan tip diameter (m) |
|---|---|---|---|
| 0 | Allison GMA 2100 A | 600 (evaluated) | 0.86 |
| 1 | RR Tay 650(651) | 1533 | 1.14 |
| 2 | Weighted over typical engine characteristics | 2980 | 1.79 |
| 3 | GE CF6-80A3 | 3959 | 2.19 |
| 4 | Trent 772 | 4788 | 2.47 |
| 5 | Trent 800er Series | 6486 | 2.85 |
| 6 | Broken Trent 800er | 2962 | 1.37* |

* Intermediate pressure compressor part.

The characteristics of the impactors (aircraft and aircraft engines) were used to develop impact load characteristics, deflagration load characteristics (based on the fraction of fuel load ignited in a deflagration mode following the impact) and fire load characteristics (pool fire load outside the plant buildings in open areas and on flat ceilings).

For the development of the load–time functions for the aircraft, the Riera approach was used, as described in Ref. [II–3]. For the development of the load–time characteristics, data on the mass distribution and on the plastic resistance from literature and vendors were used. Figures II–2 and II–3 show examples of load–time functions for different types of aircraft and impact velocity. A total set of 36 load–time functions for the different aircraft classes and for different impact velocitys were developed as the basis for the analysis of the load capacity of important buildings and structures.

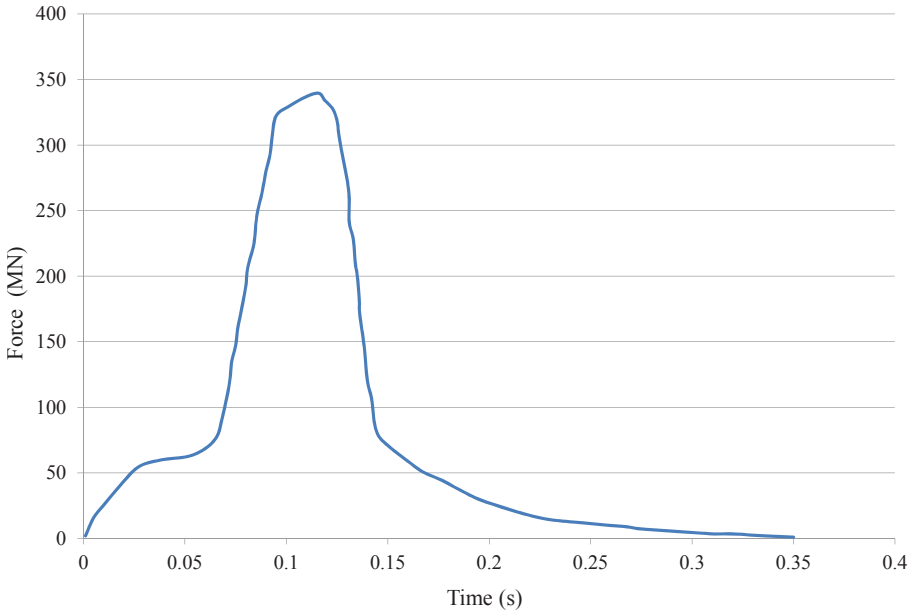



*FIG. II–2. Example of a force–time function for a generic Airbus A310, impact velocity 180 m/s.*

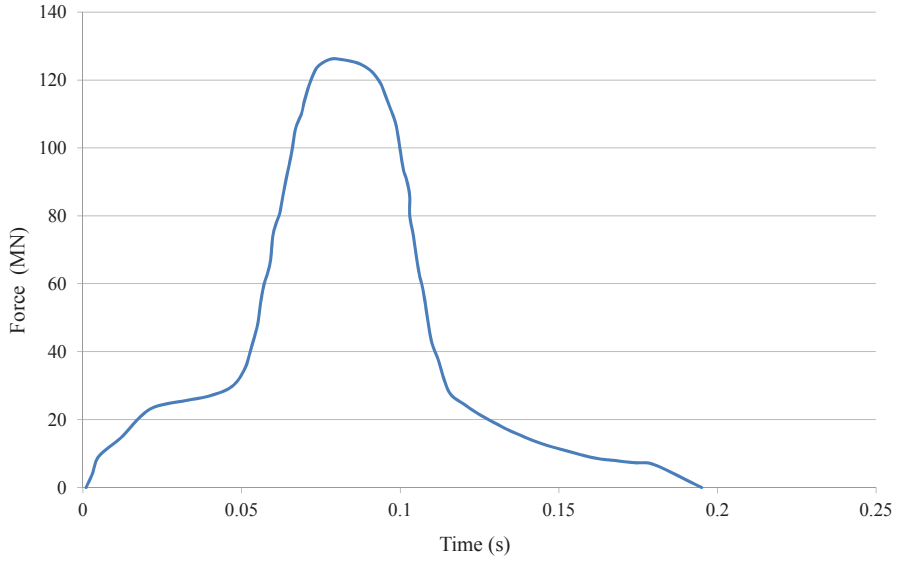



*FIG. II–3. Example of a force–time function for a generic Fokker 100, impact velocity 180 m/s.*

Additional mechanical impact load characteristics were developed for debris loads. Because the spatial distribution of debris cannot be defined exactly, a set of equivalent loads for different types of debris were developed for the evaluation of required protection depth of defending walls:

(a) Tail, with a mass of 15 tonnes and an impact velocity of 20 m/s (normal direction):
— For tail loads from large aircraft, a minimal protection depth of 0.8 m was required (otherwise guaranteed failed).

(b) Non-massive debris:
— Small, deformable parts, with a total mass of 250 kg and an equivalent impact diameter of 30 cm;
— Normal distribution of the impact velocity, with a mean value of $\mu = 60$ m/s, and standard deviation of $\sigma = 8$ m/s.

(c) Impact of aircraft engines (not normally directed impact):
— Characteristics of the engines given in Table II–2 used with a normal distribution of the impact velocity, with mean value of $\mu = 50$ m/s and standard deviation of $\sigma = 8$ m/s.

For the development of deflagration loads, measured flame propagation velocities derived from the analysis of the events of the 11 September 2001

scenarios were used. As a typical overpressure load, a value of 5 kPa (without reflexion on building surfaces) was used. The amount of fuel burned in the deflagration depends on the type of aircraft (location of tanks) and was assessed to be in the range of 12–50% of the total fuel load. For pool fire analysis outside the buildings, as a conservative assumption, it was assumed that 50% of the total fuel load can burn in this fire mode. It was demonstrated that outside pool fires do not endanger typical nuclear power plant structures, but they may limit the accessibility to areas from which operator actions or accident management actions have to be performed. The data described above are based on the assumption that the outer wall of the building hit by the airplane will not fail under the load.

An important step for the development of the PSA model is the classification of accident sequence scenarios and the derivation of critical failure modes. Such a classification helps to identify the need for, and the scope of, more detailed structural analysis. For the analysis described here, the following classification was used.

### II–2.1. Fast accident scenarios

Fast accident scenarios are characterized by small time windows for counteractions. This fact substantially reduces the chances for any type of recovery action. Fast accident scenarios may occur as the consequence of:

(a) A direct mechanical impact on the reactor or the reactor cooling system, leading to a large loss of coolant accident (LOCA);
(b) Unisolated induced piping breaks with medium or large break areas;
(c) An induced anticipated transient without scram (ATWS) (if reactor trip system is not designed ‘fail safe’);
(d) Large scale internal fires (with collateral mechanical damage) inside the containment;
(e) A total loss of all supporting functions (fast ‘station blackout’ within one hour after the impact).

### II–2.2. Slow accident scenarios

Slow accident scenarios are characterized by large time windows for counteractions, such as firefighting, accident management (including severe accident management guidelines) for the recovery of core cooling or mitigating potential radioactive releases. The support by external forces under these conditions is feasible.

In these scenarios, the direct loss of coolant is avoided (transient type of accident and small secondary side pipe breaks of a pressurized water reactor)

and the functional sequences which may potentially lead to core damage are characterized by the loss of operational and support systems, for example as the consequence of a long term loss of off-site power, with collateral damage to some redundancies of the safe shutdown systems and later evolving subsequent failures of emergency power supply due to the lack of reserves (i.e. diesel fuel for diesel generators or cooling water for injection systems) for the remaining safe shutdown path.

This classification is important for the assessment of potential releases. They are often related to fast accident scenarios. In the case of slow accident scenarios, they may occur owing to failures of the containment isolation system due to a loss of power supply or air (for air operated isolation valves).

Each of those two categories can take place with both intact and damaged confinement. Based on the given classification of scenarios, it can be concluded that the most critical scenarios with regard to the release of radioactive material are fast accident scenarios with a loss of containment integrity. This provides the basis for focusing the main effort for the evaluation of load capacity on the reactor building. The main impacts and failure modes to be considered with regard to fast accident scenarios are:

(a) Global failure modes:
   — Overturn of the reactor building (aircraft crash and overpressure load for distant explosions);
   — Reactor building collapse due to mechanical impacts and subsequent large internal fires;
   — Induced vibrations, leading to pipe breaks.

