IAEA TECDOC SERIES

IAEA-TECDOC-1804

IAEA-TECDOC-1804

Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants

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.

ATTRIBUTES OF FULL SCOPE LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT (PSA) FOR APPLICATIONS IN NUCLEAR POWER PLANTS

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

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

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

IAEA-TECDOC-1804

ATTRIBUTES OF FULL SCOPE LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT (PSA) FOR APPLICATIONS IN NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

COPYRIGHT NOTICE

For further information on this publication, please contact:

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

Printed by the IAEA in Austria
October 2016

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Attributes of full scope level 1 Probabilistic Safety Assessment (PSA) for applications in nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2016. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1804 | Includes bibliographical references.
Identifiers: IAEAL 16-01062 | ISBN 978–92–0–107316–7 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Safety measures. | Nuclear power plants — Risk assessment. | System safety. .

FOREWORD

Probabilistic safety assessment (PSA) of nuclear power plants complements the deterministic safety analysis and is widely recognized as a comprehensive and structured analytical approach to identifying accident scenarios and deriving numerical estimates of risks of undesirable consequences concerning nuclear power plant operation and associated plant vulnerabilities. Recently, PSA has been more broadly applied to support numerous applications and risk informed decisions on various design related, operational and regulatory issues. The expanded use of PSA in the integrated risk informed decision making process requires that the PSA possess certain features to ensure its technical consistency and quality.

This publication aims to further promote the use and application of PSA in Member States by providing a comprehensive list of PSA applications and describing what technical features (termed ‘attributes’) of a PSA need to be satisfied to reliably support the PSA applications of interest. Consideration has also been given to the basic set of attributes characterizing a ‘base case PSA’ that is performed to assess overall plant safety.

The present publication can support PSA practitioners in appropriate planning of a PSA project taking into account possible uses of the PSA in the future. It can also be used by reviewers as an aid in assessing the quality of PSAs and judging the adequacy of a PSA for particular applications.

This publication supersedes IAEA-TECDOC-1511, Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants (published in 2006), which provided detailed information on technical features of a restricted scope PSA aimed at analysing only internal initiating events caused by random component failures and human errors, and accident sequences that may lead to reactor core damage during operation. The present publication extends the scope of the PSA to cover a broader range of internal and external hazards, and low power and shutdown modes of nuclear power plant operation. In addition, some PSA aspects relevant to lessons learned from the accident at the Fukushima Daiichi nuclear power plant are also considered.

The IAEA officers responsible for this publication were A. Lyubarskiy, I. Kuzmina and O. Coman of the Division of Nuclear Installation Safety.

ACKNOWLEDGEMENTS

The IAEA would like to thank the many PSA experts who participated in the consultants and technical meetings for their valuable contributions to this publication, and in particular P. Amico of Jensen Hughes (United States of America), P. Berg of the Federal Office for Radiation Protection (BfS) (Germany), K. Fleming of KNF Consulting Services LLC (United States of America), D. Henneke of GE-Hitachi (United States of America), J. Preston (United Kingdom), M. Ravindra of M.K. Ravindra Consulting (United States of America), T. Szikszai of Ri-Man Consulting (Hungary), M. Szoke of EdF-Energy (United Kingdom) and G. Tokmachev of Atomenergoproject (Russian Federation).

EDITORIAL NOTE

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

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

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

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

The 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

Increasingly, during the last years probabilistic safety assessment (PSA) of nuclear power plants (NPPs) has been broadly applied to support numerous applications, such as risk informed changes to technical specifications, risk based plant configuration control, maintenance programme optimization, etc. INSAG-25 "Framework for an integrated risk informed decision making" [1] suggests that PSA is one of several key elements of the integrated risk informed decision making (IRIDM) framework; however in order to be used effectively to support decision making, PSA has to be of sufficient scope, level of detail, and technical quality.

The IAEA-TECDOC-1511 "Determining the quality of PSA for applications in nuclear power plants" was published in 2006 with the objectives to establish an approach and detailed guidance for achieving the level of technical quality of PSA needed to support various PSA applications. The publication provided information regarding the technical features (termed 'attributes') of major PSA elements (initiating events analysis, accident sequences analysis, human reliability analysis, etc.) that are appropriate for carrying out various applications, including a 'base case PSA' that is performed with the purpose of assessing the overall plant safety. That publication took into consideration the contemporary worldwide good practice and experience in the area of PSA technical quality assessment and verification, and in particular the publication developed by American Society of Mechanical Engineers (ASME) 'Standard for Probabilistic Risk Assessment (PRA) for Nuclear Power Plant Applications' [2]. The starting point for the development of the technical attributes presented in IAEA-TECDOC-1511 was the set of requirements falling in PSA Capability Category II of the ASME PRA Standard (Capability Category II requirements are representative of currently accepted good industry practices in the USA as well as in other countries). IAEA-TECDOC-1511, while providing sufficient details for assuring technical quality for internal initiating events PSA for NPP full power operation, does not cover all potential hazards that can pose risk to a plant or plant operating states other than the full power state.

In 2010 the IAEA published two Safety Guides: SSG-3 "Development and application of Level 1 probabilistic safety assessment for nuclear power plants" [3] and SSG-4 "Development and application of Level 2 probabilistic safety assessment for nuclear power plants" [4]. These Safety Guides provide a comprehensive, but still high level, set of recommendations on specific features of Level 1 and Level 2 PSA for all types of initiating events and hazards and operating conditions. The Safety Guides were not aimed at providing detailed information on state-of-the-art features of PSA in the view of various PSA applications.

Member States requested the IAEA to develop an extension of IAEA-TECDOC-1511 to cover the full range of internal and external hazards and plant operational modes.

This publication is the output of the three year development, which resulted in extension of IAEA-TECDOC-1511 to cover the full scope PSA as defined in SSG-3 [3] (all internal and external hazards and all operating modes). In this publication, which is also the revision of IAEA-TECDOC-1511, a check for consistency with the IAEA Safety Guides on PSA [3, 4] has been performed and associated modifications have been introduced to remove discrepancies when needed. It was the intention to transfer the format and contents of IAEA-TECDOC-1511 to this publication unchanged where the information contained therein is still applicable.