(b) Local failure modes:
   — Soft impact — impact of the aircraft as a whole;
   — Penetration of fuselage and centre bay tanks;
   — Large scale bending failure mode;
   — Hard impact — perforation of defence barriers by hard parts (engines) or by detonation impact leading to pipe breaks (LOCA and secondary side breaks);
   — Complete short term station blackout due to combined load effects;
   — Loss of off-site power;
   — Failure of diesel generator buildings by direct mechanical impact of aircraft parts (fuselage, and hard parts such as engines and landing gear) or direct fire impact (internal fires);
   — Additional dependent failure modes, such as induced hydrogen explosions (for generators cooled with hydrogen).

The main impacts and failure modes also to be considered with regard to slow accident scenarios are:

(i) Impact of large scale exterior fires on structures and accessibility of service areas for operator actions and accident management. This includes:
   — Analysis of fuel distribution and possible fuel drain paths (needs to include flat building ceilings and their water drain system);
   — Analysis of smoke propagation and smoke injection into buildings by ventilation systems;
   — Structural stability of buildings submitted to external heat loads;
   — Assessment of fire duration (for a pool type fire with and without interference of firefighters).
(ii) Assessment of the availability of accident management actions and emergency preparedness under the conditions analysed.
(iii) Availability of firefighters and assessment of their equipment (amount of available extinguishing foam).

In the Swiss analysis [II–2], enveloping conservative assumptions were developed with regard to the combined effects of large scale exterior fires and debris loads on buildings not specially designed against external loads. These conservative assumptions were based on two possible scenarios:

(1) Debris loads can cause breaches in the outer walls of buildings, and burning fuel can be injected directly into the building.
(2) Smoke can be injected by ventilation systems into diesel generator buildings, even in the case of recirculation ventilation mode, since diesel generator operation requires the injection of air.

Based on these scenarios, it was assumed that a building with all internal functions would fail in the case of the failure of the outer wall by debris perforation, and that all diesel generators located in the damage sector (zone of influence) would fail in the long term after the impact. To take into account these effects, damage sectors (zones of influence) were defined.

In the case of a large aircraft crash, a damage sector (zone of influence) of 180° was assumed. For smaller aircraft, this sector was reduced to 90°, centred at the impact location. A failure in the long term after the impact means, for example, that reactor protection or engineered safeguard signals, which were challenged at an early stage of the accident and were powered by batteries, would work correctly if they were not failed independently by random failures according to the plant specific failure data distributions. However, the long term emergency power supply provided by the diesel generators in the damage sector

would fail. A long term failure also means that all service areas within the zone of influence were assumed to be inaccessible for plant personnel. Therefore, all recovery actions are assumed to have failed for the damage sectors.

The typical fire duration for a large scale pool fire (50–100 tonnes of kerosene) was assessed to be between 75 minutes and 8 hours. It was demonstrated that this will not cause significant damage to typical reactor building walls. The structural analysis performed for the assessment of the load capacity of buildings was thus subdivided into:

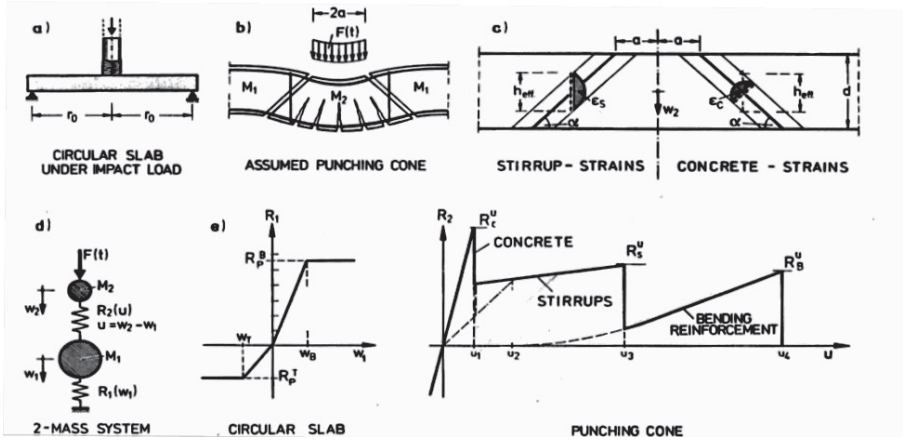
— A detailed analysis for the reactor building (containment) for full aircraft crash loads;
— An analysis for debris load effects for buildings containing equipment required for a safe shutdown.

## II–3. SUPPORTING STRUCTURAL ANALYSIS

The main goal of the structural analyses was to derive failure probabilities of buildings, given the scenario specific load (type of impactor) applied. Because of the large amount of analysis to be performed, simplified, non-linear dynamic elasto-plastic calculation models were developed, which were calibrated against a full scope analysis performed with the large scale commercial code LS-DYNA for one of the Swiss plants. The simplified models were based on the two-mass replacement model suggested in Ref. [II–4], with some improvements to take into account membrane effects due to the large bending deflections observed in the calculations. Figure II–4 illustrates the approach to the development of the replacement model.

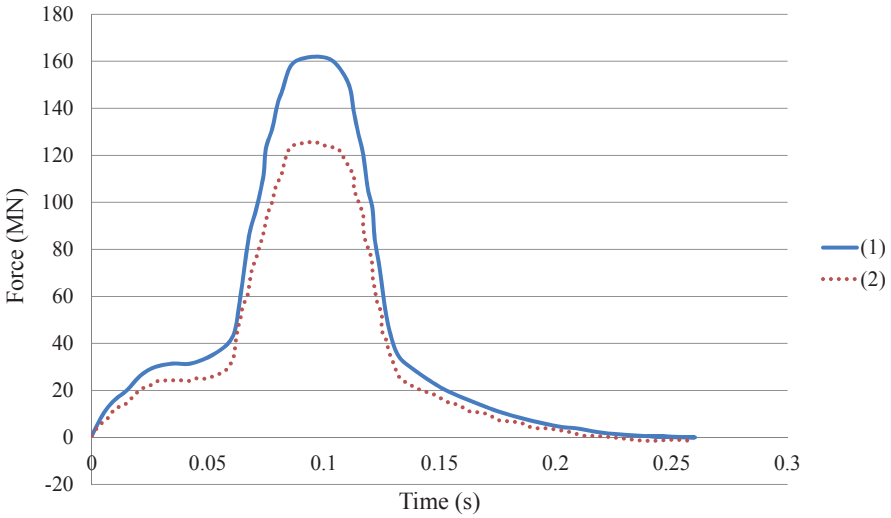
The load capacity of the reactor building was expressed in terms of a normal distribution of the critical failure velocity for the outer walls of the reactor building. In calculating the effective load capacity, the hit accuracy obtained in the flight simulator experiments was taken into consideration. Because it is practically difficult to ensure a hit normally directed at the wall surface for spherical or cylindrical surfaces, the effective load acting towards a perforation of the outer wall can be reduced.

Figure II–5 shows a numerical example for the reduction of load acting in a normal direction to the building surface with a deviation angle (in the vertical direction). This effect was taken into account by a correction factor to the load capacity obtained by the structural analysis for an impact in a normal direction to the surface.




**Note:** (a) Original system; (b) section of the impacted zone; (c) details of punching cone; (d) simulation model; (e) spring characteristics.

*FIG. II–4. Development of the two-mass replacement model (reproduced from Ref. [II–4] with permission).*




**Note:** Generic A320 with an impact velocity of 165 m/s. Impact on a spherical surface (centred impact on visible strip of the reactor building).

*FIG. II–5. Effect of deviation from normal direction on the effective force–time history.*

For all structural analyses, realistic material parameters for the concrete were used. The data were derived from the plant specific ageing management programme. The lower envelope of the obtained empirical data on material strength was used in the analysis, which nevertheless was found to be reasonably higher than typical standard material properties used in the original design. The use of conservative material data allowed the effects of random variation of material properties to be excluded in the uncertainty analysis. The effects of dynamic hardening of concrete and steel were taken into account according to the approach proposed in Ref. [II–4] for uniaxial load cases.

After defining the load capacity of the reactor building in terms of a normal probability distribution of the critical failure velocities, the failure probability of the building can then be defined as the convolution of the probability distributions of the impact velocity with the load capacity distribution. For the analysis of the effects of engine penetration, empirical correlations were used for the Swiss study. For reinforced concrete walls, with an average reinforcement ratio of about 0.8%, the empirical correlation derived by CEA/EDF in Berriaud et al. [II–5] is:

$$T_{\mathrm{p}} = 0.82 f_{\mathrm{c}}^{\,-0.375} \rho^{\,-0.125} \sqrt{\frac{M}{d}} v^{0.75} \qquad \text{(II–1)}$$

where

$T_{\mathrm{p}}$ is the required protection thickness (m);
$f_{\mathrm{c}}$ the ultimate concrete strength (MPa);
$\rho$ the density of concrete (kg/m$^3$);
$M$ the mass of the missile (kg);
$d$ the equivalent diameter of the missile (m);

and $v$ the impact velocity (m/s). The correlation is valid up to an ultimate strength of concrete $f_{\mathrm{c}}$ of 45 MPa.