The extended PSA scope has resulted in adding two new technical PSA elements; Plant Operational States Analysis (OS) and Hazard Events Analysis (HE). The new PSA elements are defined further in the respective sections. In addition, a number of changes have been made to the attributes of the other PSA elements in order to accommodate the enlarged PSA scope.

Therefore, this publication updates the IAEA TECDOC-1511 "Determining the Quality of Probabilistic Safety Assessment for Applications in Nuclear Power Plants", published in 2006.

It is important to mention that in the development process, the latest developments in the area of PSA technical quality assessment and verification have been taken into account and in particular various ASME/ANS PRA Standards available at the time of publication [5]-[8].

Yet, in particular the Fukushima Daiichi accident highlighted the need for a more comprehensive human reliability analysis (HRA) systematically considering and assessing human behaviour in the dynamic interaction with the working environment during the incidental evolution of the respective event sequences – also taking into consideration organizational and contextual factors, plant specific and sequence depending boundary conditions, such as harsh environmental conditions. These considerations are not discussed in the available IAEA safety report on HRA [9] and are not reflected in this publication because they require further elaboration. The IAEA is planning to develop a guidance publication on HRA that will consider recent and advanced methods and approaches. The attributes in Section 10 (on HRA) of this publication will be updated after the new publication on HRA is published.

1.2. OBJECTIVES

Various applications of PSA, including integrated risk informed decision making, require that PSAs used to support those applications have certain characteristics in terms of their scope, degree of detail, technical adequacy of the modelling, capability and flexibility to perform the required calculations, capability to support interpretation of the results, quality and type of the data used, and assumptions made in modelling important aspects. The features of a PSA that are necessary to support specific applications vary with the application. This report provides information regarding these features, written in the form of attributes of the major PSA elements, which are appropriate for carrying out various PSA applications. In so doing, this publication provides a basis for judging the technical quality of the PSA used to support an application as discussed in the next section.

The notion of ‘PSA technical quality’ refers to the technical adequacy of the methods, level of detail and data used to develop the PSA model. In order to assure that the chosen methods and data are used, applied, and documented in an adequate and controlled manner, a dedicated PSA maintenance and upgrade process needs to be established that also addresses applications of PSA. How to set up and effectively apply such a process for achieving quality in general for NPP safety is described in [10] and for the PSA in [11].

As distinct from these publications, the present TECDOC focuses on the technical information regarding approaches, methodology and data to obtain appropriate technical PSA features for specific applications. In addition, the attributes of a PSA maintenance and upgrade process that will successfully achieve and maintain technical quality in support of PSA applications is presented in Chapter 15 of this publication.

Thus, the approach provided in the publication can be used as a basis to formulate a technical framework for carrying out a specific PSA application or applications. For these reasons this publication concentrates on technical PSA aspects. In Figure 1 the overall framework for the assurance of the technical quality of PSA capable to support applications is shown identifying the roles of the existing IAEA publications and the present publication.

It is expected also that the publication will provide a technical framework for PSA-related activities and to support the independent PSA reviews conducted by the IAEA in the framework of the Technical Safety Review (TSR) service. The TSR service replaces the former International Probabilistic Safety Assessment Review Team (IPSART) service [12] conducted by the IAEA at request of Member States. The guidelines for TSR service is under development.

1.3. TECHNICAL QUALITY OF A PSA FOR AN APPLICATION

For the purposes of this publication the following is defined: ***“In the context of an application, the PSA is of an appropriate technical quality if it conforms to a set of attributes that are appropriate for the application.”***

The key to defining technical quality is thus in the definition of the attributes. The attributes that are required for a particular application depend on the purpose and characteristics of the application. When used as an input to a decision, the attributes required are a function of the process for decision making, and in particular address the acceptance criteria or guidelines against which the PSA results are to be compared. The acceptance criteria are generally in the form of a numerical value associated with a specific risk metric. Examples of metrics are the absolute value of, or increase in, core/fuel damage frequency, and importance measures.

The metrics commonly used are defined in Appendix I to this publication. The PSA has to be capable of evaluating the appropriate metrics for each application for performing the comparison of the results of the PSA with the criterion and this also impacts the required attributes for the PSA. For example, the criterion may require use of the full characterization of uncertainty as a probability distribution on the value of the metric instead of a mean value. This will be an additional attribute for the PSA application.

Two types of attributes are defined in this publication:

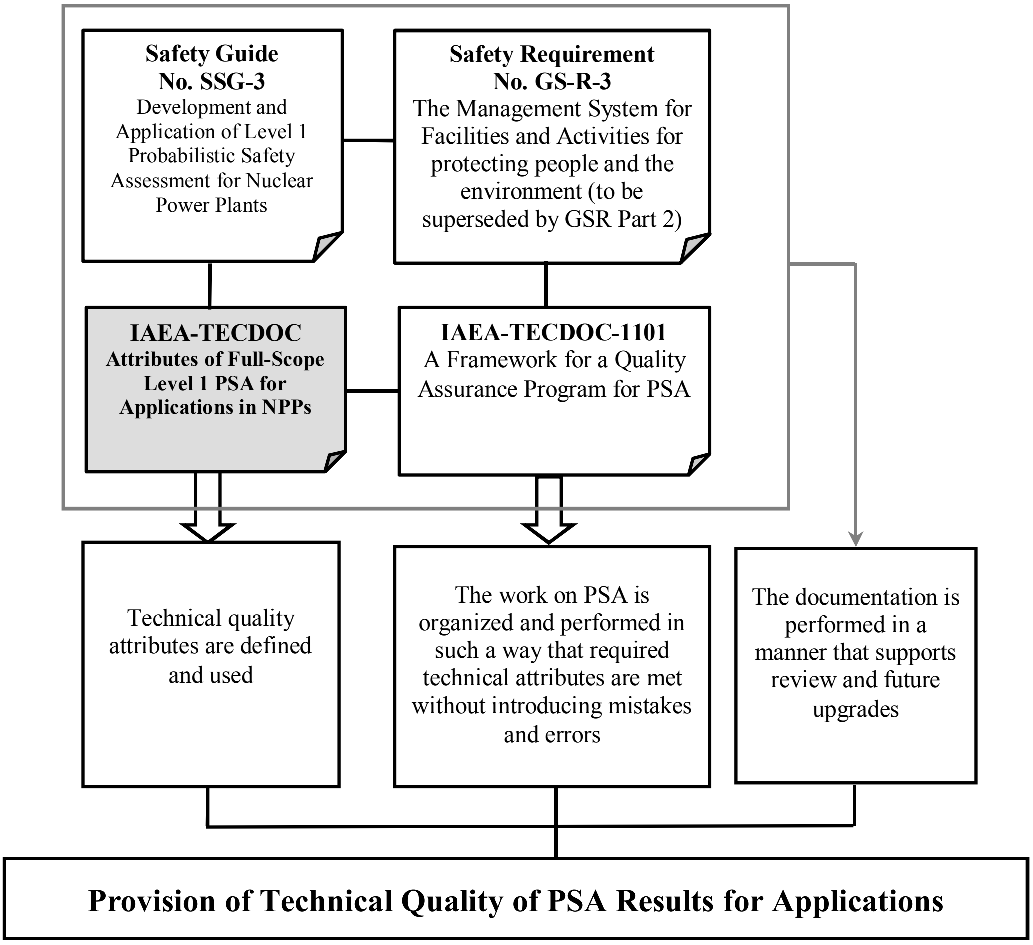
Safety Guide
No. SSG-3
Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants
Safety Requirement
No. GS-R-3
The Management System for Facilities and Activities for protecting people and the environment (to be superseded by GSR Part 2)
IAEA-TECDOC
Attributes of Full-Scope Level 1 PSA for Applications in NPPs
IAEA-TECDOC-1101
A Framework for a Quality Assurance Program for PSA
Technical quality attributes are defined and used
The work on PSA is organized and performed in such a way that required technical attributes are met without introducing mistakes and errors
The documentation is performed in a manner that supports review and future upgrades
Provision of Technical Quality of PSA Results for Applications

Fig. 1. Framework of PSA technical quality and supporting IAEA publications.

- ***General attributes,*** which apply for a typical 'base case PSA' (for the definition of a 'base case PSA' see the discussion below). The general attributes apply for all PSAs and applications.
- ***Special attributes***, which generally provide enhanced capabilities supporting certain applications of a PSA. Special attributes may not be met in a 'base case PSA'.

The purpose of a 'base case PSA' is the assessment of the overall plant safety as described for example in Section 2 and Appendix II of this publication.

Thus, the set of general attributes describing the technical features of a 'base case PSA' in this publication corresponds to the PSA application 'Assessment of the overall plant safety'.

The general attributes represent a fundamental set of attributes that can be recognized as being associated with the performance of a technically correct PSA in accordance with the present state of the art methodology and technology. According to [12], "the current state of the art of PSA is defined by the way PSAs have been practically performed in recent years by Member States according to existing guidelines and using accepted methodologies and techniques." To summarize, it is understood in this publication that the general attributes represent a minimum set of the attributes needed to perform a state of the art PSA with the aim to assess the overall plant safety. State of the art is taken to be synonymous with generally accepted best practice.

Special attributes provide elevated capabilities in terms of resolution, specificity, scope, realism, and less uncertainty for aspects of the PSA needed to support specific applications, but still corresponding to the current state of the art. It is assumed that when the special attributes are met, the corresponding general attributes are also met. Different PSA applications may require different special attributes. Some applications may not require any special attributes; the general attributes may be sufficient.

Special attributes may arise because of the need to model specific impacts of changes proposed by the application, which may require a higher level of detail for certain elements than required for the base case as defined in this publication. In addition, special attributes may be required to address unique acceptance criteria for the application.

It is expected that in order to be able to support various applications, the PSA has to address all general attributes. On the other hand, there might be applications for which not all the attributes would need to be met, or for which some attributes can be relaxed. These are applications, for which either the risk information required is limited, or for which the approach to decision making compensates for a lesser level of detail or plant specific fidelity in the PSA by making a more conservative decision than would be the case for the more detailed, plant specific model. An example of the latter is an application that addresses relaxation of requirements on components considered to be of low safety significance. Use of a more detailed, less conservative and more plant specific PSA[1] would allow more components to be classified as low safety significant, when compared with what would result from use of a less detailed model. However, even in this case, the PSA used to support that application must be technically adequate.

For many applications, the acceptance criteria may require the consideration of all contributors to risk. It is recognized that specialized PSA methods and expertise are needed to perform the assessment of risk resulting from internal hazards, such as internal fires and floods, or external hazards, such as earthquakes, high winds, etc., and from different plant operating states, such as low power and shutdown modes. The comprehensive set of attributes for all foreseeable hazards and operational modes provided in this publication may support selection of suitable methods and tools.

Which attributes are present determines to some extent the role the PSA can play in the integrated risk informed decision making process. When it is clear that the confidence in the accuracy of the PSA results is high, the PSA can play a significant role. When confidence in the accuracy is less, it must play a lesser role. However, in either case, the PSA still has to have a technical quality commensurate with its role. What makes the distinction between these cases is that those attributes that enhance realism are not necessary met in the latter case.

[1] E.g. plant specific component reliability data or success criteria analyses are used rather than generic.

When using information presented in this publication, it is proposed that in case a PSA analyst considers that an application does not necessarily require compliance with a general or special attribute or attributes, this need to be reliably justified in terms of the analysis consistency and absence of impact of a missing attribute(s) on PSA results and insights used for decision making.

1.4. SCOPE

The IAEA PSA guides and procedures [3, 4, 9, 13-15] mainly concentrate on general features and content of PSAs. In these publications, a limited consideration is given to the particular features of PSA conditioned by specific PSA applications.

Safety Guide SSG-3 [3] published in 2010 does provide recommendations to the features of the state of the art PSA; however, these recommendations are mainly directed to the approach to be used during PSA development and application and they are less focused on the detailed technical features that can assure PSA technical adequacy for particular applications. Therefore this TECDOC is aimed at providing attributes that are consistent with the recommendations given in [3], but with deeper technical details both for the base case PSA and for the PSAs to be used for particular applications.

Some attributes in this TECDOC go beyond the current state of the art reflected in [3] due to the fact that a number of approaches and techniques described in [3] have been further developed following lessons learned from Fukushima Daiichi accident, so the present publication takes into account the current state of the art regarding various aspects related to PSA methodologies. In particular, this may be especially applicable to special attributes added in order to support the assessment of certain risk contributions for which PSA methodology currently is not sufficiently mature. Since this publication is expected to be used as a reference for PSA technical quality in the foreseeable future and it is believed that specific technical solutions will be found to address those attributes, it is deemed appropriate to include them.

Due to the comprehensive amount of information covered, the scope of this publication is restricted to a Level 1 PSA for all types of hazards (internal IEs, internal and external hazards) and all operating modes, including shutdown PSA. Level 2 and 3 PSAs are outside of the scope of this publication.

In addition, consideration is not given to sources of radioactivity other than the reactor core, although many of the principles in this publication are applicable to other sources (e.g. spent fuel pool). However, some applications may require that the scope of the PSA be complete in terms of consideration of risks other than core/fuel damage.

In those cases where an application will benefit from information obtained from a Level 2 PSA or Level 3 PSA, other IAEA publications [4, 13, 14] need to be consulted in order to verify that the technical quality of Level 2 or Level 3 PSA is sufficient to allow the use of the results of these analyses in a decision making process.

It is not the intent of this publication to address what has to be done to compensate for the limited scope of a PSA. Nor does this publication attempt to describe what has to be done to compensate for attributes that are not met. These considerations are left to the decision makers. However, Appendix II provides a general discussion regarding what PSA scope and risk metrics may be needed for specific applications.

The general attributes of a 'base case PSA' form a basis for other considerations relating to specific PSA applications. The publication concentrates also on describing the appropriate features and attributes of PSA and of PSA elements and relates them to specific applications by indicating additional features and characteristics important from the viewpoint of specific applications. Only a summary of PSA approaches, techniques, and tasks is given. The publication provides information on what has to be done rather than how it should be done. Thus, regarding detailed procedures for PSA tasks, reference is made to the appropriate available PSA procedures and the publication is not intended to replace them.

In general, terminology as specified by the IAEA Safety Glossary [16] was used in this publication; however for some specific PSA related terminology, terms and reference as specified in the associated sections of this report are used.

1.5. STRUCTURE

Due to the fact that this publication is oriented towards supporting applications of PSA, first, an overview of current applications is given in Section 2. Then Section 3 introduces the scope of PSAs, main PSA elements, and provides a description of the process one should follow to determine whether the PSA is of an appropriate technical quality for an application of interest.

The attributes of the PSA elements are provided in Sections 4 through 14 separately for each PSA element, covering both general attributes (applicable for the 'base case PSA'), and application-specific ones (i.e. special attributes). Section 15 provides attributes for maintenance and upgrade of the PSA. Section 16 discusses special attributes appropriate for PSA applications and outlines a practical procedure for determination of the special attributes relevant for the application of interest. It also provides a table mapping the special attributes to the PSA applications. Conclusions are provided in Section 17.

Appendix I provides definitions of the risk metrics referred to in the publication.

Appendix II provides summary information on PSA applications, including their general description, applicable risk metrics, remarks on the use of PSA models to support specific applications, and examples.

1.6. APPLICABILITY

There are three major limitations regarding the applicability of this publication, which are as follows:

1. The information presented is directed towards PSA and PSA applications for nuclear power plants. Thus, this publication is not directly applicable for research reactors and other facilities.

2. The publication focuses on PSA and PSA attributes for vessel type light water reactors (LWRs), although the vast majority of general and special attributes are applicable for other reactor types as well. The applicability of the PSA element descriptions and of PSA attributes given in this publication for nuclear power plants of other reactor types is discussed below. The publication mainly addresses PSA performed on single reactor plants; not all aspects applicable to the PSA for sites with multiple reactor units are covered.

3. The publication is focused on PSA approaches, modelling and data for a typical 'mature' nuclear power plant, which has been in operation for a number of years without major changes in the plant. The applicability of the PSA elements descriptions and of PSA attributes given in this publication for nuclear power plants in other stages of the plants life time is discussed below.

1.6.1. Applicability for reactors other than vessel type LWRs

The present predominant reactor types for NPPs are vessel type LWRs. PSA approaches and techniques have therefore been mostly developed and applied for this kind of NPPs. For this reason the publication focuses on PSA and PSA attributes for vessel type pressurized LWRs. Most of the PSA approaches and techniques can also be applied and used for other reactor types such as gas cooled reactors, CANDU, RBMK (i.e. data analysis, human reliability analysis, systems analysis, etc.). Therefore, the attributes described in this publication apply as well for these reactor types. There is however one area regarding PSA approaches and techniques where there is a significant difference.

The concept of core/fuel damage as an accident sequence end state for Level 1 PSA and as a rough measure for consequences is a useful concept for vessel type LWRs.

The physical background for this concept is that for the compact cores of current vessel type LWRs once there is loss of cooling to substantial portions of the core and associated fuel damage it is likely that the whole core is affected and a substantial part of the fission product inventory is released from the fuel.

For reactors with physically well separated fuel channels and comparatively large cores, damage might be restricted to individual fuel channels, small portions of the core, or parts of the core. Accordingly, several Level 1 fuel or core/fuel damage end states have been defined and used in PSAs for such reactors to reflect the significantly different fractions of the fuel or core affected during different accident scenarios. The physical reason for this distinction and refinement of core/fuel damage are specific features of the reactor and system design, e.g. the design of coolant piping and the connection of emergency core cooling system (ECCS) trains to the coolant piping.

The refined definition of core/fuel damage then allows obtaining a useful consequence measure in terms of the Level 1 PSA by distinguishing scenarios with significant consequences from those with low consequences but elevated frequencies. In turn such definition of core/fuel damage categories requires interpretation and adaptation regarding the description of PSA tasks and associated attributes as given in this publication.