An analysis of the results of the Sandia National Laboratory experiments with small engine models shows that an aircraft engine can be regarded as a deformable missile [II–6, II–7]. If this effect is taken into account, the required protection thickness to avoid perforation can be reduced by multiplying the result from the CEA/EDF equation in Ref. [II–5] by a factor of 0.7.

An alternative way of calculating the required protection thickness is by using the Degen correlation [II–7, II–8]:

$$T_{\mathrm{p}} = 0.65\left[2.2\frac{X_{\mathrm{p}}}{d} - 0.3\left(\frac{X_{\mathrm{p}}}{d}\right)^2\right]d \qquad \text{(II–2)}$$

where $X_{\mathrm{p}}$ is the penetration depth, which can be defined based on the modified National Defense Research Committee formulas or on dynamic penetration analysis [II–3]. The 0.65 factor already accounts for the deformability of the missile.

Figure II–6 shows the calculated wall failure probability for the different classes of aircraft engines discussed in Table II–2 for the range of impact velocities developed for the plant specific situation at one of the Swiss nuclear power plant sites.

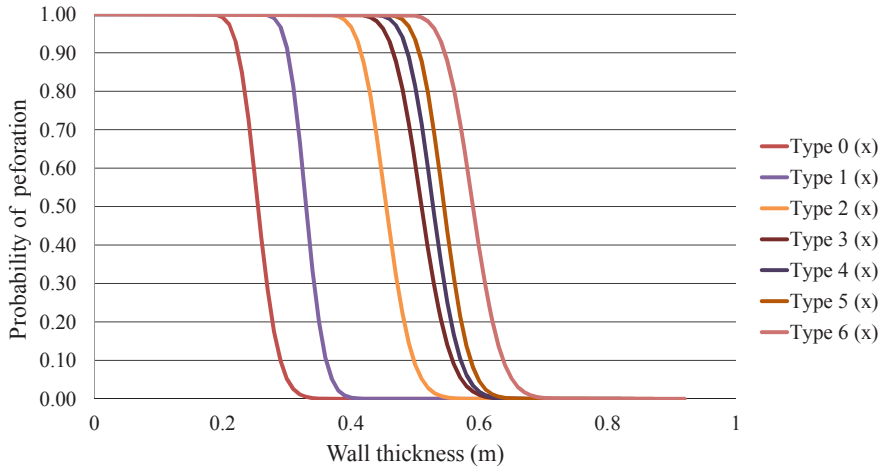



*FIG. II–6. Perforation probabilities for different engine classes as a function of defending wall thickness (m).*

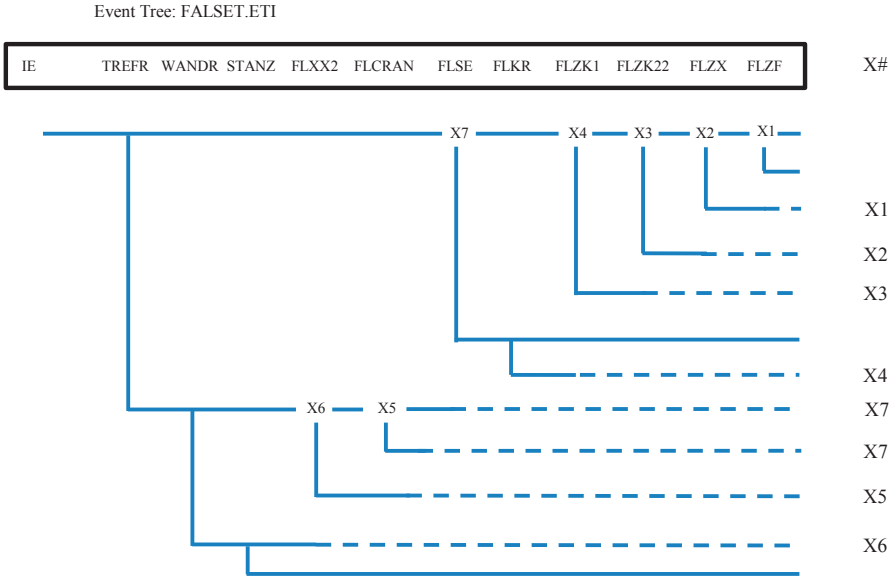
The performed analysis demonstrated that a defence wall thickness of approximately 0.7 m of high strength concrete ensures a low probability of perforation for typical aircraft engines. The analysis also showed that the most challenging load to a modern reactor building concerning the mechanical impact is the load from the soft impact caused by the aircraft crash (main body and fuselage).

With respect to the possible global failure mode due to overturn, a rather simple dynamic calculation based on an equivalent one-mass linear elastic model with two degrees of freedom demonstrated that this failure mode can be excluded from further consideration owing to the large mass of the reactor buildings analysed in the Swiss study [II–2]. The same applies to heat loads due to exterior fires. A bounding heat conduction problem analysis showed that typical containment structures will not fail under these heat loads.

To incorporate the effects of induced vibrations, the analogy to earthquake vibrations was used. For this purpose, a special analysis with a linear elastic model was performed using the commercial computer code ANSYS, and the calculated response spectra for the induced vibrations were compared with response spectra for the safe shutdown earthquake. Based on this comparison, it was concluded that vibrations induced by the impact of a large aircraft can be enveloped by the effects of a strong earthquake. It was conservatively assumed that the failure probabilities for critical components (top events) can be derived from the seismic PSA using the values for a shaking level which corresponds to twice the size of the safe shutdown earthquake of the plant (0.3g peak ground acceleration).

## II–4. DEVELOPMENT OF THE PLANT LOGIC MODEL

Based on the analysis performed, the special event tree (pre-tree) for modelling aircraft crashes was developed. The structure of the event tree used for one of the plants in the Swiss study is shown in Fig. II–7 [II–2]. Table II–3 illustrates the meaning of the top events used in the event tree.




**Note:** Top events are described in Table II–3.

*FIG. II–7. Aircraft crash sample event tree.*

## TABLE II–3. DESCRIPTION OF TOP EVENTS IN THE EXAMPLE EVENT TREE

| Top event | Description | Effect on plant logic model | Comment |
|---|---|---|---|
| IE | Initiating event: aircraft crash from a predefined direction | Loss of off-site power, long term failures in the damage sector due to combined effects of debris loads, fire and smoke propagation | Initiating event frequency equals the likelihood of the selection of the crash direction, the sum of all initiating event frequencies for each airplane class equals 1 (conditional risk quantification) |
| TREFR | Failure of top event TREFR means that the reactor building was successfully hit by the aircraft | For surrounding buildings debris loads, fire and smoke propagation have to be taken into account | Successful hit inside the no slide-off zone (spherical containment surface) |

TABLE II–3. DESCRIPTION OF TOP EVENTS IN THE EXAMPLE EVENT TREE (cont.)

| Top event | Description | Effect on plant logic model | Comment |
|---|---|---|---|
| WANDR | Failure of top event WANDR means that the reactor building was hit at high velocity | Assumed failure of safety equipment inside the reactor building in the surrounding of the impact zone: failure of one redundancy of the safety system (high pressure injection, residual heat removal cooling), failure of isolation of secondary containment (small line) | Outer wall cracking, no perforation |
| STANZ | Failure of top event STANZ means that the reactor building is perforated | Internal fire inside the reactor building modelled as direct core damage with failed containment (large release) | Conditional probability of large building perforation (TREFR = F, WANDR = F) based on convolution of distributions of impact velocity and critical perforation velocity of building quantified conditionally |
| FLXX2 | Failure of top event FLXX2 means that an induced medium/ large pipe break occurred owing to induced vibrations | Modelled as an unisolated pipe break in the reactor building annulus, large containment bypass | Split fraction derived from seismic PSA for a vibration level corresponding to a strong earthquake (twice the safe shutdown earthquake level), considered only for large aircraft |
| FLCRAN | Failure of top event FLCRAN means that a structural failure of the reactor building crane occurred, leading to an unisolated large steam line break inside containment | Modelled as break of a main steam line for steam generator 2 | Split fraction derived from seismic PSA for a vibration level corresponding to a strong earthquake (twice the safe shutdown earthquake level), considered only for large aircraft |

TABLE II–3. DESCRIPTION OF TOP EVENTS IN THE EXAMPLE EVENT TREE (cont.)

| Top event | Description | Effect on plant logic model | Comment |
|---|---|---|---|
| FLSE | Failure of top event FLSE means a functional failure of electrical building (failure of four redundancies (from six)) | Modelled as guaranteed failure | Only special emergency system (bunkered system) not affected by the impact |
| FLKR | Failure of top event FLKR given a failure of FLSE means a functional failure of all operator actions to be performed from the main control room, physical damage to the shift personnel | Modelled as guaranteed failure of all operator actions and all short term accident management actions | Only long term accident management actions available performed by external forces alarmed by the guards, the main control room is protected by several wall and ceiling layers, ventilation system can be switched to recirculation mode |
| FLZK1 | Failure of top event FLZK1 means a failure of DGB-A | Guaranteed failure of DGB-A, failure of two diesel generators and the corresponding emergency power supply trains | Failures in the damage sector (zone of influence) described above, battery powered reactor protection and engineered safeguard signals not affected, includes also underground power cable failures |
| FLZK2 | Failure of top event FLZK2 means a failure of DGB-B | Guaranteed failure of DGB-B, failure of two diesel generators and the corresponding emergency power supply trains | Failures in the damage sector (zone of influence) described above, battery powered reactor protection and engineered safeguard signals not affected, also includes underground power cable failures |

TABLE II–3. DESCRIPTION OF TOP EVENTS IN THE EXAMPLE EVENT TREE (cont.)

| Top event | Description | Effect on plant logic model | Comment |
|---|---|---|---|
| FLZX | Failure of top event FLZX means a functional failure of the bunkered special emergency system | Guaranteed failure of the bunkered special emergency system (2 diesel driven emergency feedwater pumps, 2 diesel generators, 2 residual heat removal pumps) | Long term failures in the damage sector (zone of influence), battery powered reactor protection and engineered safeguard signals unaffected, due to the topographical conditions, the bunkered system cannot be attacked directly by a large aircraft at high velocity |
| FLZF | Failure of top event FLZF means a functional failure of the turbine building | Guaranteed failure of all equipment inside the turbine building, breaks of feedwater and steam line, which can be isolated outside the turbine building by the automatic isolation signals | Impacts included are:<br>— Damage by mechanical impact<br>— Damage by fire<br>Potential damage by a hydrogen explosion (hydrogen cooled generator) |

**Note:** DGB — diesel generator building; F — failure.

In the study, no allowance was taken for extinguishing the large scale exterior fire or for the area drains removing kerosene from the outside area surface [II–2]. The potential for negative drain effects was analysed and it could be excluded from the model. For other designs, operator actions for successful firefighting outside the buildings were taken into account. Successful firefighting may increase the chance of success of the accident management actions, since the access to essential service areas is improved.

## II–5. QUANTIFICATION

The conditional frequencies of core damage, large early release, and small and large late release were all quantified [II–2]. An uncertainty analysis was performed for the conditional frequency of core damage and large early release. The size of the potential release source terms was estimated based on existing source term calculations performed for the Level 2 PSA.

The results of the quantification and the main contributors to risk are not publicly available owing to security reasons. However, according to the

qualitative results included in Ref. [II–2] for the two older Swiss plants, Beznau and Mühleberg, the possibility of penetration of the reactor building could not be ruled out in the higher impact velocity scenarios. In the case of penetration, the extent of the damage would depend on the consequences of the fire within the building. Other buildings containing emergency systems were adequately protected against fire and debris, but smoke might affect the performance of some emergency equipment outside the reactor building.

For the two most recently constructed plants, Leibstadt and Gösgen, the possibility of penetration of the reactor building was ruled out owing to the negligible frequency. These plants were designed to withstand the impact of a passenger aircraft impacting at 370 km/h, but the analyses showed that they could support the impact of larger aircraft impacting at higher velocities.

## REFERENCES


[II–1] ABS CONSULTING, RISKMAN for Windows: User's Manual, ABS Consulting, Irvine, CA (2003).

[II–2] SWISS FEDERAL NUCLEAR SAFETY INSPECTORATE, Stellungnahme der HSK zur Sicherheit der schweizerischen Kernkraftwerke bei einem vorsätzlichen Flugzeugabsturz, Rep. HSK-AN-4626, HSK, Würenlingen (2003).

[II–3] 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).

[II–4] SCHLÜTER, F.H., "Dicke Stahlbetonplatten unter stossartiger Belastung: Flugzeugabsturz", Vol. 2, Massivbau, Baustofftechnologie Karlsruhe: Schriftreihe des Instituts für Massivbau und Baustofftechnologie, IfMB, Karlsruhe (1987).

[II–5] BERRIAUD, C., VERPEAUX, P., HOFFMANN, A., JAMET, P., AVET-FLANCARD, R., "Test and calculation of the local behaviour of concrete structures under missile impact", Loading Conditions and Structural Analysis of Reactor Containment (Trans. 5th Int. Conf. SMiRT 5, Berlin, 1979), Vol. J, Commission of the European Communitites (1979).

[II–6] MUTO, K., et al., "Experimental studies on local damage of reinforced concrete structures by the impact of deformable missiles", Parts 3 and 4, Structural Mechanics in Reactor Technology (Trans. 10th Int. Conf. SMiRT 10, Anaheim, 1989), American Association for Structural Mechanics in Reactor Technology, Los Angeles, CA (1989).

[II–7] SUGANO, T., et al., Local damage to reinforced concrete structures caused by impact of aircraft engine missiles — Part 2: Evaluation of test results, Nucl. Eng. Des. **140** (1993) 407–423.

[II–8] DEGEN, P.P., Perforation of reinforced concrete slabs by rigid missiles, J. Struct. Div. **106** (1980) 1623–1642.

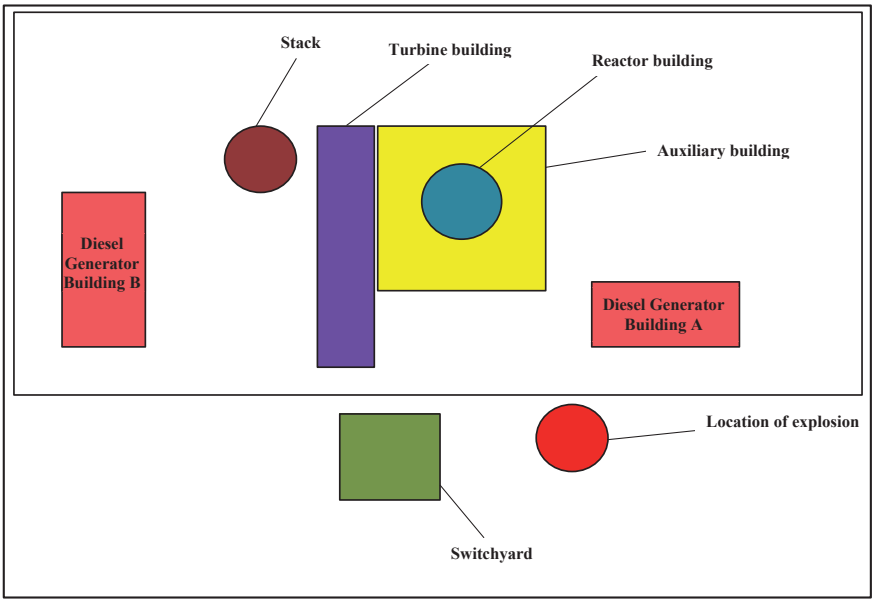
## Annex III

## EXAMPLE APPLICATION OF THE SIMPLIFIED EVENT TREE APPROACH AND ITS ELEMENTS FOR EXPLOSION HAZARD

### III–1. EXTERNAL EXPLOSION: DESCRIPTION OF SCENARIO

It is assumed that outside the site of a nuclear power plant with a boiling water reactor, a full bore rupture of a natural gas pipeline takes place. The gas in the pipeline is liquefied under pressure. A total amount of 30 tonnes of liquefied gas is ejected and a gas cloud forms. The gas is assumed to be methane ($CH_4$).

The purpose of this exercise is to assess the potential consequences of a deflagration of the gas cloud on the safety of the nuclear power plant, after the cloud moved to the location shown in Fig. III–1. The potential deflagration would take place in the immediate vicinity of the switchyard of the plant to the power grid. Tables III–1 and III–2 provide the required input data.




**Note:** Buildings are representative only and not to scale.

*FIG. III–1. Illustration of the explosion scenario.*

TABLE III–1. BUILDING AND STRUCTURE DATA

| Building and structure | Distance (m) | Natural frequency of the building (Hz) | Design overpressure of the building (kPa) |
|---|---|---|---|
| Reactor building surrounded by the auxiliary building | 260 | 5 | 90 |
| Diesel Generator Building A | 200 | 4 | 60 |
| Diesel Generator Building B | 320 | 4 | 60 |
| Auxiliary building (containing emergency core cooling systems, standby liquid control system and main control room) | 245 | 3.3 | 50 |
| Turbine building | 230 | 3.5 | 25 |
| Stack (located behind the turbine building) | 280 | 7 | 55 |

TABLE III–2. BUILDING DIMENSIONS

| Building | Length (m) | Width (m) | Height (m) |
|---|---|---|---|
| Diesel Generator Building A | 10 | 25 | 8 |
| Diesel Generator Building B | 25 | 10 | 8 |
| Turbine building | 75 | 8 | 15 |
| Auxiliary building | 90 | 60 | 35 |
| Reactor building | 60 | 60 | 45 |

Table III–3 provides a template for the mean fragility curve for structures, systems and components (SSCs) under blast loads from distant explosions. The conditional probability of failure is given as a function of ‘equivalent static pressure’ on the component. As described in Ref. [III–1], the equivalent static pressure is computed from the peak overpressure and the natural frequencies. In order to normalize the curve, the equivalent static pressure is divided by the

median capacity equivalent static pressure of the component. Median SSC blast capacities designed for wind gust speeds of 30–35 m/s are given in table II–2 of IAEA Safety Standard Series No. NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants [III–2]. The template for the fragility curve can also be used when the SSC has been specifically designed for blast loadings. In this case, design equivalent static pressure can be linked to a conditional probability of failure of 0.5%. Blast design values for typical structures can be found, for example, in Ref. [III–3].