For certain plant designs the concept of core/fuel damage is not applicable (e.g. reactors with a homogeneous core or high temperature gas cooled reactors - HTGR). However, the Level 1 PSA methodology is fully applicable for these designs if the term core/fuel damage is replaced by a definition of "undesirable consequences" that is applicable to the specific reactor type. In addition it should be noted that analytical and in particular experimental information on details of the accident progression in the beyond design accident range is limited for other reactor types if compared to vessel type LWRs. This may also affect the formulation of safety function success criteria and delineation of accident sequences.

Therefore, accident progression and the characterization of Level 1 end states for reactor types other than vessel type LWRs is based on expert judgment rather than on realistic assessment and experimental justification.

1.6.2. Applicability for NPPs in different stages of the plant life time

In order to provide a comprehensive description of PSA tasks and associated attributes the publication is focused on PSA approaches, modelling aspects, and data for a typical 'mature' nuclear power plant, which typically has been in operation for a number of years without major changes to the plant.

It is recognized that significant differences exist regarding PSA approaches, modelling aspects, and data for different stages of the plants lifetime.

The reason why this publication concentrates on PSA for a 'mature' nuclear power plant is that only at this stage can the full range of PSA techniques be applied including evaluation and use of reliable information on the plant arrangement, cable tracing and piping locations as well as a reasonable amount of operational experience data from the plant itself. During the design stage of a plant, for example, detailed information on design and operational features might be limited and no operational experience data from the plant is available. For a completely new design even applicable experience data from comparable plants might not be available. A number of attributes formulated in this publication for a 'mature' NPP therefore require interpretation and adaptation when applied for an NPP in an earlier life stage.

PSA techniques can be used beginning at an early design stage of a plant. At this time even the conceptual design of engineered safety features (ESFs) might not be entirely fixed, e.g. the number of redundant trains in an ECCS. Diverse ECCSs might be under consideration for a particular emergency core cooling function. In these situations, PSA techniques can be used to support conceptual decisions. However, there are major differences in PSA approaches, techniques and data as listed below:

- Detailed design information on systems and their support systems might not or only partially be available. This missing information can be bridged by related assumptions for PSA purposes.
- Detailed operating procedures are not available. Information from similar NPPs

might be used instead.

- No or only generic operational experience is available. Information from similar NPPs might be used instead.
- Information on thermal hydraulic analyses, accident progression, accident scenarios might be limited. Information from similar NPPs might be used instead.
- Completeness of initiating events is difficult to ascertain. Information from similar NPPs might be used instead, or a more comprehensive review for initiating events may be needed.
- Limited information on human machine interface (HMI) and on training of operating staff is available. Assumptions would need to be made, and verified as the design process is completed and plant operation occurs.
- Limited information on maintenance practices and procedures. Assumptions would need to be made, and verified as the design process is completed and plant operation occurs. Information from similar NPPs might be used instead.
- Equipment/cable/piping location information is limited or missing (important for internal hazards analysis, CCF modelling and modelling of secondary effects). Assumptions would need to be made, and verified as the design process is completed and plant operation occurs.
- Details on technical specifications (TSs) are missing or limited. Assumptions would need to be made, and verified as the design process is completed and plant operation occurs. Information from similar NPPs might be used instead.

In summary, a considerable number of attributes that apply for a PSA for a ‘mature’ plant do not strictly apply for a plant in the design stage, simply because the required knowledge and data are not yet available. Accordingly, simplifications and assumptions need to be made to bridge the missing information. Furthermore, the applicability and adequacy of the assumptions themselves could be limited, introducing elements of variability and uncertainty even if not directly visible or stated. A typical example for a new NPP concept in an early design stage are the advanced reactors incorporating new concepts for safety features, e.g. passive systems, where even the assessment of thermal-hydraulics and consideration of reliability aspects are still under development and where operational experience is not available.

Uncertainty inherent in PSA models and results for a reactor in the design stage needs to be fully addressed if the PSA is used for decision making.

One way to deal with these uncertainties in the early stages of plant life is to use PSA in a relative way, e.g. by comparing different design variants using similar models and assumptions. Another useful approach is to check the robustness of results by changing the assumptions to see how the results are affected by such changes.

During the further development of the plant, increasing details on design and operational features of the plant become available. This progress is then usually reflected in refining PSA models, which in turn reduces associated variability and uncertainties.

Even for a ‘mature’ plant, there might be major backfits or major changes regarding the plants design and operational features. A major change in this sense would be a significant redesign of the core, including redesign of protection instrumentation and control (I&C) and of ESFs. This in turn would mean that the PSA would need to be redone because such a major change is likely to change the entire PSA model structure and because similar conditions would apply again for parts of the plant or for the entire plant as during the design stage, which has to be reflected in the PSA techniques and data.

2. OVERVIEW OF PSA APPLICATIONS

2.1. PSA APPLICATION CATEGORIZATION

Since the beginning of the 1990s, PSA techniques have been used increasingly widely in many countries in the risk informed decision making process in NPP design, operation, and licensing activities. IAEA-TECDOC-1200 [17], published in 2001, identified a number of PSA applications. In the current publication, some additional applications have been included, and the PSA applications have been categorized in the following way according to their purpose:

1. **Safety assessment:** to assess the overall safety of the plant and to develop an understanding of the main contributors to risk.
2. **Design stage:** to provide support for design improvements during the design and pre-operational state.
3. **NPP operation:** to provide support for day-to-day operation of the plant (not including permanent changes to design or operational practices).
4. **Permanent changes to the operating plant:** to assess the safety significance of proposed permanent changes to the plant systems, structures and components or administrative controls (e.g. operating procedures, the licensing basis) as an aid to decision making.
5. **Oversight activities:** to support plant performance monitoring and assessment (both regulatory and industry).
6. **Evaluation of safety issues:** to evaluate the significance of safety issues.

Several application groups can be defined under the six categories based on a more specific consideration of the purpose and subject of PSA applications. Table 2.1 provides a list of PSA application categories, groups within the categories, and specific applications within the groups.

2.2. PSA RESULTS AND METRICS USED IN DECISION MAKING

In order to use a PSA in the decision making process, it is necessary to define what results are needed, and define criteria these results may be compared with. In some cases, the results may be qualitative, but in most cases, the results are quantitative. In such cases, some parameters that can be calculated using the PSA model are defined, which are referred to as metrics. Such metrics are defined both for PSA on individual reactor plants as well as multiunit site PSAs.