TABLE III–3. FAILURE PROBABILITIES OF STRUCTURES, SYSTEMS AND COMPONENTS FOR BLAST LOADS FROM DISTANT EXPLOSIONS

| Equivalent static pressure and median capacity equivalent static pressure | Failure probability |
|---|---|
| 2 and higher | 1.00 |
| 1.00 | 0.50 |
| 0.85 | 0.22 |
| 0.75 | 0.083 |
| 0.60 | 0.005 |

## III–2. QUALITATIVE EVALUATION OF THE SCENARIO

The deflagration of the gas cloud will result in a pressure wave hitting the site of the nuclear power plant. Owing to the vicinity of the switchyard of the plant, a loss of off-site power event needs to be assumed as guaranteed. It is very unlikely that an available reserve connection to the external grid would function under the analysed conditions.

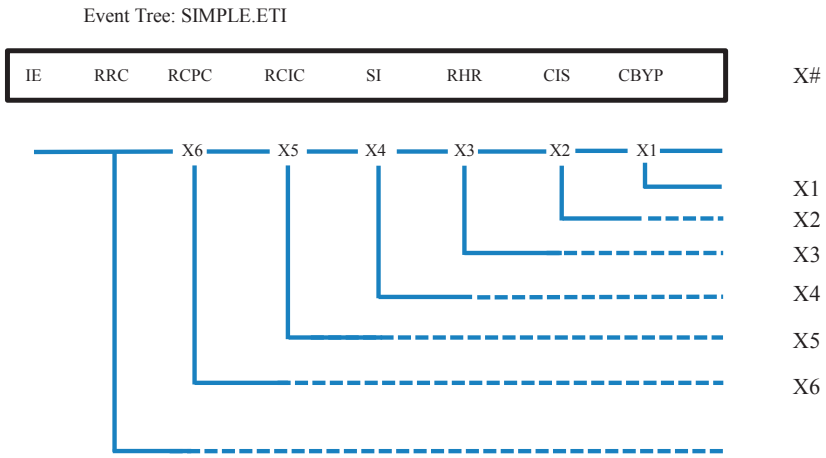
On the other hand, the pressure wave could cause severe damage to the two diesel generator buildings, which may result in a subsequent diesel generator failure and lead to a complete station blackout. The auxiliary building could also fail. In the case that the building remains intact, induced vibrations caused by the pressure wave may cause some piping damage inside the building, resulting in an interfacing system loss of coolant accident (LOCA).

The reactor building is circled by the auxiliary building; hence, damage to the reactor building is very unlikely. Only the upper part of the building is exposed to the pressure wave. Induced vibrations, if strong enough, may result in a failure of the reactor building crane, leading to a steam line break inside containment.

If a stack is located behind the turbine building and in a downward direction of the reactor building, its failure would not lead to any additional damage to the safety related buildings of the plant.

## III–3. DEVELOPMENT OF THE LOGIC MODEL AND FAILURE PROBABILITIES

The standard simplified event tree in Fig. III–2 is used as the baseline model for the analysis. The quantification of the failure probabilities are based on simplified structural analysis and on expert judgement of the consequences of the postulated gas cloud deflagration.




**Note:** Top events are described in Table 1, Section 3.6.2. IE — initiating event.

*FIG. III–2. Simplified event tree.*

### III–3.1. Structural analysis and failure probabilities for structures

The blast overpressures acting on the different buildings and structures are evaluated from the amount of gas in the exploding cloud and the distances. The methods given in Ref. [III–1] can be used for this purpose. The maximum overpressure (reflected pressure) is used for an estimate of the failure probability of a structure or building. As described in Ref. [III–1], based on the natural frequency of the building and on an estimate of the pressure pulse duration, the equivalent static overpressure will be calculated for the buildings and structures. Then, using the fragility curve of Table III–3, the failure probability is calculated. It is assumed that a severe building failure will lead to a complete loss of function of all equipment housed in the building.

In this example, the ratio between the flame front speed and the pressure wave speed is assumed to be 0.3 for $CH_4$. This means that the effective flame front speed is 102 m/s. The expansion ratio for $CH_4$ is 6.12; and combustion equals 0.5 for gas liquefied under pressure.

Because the buildings are mainly built out of concrete, a minimal ductility factor of $\mu = 2$ can be assumed for the calculation of the equivalent static load. Table III–4 shows some intermediate results of the calculation. Table III–5 shows the results of the calculated equivalent static loads and the corresponding failure probabilities.

TABLE III–4. STRUCTURAL ANALYSIS: INTERMEDIATE RESULTS

| Building | Distance (m) | $R_{mix}$ (m)[a] | $R_{cloud}$ (m)[b] | Dimensional distance[c] | Overpressure of incoming wave (kPa) | Peak (reflected) overpressure (kPa) |
|---|---|---|---|---|---|---|
| Diesel Generator Building A | 200 | 58.23 | 106.50 | 3.43 | 6.46 | 13.27 |
| Turbine building | 230 | 58.23 | 106.50 | 3.95 | 5.62 | 11.50 |
| Auxiliary building | 245 | 58.23 | 106.50 | 4.21 | 5.26 | 10.76 |
| Reactor building | 260 | 58.23 | 106.50 | 4.47 | 4.95 | 10.11 |

TABLE III–4. STRUCTURAL ANALYSIS: INTERMEDIATE RESULTS (cont.)

| Building | Distance (m) | $R_{mix}$ (m)[a] | $R_{cloud}$ (m)[b] | Dimensional distance[c] | Overpressure of incoming wave (kPa) | Peak (reflected) overpressure (kPa) |
|---|---|---|---|---|---|---|
| Stack | 280 | 58.23 | 106.50 | 4.81 | 4.58 | 9.35 |
| Diesel Generator Building B | 320 | 58.23 | 106.50 | 5.50 | 3.98 | 8.10 |

[a] Initial radius of cloud from explosive material.
[b] Radius of the cloud after expansion.
[c] The dimensional distance is distance/$R_{mix}$.

TABLE III–5. RESULTS OF STRUCTURAL ANALYSIS: FAILURE PROBABILITIES OF BUILDINGS

| Building | Building period (s) | $t_d/T$[a] | Load factor $P_{max}/P_0$[b] | Equivalent static load (kPa) | Design static overpressure (kPa) | Load/ design ratio[c] | Failure probability |
|---|---|---|---|---|---|---|---|
| Diesel Generator Building A | 0.25 | 0.88 | 1.02 | 13.54 | 60 | 0.23 | 0.001 |
| Turbine building | 0.28 | 3.15 | 1.40 | 16.10 | 25 | 0.64 | 0.005 |
| Auxiliary building | 0.33 | 3.71 | 1.40 | 15.07 | 50 | 0.30 | 0.001 |
| Reactor building | 0.20 | 1.96 | 1.35 | 13.65 | 90 | 0.15 | 0.001 |
| Stack | 0.14 | 2.10 | 1.35 | 12.62 | 55 | 0.23 | 0.001 |
| Diesel Generator Building B | 0.25 | 1.29 | 1.10 | 8.90 | 60 | 0.15 | 0.001 |

[a] Ratio of duration of load to natural period.
[b] Load factor of maximum pressure, $P_{max}$, and ambient pressure, $P_0$.
[c] Ratio of equivalent static load to design static overpressure.

According to the rules derived for the calibration of expert judgement, the minimum value assigned to the building failure probabilities is 0.001. The results of the structural analysis show that the risk of severe structural failures is very low for the analysed case of a gas cloud deflagration outside the site of the plant.

### III–3.2. Split fractions for the simplified event tree

A split fraction (SF) is the conditional probability that a certain top event will fail under the given scenario (path) through the event tree. Following the methodology used in this example, these conditional probabilities are calculated based on a combination of results from the structural analysis and from expert judgement. For the quantification of the event tree, it is important to develop split fractions both for the success and failed states of top events located before the top event is analysed.

For the scenario analysed, the deflagration of the gas cloud would lead to a loss of off-site power transient, which would cause a challenge to the reactor trip system and very likely to main steam lines isolation. The possible damage to the turbine building may cause damage to the main steam lines and hence also lead to an isolation of the main steam lines. In addition, the feedwater supply to the reactor may fail under this condition.

The equipment required for a reactor trip is located inside the reactor building (control rod drives, accumulators, piping and valves) and partially in the auxiliary building (standby liquid control system, main control room and operators to initiate the standby liquid control system). In addition, all accident management actions need to be initiated from the main control room. The structural analysis resulted in a failure probability for both buildings (reactor and auxiliary building) of 0.001. In the case of a failure of the reactor building, the automatic trip function may fail and manual interference is required to start the standby liquid control system or to try to drop control elements with the control rod drive system into the reactor. The likelihood that this action would also fail in the case of severe damage to the reactor building is very high because part of the required equipment is inside the reactor building. The correct Boolean expression would lead to an OR function adding the failure probabilities for both buildings. Because the results of the structural analysis showed a large difference between the required equivalent static load and the design load, and a roundup of the failure probability had already been performed, the likelihood of failure of the reactivity control system can be judged as close to guaranteed success. Thus, the split fraction for the top event ‘reactor reactivity control’ (RRC) is set to 0.001.

For the top event ‘reactor coolant pressure control’ (RCPC), now two failure states are possible. In the case of a successful reactor trip, the possible pressure increase due to the loss of off-site power leading to a steam line isolation

is lower than for the case of failure of the reactor trip system (RRC = fail). The case of successful reactor trip corresponds to the design case, hence the success chances for successful operation of the safety relief valves (SRVs) located inside the reactor building are very high (Evaluation LL[1], SF = 0.01). In the case of failure of the reactor trip function, the challenge to the SRVs is much higher (more valves will be operated for successful limitation of reactor pressure). A failure of the reactor building itself may cause also functional failure of SRVs. Based on this qualitative assessment the result of the expert judgement is that the successful operation of SRVs is uncertain (Evaluation A, SF = 0.5).

The top event 'reactor coolant inventory control' (RCIC) is to be evaluated for (at least) two possible failure states:

— Successful operation of the pressure limitation system (failure state F1);
— Failure of the pressure limitation system (failure state F2).

It is also possible to distinguish different situations depending on the state of the top event RRC because the pressure increase would be different. In the current situation, this is not necessary because any failure of the pressure limitation system would lead to a failure of the top event, which means the loss of inventory.

In the case of the successful operation of the pressure limitation system, the possibility that at least one of the SRVs challenged will not reclose is to be taken into account. The likelihood of this happening is judged to be low (L). The additional impact of a potential loss of off-site power scenario (loss of both diesel generator buildings) on the top event RCIC is very low and included into the expert judgement.

The top event 'safety injection' (SI) will only be challenged if the top event RCIC (inventory control) fails. In all other cases, this function is not necessary at all (failure state F1). In the case of loss of inventory, the failure probability for the safety injection systems is driven by their own reliability and availability (or unavailability due to maintenance) because the failure probability for the auxiliary building housing the required equipment and for the reactor building housing the injection points due to structural damage is very low. The corresponding expert judgement for this situation is L, resulting in the corresponding split fraction value. The additional impact of a potential loss of off-site (emergency) power scenario (loss of both diesel generator buildings) on the top event SI is very low and included into the expert judgement.

---

[1] The scale of evaluation is based on judgement of the expert to assign the probability of failure of a split fraction. Scale can be from LL (very low), L (low), M (medium), A (high), to GF (very high — involves failure of the system).

The top event ‘residual heat removal’ (RHR) has to be analysed for three different failure states:

— Successful reactor trip and successful operation of the pressure limitation system (failure state F1);
— Failure of reactor trip function and failure of pressure limitation system with successful safety injection (failure state F2);
— Failure of reactor trip function and failure of pressure limitation system combined with the failure of the safety injection (failure state F3).

For the failure state F3, it is obvious that there is no chance for successful heat removal, so the failure probability is 1 (GF). Failure states F2 and F1 are slightly different because the operation of RHR systems after, or in combination with, safety injection is more complicated and interdependencies between the systems have to be taken into account. The failure probability of the RHR function due to structural failures is very low. For the failure state F2, the expert evaluation is M, resulting in a split fraction value of 0.25. The corresponding value for the failure state F1 is L (SF = 0.05). The additional impact of a potential loss of off-site power scenario (loss of both diesel generator buildings) on RHR is very low and included into the expert judgement.

For the top event containment isolation (CIS), two separate damage states have to be evaluated:

— No challenge to the system (failure state F1) — leading to a failure probability of 0;
— Failure of isolation due to structural damage, loss of power supply of hardware failures under conditions of concern (failure state F2).

The failure state F1 applies for all circumstances with RCIC = S and RHR = S (no loss of inventory, successful heat removal); the failure state F2 applies to all other conditions. The expert judgement resulted in an assessment as L. The corresponding failure probability is 0.05.

A containment bypass scenario (CBYP) may occur owing to induced vibrations or direct physical damage to piping outside the containment as a consequence of structural building damage. Due to the low overpressure peak values estimated and the relatively long duration of the interaction with the building, the risk of pipe failure outside the containment can be judged as very low (LL), resulting in a split fraction of 0.01. Because the failure probability for direct structural damage to the auxiliary building is much lower than the value derived by expert judgement, the latter is used.

Table III–6 shows the results for the evaluation of top event split fractions in dependence of the failure states as explained.

TABLE III–6. TOP EVENT SPLIT FRACTIONS

| Top event | Description | Failure state | SF value | Comment |
|---|---|---|---|---|
| RRC | Reactor reactivity control | F1 | 0.001 | In the case of reactor building or auxiliary building failure, combined failure modes are very likely to lead to the failure of the complete reactivity control system |
| RCPC | Reactor coolant pressure control | F1 | 0.01 | RRC = S |
| | | F2 | 0.50 | RRC = F |
| RCIC | Reactor coolant inventory control | F1 | 0.05 | SF value governed by the likelihood of the failure to reclose of one of the challenged SRVs, judged as L |
| | | F2 | 1.00 | Failure of pressure limitation system leads to a loss of coolant |
| SI | Safety injection | F1 | 0.00 | No loss of inventory |
| | | F2 | 0.05 | Failure of required amount of trains for safety injection, judged as L |
| RHR | Residual heat removal | F1 | 0.05 | Heat removal after a typical loss of off-site power scenario with main steam line isolation |
| | | F2 | 0.25 | Heat removal under the condition of loss of inventory and operating safety injection system |
| | | F3 | 1.00 | Failed safety injection gives no chance for heat removal |

TABLE III–6. TOP EVENT SPLIT FRACTIONS (cont.)

| Top event | Description | Failure state | SF value | Comment |
|---|---|---|---|---|
| CIS | Containment isolation | F1 | 0.00 | No challenge to the system |
| | | F2 | 0.05 | Expert judgement L, includes also potential structural damage and loss of power or other hardware impacts |
| CBYP | Containment bypass | F1 | 0.01 | Expert judgement LL |

**Note:** L — low; LL — very low; SF — split fraction; SRVs — safety relief valves.

### III–3.3. Plant logic model

Using the scenario description and the failure state definitions, the plant logic model is developed in the format of the simplified event tree used by the methodology (see Fig. III–2). Owing to the simplicity of the model, it is also feasible to evaluate the event tree on the basis of a spreadsheet program.

For the quantification, it is important to define the failure states. It is obvious from the previous discussion that any failure of the RHR top event corresponds to a core damage state (RHR = F). If under this condition the containment isolation fails or a containment bypass occurs, the damage will lead to a large release. So the corresponding logic expressions are:

Core damage: RHR = F
Large release: RHR = F * (CIS = F + CBYP = F)

where '+' indicates a logical OR and '*' indicates a logical AND.

### III–3.4. Results

The event tree in Fig. III–2 is evaluated for an initiating event frequency of 1 (it is postulated that the deflagration occurs) to obtain the required conditional risk measures. After quantification of the event tree for the described blast scenario, the following results were obtained (conditional probabilities of frequency):

— Core damage frequency occurring with isolated containment (no release outside containment): CDF = 0.0600;

— Large release frequency (core damage with open containment): CLRF = 0.00380;
— No damage frequency: CNDF = 0.936.

Evaluating the results, it can be concluded that the sample plant possesses a very high degree of defence against the scenario analysed. In more than 93% of all analysed sequences, the blast scenario will not cause any safety significant damage. The conditional probability of release frequency is very low.

## REFERENCES


[III–1] 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).

[III–2] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standard Series No. NS-G-1.5, IAEA, Vienna (2003).

[III–3] AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, Guidelines for Evaluating Process Plant Buildings for External Explosions and Fires, Center for Chemical Process Safety, New York (1996).

## ANNEX IV

## GUIDANCE TO MITIGATE A SITE DISRUPTIVE ACCIDENT

### IV–1. INTRODUCTION

In the light of the Fukushima Daiichi accident, the IAEA prepared the IAEA Action Plan on Nuclear Safety (the Action Plan) [IV–1]. The Action Plan calls for:

> "The Commission on Safety Standards and the IAEA Secretariat to review, and revise as necessary using the existing process in a more efficient manner, the relevant IAEA Safety Standards[3] in a prioritised sequence.
> "[3] This review could include, inter alia, regulatory structure, emergency preparedness and response, nuclear safety and engineering (site selection and evaluation, assessment of extreme natural hazards including their combined effects, management of severe accidents, station blackout, loss of heat sink, accumulation of explosive gases, nuclear fuel behaviour and ways to ensure the safety of spent fuel storage)."

These are important aspects: the emergency response is vital for protection of the public and the environment, and severe accident management is the tool that plant operators have at their disposal to prevent a damaged core leading to radioactive releases. Severe accident management is typically a series of measures in what is called the mitigative domain: core damage has occurred, and now the consequences are to be mitigated. They are described in a series of severe accident management guidelines (SAMGs).[1]

However, the response to a site disruptive accident is more complex and requires more measures than emergency response or SAMGs. This annex provides an overall description of what is needed, since the accident management could be an integral part of the margin assessment for extreme external events. The purpose is to provide the analyst assessing the margins with an overall view of the requirements for mitigation and the conditions under which plant operators will work after such an accident.