Typically, used reactor based metrics are PSA importance measures (F-V, RAW, RRW), core damage frequency (CDF), large early release frequency (LERF), conditional core damage probability (CCDP), quantitative health objectives (QHO), etc. When considering fuel damage from other locations other than the core, the more generic terms such as fuel damage frequency (FDF), and conditional fuel damage frequency (CFDF) are used.

TABLE 2.1 PSA APPLICATIONS

Application Category	Application Group	Specific Application
1. SAFETY ASSESSMENT		1.1. Assessment of the overall plant safety 1.2. Periodic safety review 1.3. Analysis of the degree of defence in depth and safety margin against beyond design basis site hazards, including correlated site hazards
2. DESIGN STAGE		2.1. Application of PSA to support decisions made during the NPP design (plant under design) 2.2. Licensing of design 2.3. Optimization of protection against hazard events (e.g. fires, floods) and common cause failures, including consideration of correlated site hazards and hazard-induced fires and floods 2.4. Establishment of equipment reliability targets for manufacturers 2.5. Identification of R&D which are necessary to support the design 2.6. Development operator procedures and training programmes and support for Human Factors Engineering
3. NPP OPERATION	3.1. NPP maintenance	3.1.1. Maintenance programme optimization 3.1.2. Risk informed house keeping 3.1.3. Risk informed support for plant ageing management programme 3.1.4. Risk informed on-line maintenance 3.1.5. Plant outage management
	3.2. Accident mitigation and emergency planning	3.2.1. Development and improvement of the emergency operating procedures 3.2.2. Support for NPP accident management (severe accident prevention, severe accident mitigation) 3.2.3. Support for NPP emergency planning
	3.3. Personnel training	3.3.1. Improvement of operator training programme 3.3.2. Improvement of maintenance personnel training programme 3.3.3. Improvement of plant management training programme
	3.4. Risk based configuration control/ Risk monitors	3.4.1. Configuration planning (e.g. support for plant maintenance and test activities) 3.4.2. Real time configuration assessment and control (response to emerging conditions) 3.4.3. Exemptions to TS and justification for continued operation 3.4.4. Dynamic risk informed TS

Application Category	Application Group	Specific Application
4. PERMANENT CHANGES TO THE OPERATING PLANT	4.1. Plant changes	4.1.1. NPP upgrades, backfitting activities and plant modifications 4.1.2. Life time extension
	4.2. Technical specification changes	4.2.1. Determination and evaluation of changes to allowed outage time and changes to required TS actions 4.2.2. Risk informed optimization of TS
		4.2.3. Determination and evaluation of changes to surveillance test intervals 4.2.4. Risk informed surveillance programme 4.2.5. Risk informed in-service inspections (RI-ISI)
	4.3. Establishment of graded QA programme for SSC	4.3.1. Categorization of SSC for equipment risk significance evaluation 4.3.2. Evaluation of risk impact of changes to quality requirements
	4.4. Risk informed special site protection measures	4.4.1. Risk informed fire protection 4.4.2. Risk informed internal flood protection 4.4.3. Risk informed defence in depth for individual and correlated site hazards
5. OVERSIGHT ACTIVITIES	5.1. Performance monitoring	5.1.1. Planning and prioritization of inspection activities (regulatory and industry) 5.1.2. Long term risk based performance indicators 5.1.3. Short term risk based performance indicators
	5.2. Performance assessment	5.2.1. Assessment of inspection findings 5.2.2. Evaluation and rating of operational events
6. EVALUATION OF SAFETY ISSUES	6.1. Risk evaluation	6.1.1. Risk evaluation of corrective measures 6.1.2. Risk evaluation to identify and rank safety issues 6.1.3. Assessment of the safety importance of deviations between an existing plant design and updated/revised deterministic design rules or new information about the site hazards. 6.1.4. Assessment of the significant of overall site risk for multiunit accidents 6.1.5. Assessment of the significant of overall site risk from all radioactive sources
	6.2. Regulatory decisions	6.2.1. Long term regulatory decisions 6.2.2. Interim regulatory decisions

3. PROCEDURE TO ACHIEVE TECHNICAL QUALITY IN PSA APPLICATIONS

This section is devoted to the description of the general approach for the presentation of information in this publication including definitions of PSA elements and attributes, the coding scheme for naming general and special PSA attributes, and how the publication can be applied for the purpose of assessing and enhancing the PSA technical quality.

3.1. PSA ELEMENTS AND ATTRIBUTES

The PSA features (termed ‘attributes’ in this publication) are provided for the eleven PSA elements that comprise full scope internal events, internal and external hazards Level 1 PSA for all modes of operation. The PSA elements identify the major analysis areas. It should be noted that while the eleven PSA elements are identified, this division is to some extent arbitrary because all the analysis areas are interconnected and influence each other. In addition to the eleven PSA elements, attributes are defined for “Maintenance and Upgrade of the PSA”. This aspect is not, per se, an “element” of the PSA, but is rather the description of the attributes of developing and implementing a process to be used to assure that the PSA continues to comply with the elements as the plant changes and PSA methods improve. For the sake of convenience the same structure is used for defining attributes for all PSA elements and “Maintenance and Upgrade of the PSA”.

The PSA elements (including maintenance and upgrade) and associated abbreviations used in this publication are the following:

1.	Plant Operational States Analysis	OS	(Section 4)
2.	Hazards Events Analysis	HE	(Section 5)
3.	Initiating Events Analysis	IE	(Section 6)
4.	Accident Sequence Analysis	AS	(Section 7)
5.	Success Criteria Formulation and Supporting Analysis	SC	(Section 8)
6.	Systems Analysis	SY	(Section 9)
7.	Human Reliability Analysis	HR	(Section 10)
8.	Data Analysis	DA	(Section 11)
9.	Dependent Failures Analysis	DF	(Section 12)
10.	Model Integration and Risk Metric Frequency Quantification	MQ	(Section 13)
11.	Results Analysis and Interpretation	RI	(Section 14)
12	Maintenance and Upgrade of the PSA	MU	(Section 15)

Each PSA element is described in a separate section of the publication as indicated above including a description of the objectives of the analysis relating to the PSA element, a list of major analysis tasks, and tables describing general and special attributes for the tasks.