---

[1] See https://www.iaea.org/NuclearPower/SAMG-D/index.html

## IV–2. EXTENSIVE DAMAGE MITIGATION GUIDELINES

Some Member States have developed approaches to the mitigation of a site disruptive accident. An example can be seen in Ref. [IV–2]. These approaches require a number of measures in the preventive domain (i.e. before core damage has occurred) and are largely helped by portable equipment, available on-site as well as off-site. The guidelines concerned are often called extensive damage mitigation guidelines (EDMGs), and there are typically 10–30 guidelines for an operating nuclear power plant.

In general, the approach is twofold:

(1) Actions to restore command and control, should these have been lost;
(2) Actions to mitigate challenges to the reactor and the spent fuel pool, after command and control have been re-established (if lost before).

Command and control can be lost if the site disruptive accident is caused by a large fire or explosion, destroying the control room and emergency shutdown room. Measures need to be in place to assemble remaining or surviving staff to put together a new command and control function, and to establish the emergency response organization (ERO). Such staff may include personnel from security and the fire brigade, among others, and the re-establishing of the ERO includes restoring communication, both on-site as well as with off-site parties (e.g. fire brigades, medical services and police).

The newly formed ERO has a number of tasks (see Fig. IV–1):

(a) If the accident involves a violent action by third parties, the ERO needs to make sure that safe access to all vital areas of the plant will be regained. It is assumed that this is the responsibility of the local security personnel. In addition, the ERO needs to take measures to take care of the wounded and arrange that medical assistance is provided for those in need.
(b) The ERO needs to estimate the damage at the site and to initiate measures to limit such damage. Priority may be given first to the auxiliary and fuel building, then control building and turbine building. Measures may include containing and extinguishing fires, evacuating personnel in danger and making sure sufficient water is available. If the threat is from flooding, personnel needs to be protected, and damage to power sources needs to be limited or mitigated. Other hazardous material is to be secured in agreement with applicable plant procedures.

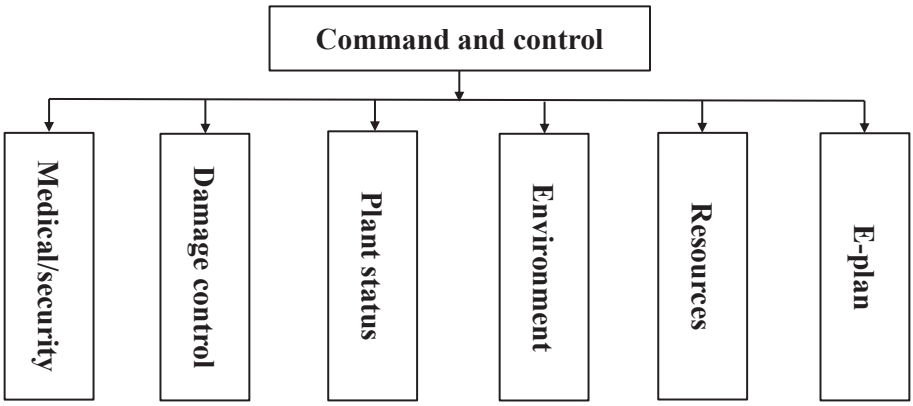



*FIG. IV–1. Overview of tasks in a site disruptive accident.*

(c) The ERO needs to initiate actions to stabilize the plant. These are shutdown of the reactor and starting decay heat removal functions. Actions may be done locally or manually, according to pre-established procedures, for example:
   — For a pressurized water reactor (PWR), this includes starting the turbine driven auxiliary feedwater pump locally and manually;
   — For a boiling water reactor (BWR), this includes starting the reactor core isolation cooling system locally and manually. This may include the need for emergency lighting, dosimeters, protective clothing, ladders and other equipment. In addition, a number of other actions are needed (see Section IV–3).

(d) The ERO needs to monitor and mitigate releases and make sure working areas are habitable. Where needed, doses are to be estimated. If required, sprays can be used to scrub fission products. The ERO needs to make sure spent fuel is, and remains, submerged.

(e) The ERO has to establish the needed resources for the actions under (c). This may include AC and DC power, air (pneumatic devices) and fuel for emergency diesel generators. Load shedding may be one strategy to extend battery life. Diesel generators may be started manually and, if no cooling is available, run with intervals. The required water tanks need to be filled (e.g. for the fire extinguishing system). There needs to be sufficient site personnel available at all times. Finally, the ERO has to initiate the plant emergency plan, including radiological assessments. Actions may include evacuation of relevant rooms, including the control room.

Focus now shifts to the actions under restoring command and control and on the actions to maintain plant safety, as indicated briefly under item (c). The first group of actions calls for surviving staff to assemble at some predefined location and restore a command and control structure, with the 'best' people they have (e.g. a senior reactor operator as the leader of the ERO, until a more qualified person is able to take over command). They then take action, for example, to control again the site, limit damage (e.g. firefighting), take care of wounded, check condition of key SSCs, such as reactor, containment, emergency core cooling systems and support systems (AC, DC, water and air) and execute the emergency plan. If not enough of such people are available, then an ERO may be established on the site with the help of a neighbouring nuclear power plant. The (new) ERO then initiates the second group of actions.

The second group of actions consists mainly of all types of manual and local action using, where needed, mobile equipment. It consists of major functions and the associated strategies to fulfil these functions (see Table IV–1).

TABLE IV–1. BASIC SAFETY FUNCTIONS AND MITIGATION STRATEGIES IN A SITE DISRUPTIVE ACCIDENT

| | Boiling water reactor | Pressurized water reactor |
|---|---|---|
| Safety functions | Reactor pressure vessel level control | Reactor coolant system inventory control |
| | Reactor coolant system heat removal | Reactor coolant system heat removal |
| | Containment isolation | Containment isolation |
| | Containment integrity | Containment integrity |
| | Release mitigation | Release mitigation |

TABLE IV–1. BASIC SAFETY FUNCTIONS AND MITIGATION STRATEGIES IN A SITE DISRUPTIVE ACCIDENT (cont.)

| | Boiling water reactor | Pressurized water reactor |
|---|---|---|
| | Manual operation of reactor core isolation cooling or isolation condenser | Make-up to reactor water storage tank |
| | DC power supplies to allow depressurization of reactor pressure vessel and injection with portable pump | Manually depressurize steam generators to reduce inventory loss |
| | Utilize feedwater and condensate | Manual operation of turbine (or diesel) driven auxiliary feedwater pump |
| Mitigation strategies | Make-up to hot well | Manually depressurize steam generators and use portable pumps |
| | Make-up to condensate storage tank | Make-up to condensate storage tank or alternate feedwater source |
| | Procedure to isolate the reactor water cleanup system | |
| | Manually open containment vent lines | |
| | Inject water into the dry well | |
| | Portable sprays | Portable sprays |

Whatever system available to provide cooling water is used, this will include the fire water system, if still available, or using portable pumps, stored elsewhere on the site. Essential initiating actions are the reactor trip and starting either the reactor core isolation cooling/isolation condenser (BWR) or the turbine driven auxiliary feedwater pump (PWR).

The portable equipment is stored in separate warehouses on the site but remote from the nuclear power plant structures and is assumed to remain available. Examples of such equipment are given in Ref. [IV–2].

For manual and local actions, information is required on whether access to the components concerned exists. This involves, for example, emergency lighting, dosimeters, protective clothing, portable batteries, calibrators if only voltage reading is possible, ladders and other equipment.

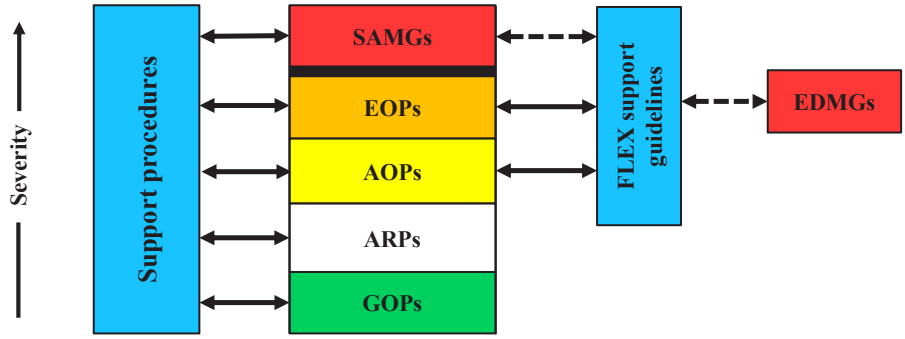
Emergency procedures and SAMGs are normally developed under the assumption of normal control or emergency shutdown facilities and that staff are available. On the other hand, the EDMGs can also be executed only if limited staff are available, as described. The EDMGs described are for at-power states only.

## IV–3. PORTABLE EQUIPMENT TO STRENGTHEN ACCIDENT MANAGEMENT

In the light of the Fukushima Daiichi accident, it became clear that additional, portable equipment could have played a major role in mitigating the consequences. In many countries, such additional equipment has now been installed. In the United States of America, this is called diverse and flexible coping strategies (FLEX). The approach basically consists of three steps [IV–3]:

(1) To make sure best use is made of existing in-plant equipment, strengthened where needed;
(2) To install portable equipment on-site and, in addition, the means to transport it to the plant and connect it;
(3) To have portable equipment available off-site, plus a transport means — usually by air — to the stricken site and ways to connect it; this includes off-site organizational matters.

The approach assumes that command and control is available. Therefore, this equipment is meant to be in addition to emergency procedures and SAMGs, with a focus on mitigating extended loss of AC power and loss of ultimate heat sink. The role and place of FLEX and EDMGs are shown in Fig. IV–2. The dashed line means that FLEX has so far not been designed to support SAMGs, and EDMGs have not been designed as part of the FLEX approach. At present, some Member States are making an effort to integrate FLEX and EDMG equipment and procedures, including SAMGs. Currently, FLEX may be used for SAMGs, although it has not been designed for that function. Vice versa, EDMG strategies can enhance safety functions by local and manual actions. In principle, however, local and manual actions are already part of the emergency operating procedures (EOPs) and SAMGs or, alternatively, in the FLEX support guidelines.




**Note:** AOPs — abnormal operating procedures; ARPs — alarm recovery procedures; EDMGs — extensive damage mitigation guidelines; EOPs — emergency operating procedures; GOPs — general operating procedures; SAMGs — severe accident management guidelines.

*FIG. IV–2. Overview of procedures to mitigate large scale events and accidents (adapted from Ref. [IV–3] with permission).*

A limitation is that both EOPs and SAMGs have been developed mostly on the basis of scenarios evolving from internal events. For example, many SAMGs see a challenge to the containment integrity as a late challenge and, hence, they have shaped the guidance accordingly. In an extreme external event, fission product boundaries (containment) may have been damaged already at the beginning, which may alter the priorities in SAMGs.

Table IV–2 provides an overview of the key functions in a PWR and how they can be supported by FLEX equipment.

## REFERENCES

[IV–1] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Action Plan on Nuclear Safety (2011), http://www.iaea.org/sites/default/files/actionplanns.pdf

[IV–2] NUCLEAR ENERGY INSTITUTE, B.5.b Phase 2 & 3 Submittal Guideline, NEI 06-12, Rev. 2, NEI, Washington, DC (2006).

[IV–3] NUCLEAR ENERGY INSTITUTE, Diverse and Flexible Coping Strategies (FLEX) Implementation Guide, NEI 12-06, Rev. 0, NEI, Washington, DC (2012).

TABLE IV–2. PWR FLEX BASELINE CAPABILITY SUMMARY

| | Safety function | Method | Baseline capability |
|---|---|---|---|
| Core cooling | Reactor core cooling and heat removal (steam generators available) | Auxiliary/emergency feedwater<br>Depressurize steam generator for make-up with portable injection source<br>Sustained source of water | Use of installed equipment for initial coping<br>Connection for portable pump to feed required steam generators<br>Use of alternate water supply to support core heat removal |
| | Reactor coolant system inventory control and core heat removal (shutdown modes with steam generators not available) | Low leak reactor coolant pump seals and/or reactor coolant system high pressure make-up<br>All plants provide means to provide borated reactor coolant system make-up | Low leak reactor coolant pump seals and/or providing on-site high pressure reactor coolant system make-up capability<br>Diverse make-up connections to reactor coolant system for long term make-up and shutdown mode heat removal<br>Source of borated water<br>Letdown path if required |
| | Key reactor parameters | Steam generator level<br>Steam generator pressure<br>Reactor coolant system pressure<br>Reactor coolant system temperature | (Re-)powered instruments |
| Containment | Containment pressure control and heat removal | Containment spray | Connection point on containment spray header for use with portable pump or alternate capability or analysis demonstrating that containment pressure control is not challenged (e.g. MAAP analysis) |
| | Containment integrity (ice condenser containments only) | Hydrogen igniters | Re-powering of hydrogen igniters with a portable power supply. |
| | Key containment parameters | Containment pressure | (Re-)powered instruments consistent |
| Spent fuel pool cooling | Spent fuel cooling | Make-up with portable injection source | Make-up via hoses direct to pool<br>Make-up via connection to spent fuel pool make-up piping or other suitable means<br>Spray via portable nozzles |
| | Spent fuel pool parameters | Spent fuel pool level | Reliable spent fuel pool instrumentation |

**Source:** Table 3-2 of Ref. [IV–3].

# ABBREVIATIONS

| | |
|---|---|
| AC | alternating current |
| BWR | boiling water reactor |
| CCDP | conditional core damage probability |
| DC | direct current |
| DEE | design extension external event |
| EDMGs | extensive damage mitigation guidelines |
| EMEG | emergency management equipment guidance |
| EOPs | emergency operating procedures |
| ERO | emergency response organization |
| FLEX | diverse and flexible coping strategies |
| HCLPF | high confidence of low probability of failure |
| LOCA | loss of coolant accident |
| PSA | probabilistic safety assessment |
| PWR | pressurized water reactor |
| SAMGs | severe accident management guidelines |
| SEL | selected equipment list |
| SF | split fraction |
| SRV | safety relief valve |
| SSCs | structures, systems and components |

# CONTRIBUTORS TO DRAFTING AND REVIEW

| | |
|---|---|
| Altinyollar, A. | International Atomic Energy Agency |
| Basu, P. | International Atomic Energy Agency |
| Beltran, F. | International Atomic Energy Agency |
| Blahoianu, A. | Canadian Nuclear Safety Commission, Canada |
| Henkel, F.-O. | Wölfel Beratende Ingenieure, Germany |
| Iqbal, J. | Pakistan Atomic Energy Commission, Pakistan |
| Johnson, J.J. | James J. Johnson & Associates, United States of America |
| Kennedy, R.P. | RPK Structural Mechanics Consulting, United States of America |
| Kluegel, J.-U. | Kernkraftwerk Gösgen-Däniken, Switzerland |
| Markovic, D. | Electricité de France, France |
| Morita, S. | International Atomic Energy Agency |
| Orbovic, N. | Canadian Nuclear Safety Commission, Canada |
| Pino, G. | ITER Consult, Italy |
| Pisharady, A. | Atomic Energy Regulatory Board, India |
| Rangelow, P. | AREVA, Germany |
| Ravindra, M.K. | M.K. Ravindra Consulting, United States of America |
| Ricciuti, R. | CANDU Energy, Canada |
| Saarenheimo, A. | VTT Technical Research Centre, Finland |
| Samaddar, S.K. | International Atomic Energy Agency |
| Välikangas, P. | Radiation and Nuclear Safety Authority, Finland |
| Varpasuo, P. | Fortum Nuclear Services, Finland |
| Vayssier, G. | Nuclear Safety Consultancy (NSC) Netherlands, Netherlands |

**Consultants Meetings**

Ottawa, Canada: 28–29 March 2011; 10–14 September 2012
Vienna, Austria: 4–7 October 2011; 12–14 November 2012; 17–21 December 2012;
31 January – 1 February 2013; 11–15 November 2013

IAEA
International Atomic Energy Agency

No. 24

# 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.

## BELGIUM

***Jean de Lannoy***
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

## 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: http://www.renoufbooks.com

***Bernan Associates***
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

## 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: http://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: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

***Lavoisier SAS***
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

***L'Appel du livre***
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 43 43 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

## 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: http://www.goethebuch.de

## HUNGARY

***Librotrade Ltd., Book Import***
Pesti ut 237. 1173 Budapest, HUNGARY
Telephone: +36 1 254-0-269 • Fax: +36 1 254-0-274
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

## 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: http://www.alliedpublishers.com

***Bookwell***
3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: http://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: http://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: http://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: http://www.secnrs.ru

## UNITED STATES OF AMERICA

***Bernan Associates***
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

***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: http://www.renoufbooks.com

**Orders for both priced and unpriced publications may be addressed directly to:**

IAEA Publishing Section, 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
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

**EXTERNAL EVENTS EXCLUDING EARTHQUAKES IN THE DESIGN OF NUCLEAR POWER PLANTS**
IAEA Safety Standards Series No. NS-G-1.5
STI/PUB/1159 (105 pp.; 2003)
ISBN 92–0–101099–0 Price: €27.00

**EXTERNAL HUMAN INDUCED EVENTS IN SITE EVALUATION FOR NUCLEAR POWER PLANTS**
IAEA Safety Standards Series No. NS-G-3.1
STI/PUB/1126 (49 pp.; 2002)
ISBN 92–0–111202–5 Price: €14.50

**SAFETY ASPECTS OF NUCLEAR POWER PLANTS IN HUMAN INDUCED EXTERNAL EVENTS: GENERAL CONSIDERATIONS**
Safety Reports Series No. 86
STI/PUB/1721 (88 pp.; 2017)
ISBN 978–92–0–111015–2 Price: €41.00

This publication provides detailed methodology and procedures for assessing the safety margins of nuclear power plants against human induced external events of either the postulated type or accidental type. The hazards covered in this publication are explosions, aircraft crashes and fires. It addresses the different tasks of margin assessment, such as: accident sequence analysis; systems analysis; in-plant evaluations; capacity evaluation of structures, systems and components; and margin assessment (deterministic and probabilistic method) of the systems and plant.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–111415–0
ISSN 1020–6450