Sections 4-15 present general and special attributes for the twelve PSA elements listed above. An identifier is assigned to each general and special attribute in accordance with the coding scheme provided in Section 3.2. Several special attributes may be defined for a general attribute. They are provided together: special attributes underneath the corresponding general attribute. The tables include the identifiers of general attributes in the first column ('GA' in the table heading), the description of general attributes and, where appropriate, the identifiers/descriptions of the associated special attributes (in italics) in the second column, as well as rationale/comments/examples for general attributes and special attributes (in italics) in the third column.

If a PSA meets solely the general attributes, it would not necessarily mean that the PSA could be used consistently and reliably for any PSA application, e.g. the applications listed in Section 2. Sometimes, special attributes may be important to enhance the depth and level of detail of the analysis in specific areas to facilitate the use of PSA for specific applications. Section 16 discusses what special attributes are appropriate for particular applications and how to determine them.

It should be noted that the PSA results used in the decision making process might be adequate even if certain attributes are not met or not met fully. However, this would generally require that either a demonstration that the attribute is not required to produce the results needed to support the application, or that the decision has compensated for this failure to meet the attribute, by, for example, restricting the scope of the application to that supported by the PSA results. The methods by which this may be demonstrated are not within the scope of the publication.

3.2. CODING SCHEME FOR ATTRIBUTES IDENTIFIERS

General attribute

The identifier of a general attribute is represented by the following string:

XX-YNN,
where:

XX – the identifier of a PSA element as provided in Section 3.1 (IE, DA, etc.);

Y – a letter (in alphabetic order) designating the task within the PSA element;

NN – a two digit number designating the sequential number of the general attribute within Task 'Y'.

Example: **IE-A01 -** this is the identifier of the first general attribute for Task 'A' of the PSA element 'IE'.

Special attribute

The identifier of a special attribute represents the following string:

XX-YNN-SM,

where:

XX-YNN – the identifier of the general attribute, for which a special attribute is provided;

S – the letter ‘S’ indicating that a special attribute is defined for general attribute ‘XX-YNN’;

M – a one digit number designating the sequential number of the special attribute relating to the considered general attribute.

Example: ***IE-A01-S1*** **-** this is the identifier of the first special attribute related to the first general attribute for Task ‘A’ of the PSA element ‘IE’.

3.3. CONNECTION TO IAEA SAFETY GUIDES ON PSA

All PSA elements are addressed in the Safety Guides SSG-3 and SSG-4 [3, 4]. More technical details on the modelling aspects of the PSA elements applicable to a Level 1 at-power internal event PSA are principally addressed in the IAEA Level 1 PSA Procedure Guide[2], those that are applicable to external hazards PSA – in the IAEA Safety Series report [15], internal fire PSA in [18], seismic hazards in [19] and low power and shutdown PSA in [20].

There are also IAEA publications providing more details on the following PSA elements:

- Human Reliability Analysis [9];
- Initiating Events Analysis [21];
- Dependent Failures Analysis [22].

Some of the IAEA publications listed above are rather old and currently the IAEA is developing a set of guidelines to reflect on current state-of-the art in PSA methodology for specific PSA tasks as appropriate, e.g. human reliability analysis, external hazards PSA development (including seismic hazard) and multi-units PSA. Some of these publications are expected to be issued in years 2016-2017 and will replace [15, 19].

3.4. THE PROCEDURE FOR USE OF THE TECDOC

This publication is expected to support two major activities:

1) PSA review as carried out by the IAEA within IPSART missions and as part of other activities.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, IAEA, Vienna (1992).

2) Planning of a PSA project, to make sure that appropriate quality of the full scope Level 1 PSA for each applicable POS is achieved, or assessing the applicability of an existing PSA intended for use in an application.

The general procedure of application of the approach provided in this publication for assessing and enhancing the PSA quality involves consideration of general and special attributes. The following three major steps are involved:

STEP (1) For the PSA application consideration needs to be given to plant design and operational features affected by the application (and related PSA models). PSA scope and results/metrics required for the application have to be determined. In case the scope and results/metrics are insufficient, there may be a need to refine, complete, or upgrade the PSA. For instance, in case an application (e.g. severe accident management) requires Level 2 PSA results, but these are not available, an extension of the PSA scope would be needed. Alternatively, the developer could provide supplementary arguments/analysis/data to bridge limitations, or restrict the scope of the application to that supported by the PSA.

STEP (2) For each PSA element, a determination needs to be made whether the general attributes provided in Sections 4-14 characterizing a 'base case PSA' have been met. If not, refinements need to be considered for the PSA to bring it in compliance with the general attributes. Alternatively, the developer could provide supplementary justifications to demonstrate that the general attributes not met are not required for the application.

STEP (3) For the PSA application, a determination needs to be made whether special attributes needed for this PSA application have been met. Section 16 of this publication needs to be consulted regarding the practical steps for identification of a set of special attributes of PSA elements relevant for the application of interest.

A determination needs to be made whether the special attributes have been made. If not, refinements need to be considered for the PSA to bring it in compliance with the special attributes.

The procedure for determination of PSA quality for applications is shown in Figure 2.

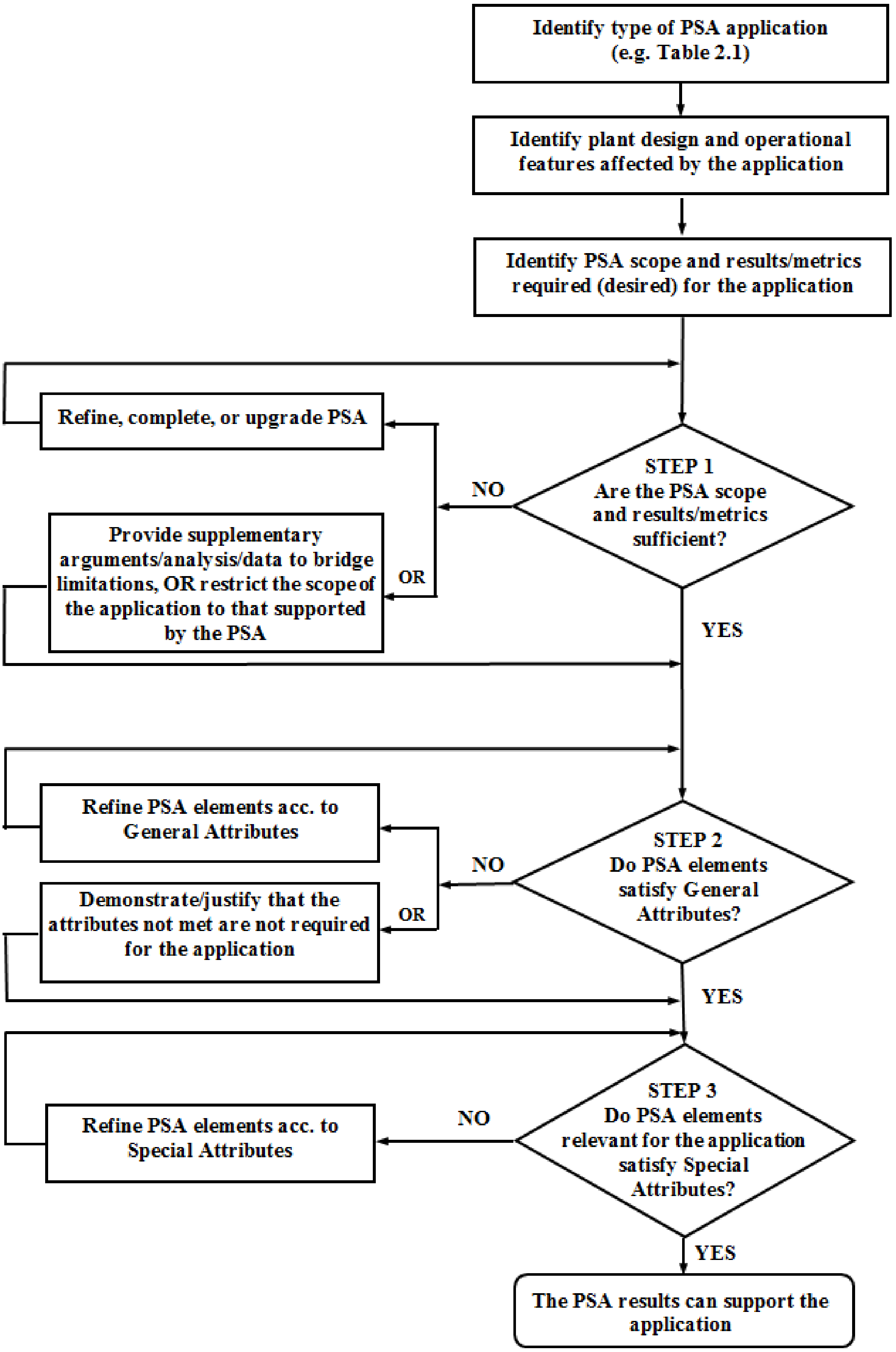
Identify type of PSA application (e.g. Table 2.1)
Identify plant design and operational features affected by the application
Identify PSA scope and results/metrics required (desired) for the application
Refine, complete, or upgrade PSA
STEP 1 Are the PSA scope and results/metrics sufficient?
NO
Provide supplementary arguments/analysis/data to bridge limitations, OR restrict the scope of the application to that supported by the PSA
OR
YES
Refine PSA elements acc. to General Attributes
STEP 2 Do PSA elements satisfy General Attributes?
NO
Demonstrate/justify that the attributes not met are not required for the application
OR
YES
STEP 3 Do PSA elements relevant for the application satisfy Special Attributes?
NO
Refine PSA elements acc. to Special Attributes
YES
The PSA results can support the application

Fig. 2. General procedure for determination of technical quality of PSA for applications.

4. PSA ELEMENT ‘OS’: PLANT OPERATIONAL STATES ANALYSIS

4.1. MAIN OBJECTIVES

The main objective of the Plant Operational States (POS) analysis is to define specific reactor and plant conditions (i.e. POSs) that together cover the entire spectrum of plant operation.

The POS analysis provides the basis for the PSA and ensures its completeness. The risk profile can be incomplete and distorted if important power operating modes defined in plant Technical Specifications or specific plant outages are incorrectly taken into consideration. A POS for the purpose of PSA is defined as a plant configuration during which plant conditions do not significantly change (and activities that impact risk are relatively similar).

The key differences between different POSs relate to the activities being performed and the plant’s ability to prevent a core/fuel[3] damage accident that would lead to a release of radionuclides. These differences are related to available decay heat removal mechanisms, system and component success criteria, the effectiveness of barriers to release, and operator actions that could lead to undesired events that can challenge plant safety. Typical information used to define these differences include: core decay heat level, balance of plant system configuration, primary water level, primary pressure and temperature, reactor coolant system integrity, available residual heat removal mechanisms, containment (confinement) integrity, etc.

A POS can be a steady state POS (for example, full power, low power, hot standby, cold shutdown while on residual heat removal cooling, etc.) or can represent a transition phase between steady states. In order to transit from full power to cold shutdown, there are normally several transition POSs. The complete set of POSs for a specific outage type represents a discretised representation of the outage from a risk perspective. Full power operations can be considered as one plant operating state.

The important POS analysis topics are:

- Identification of a full scope of plant operating states, such as full power operation, power reduction, forced or unplanned outage, scheduled plant shutdown, refuelling outages, maintenance outages, start-up, power increase, etc.;
- Identification of a reasonably complete set of the POSs that reflect the identified plant operating modes and provide a realistic representation of the plant;
- Grouping of similar POSs together to facilitate the practical evaluation of initiating events, accident sequences, success criteria, operator actions, etc., provided that the most severe boundary conditions are assumed for the entire group;
- Estimation of the applicable POS group duration and frequency using information available from operating experience and plant documentation.

[3] During certain POSs, such as refueling, it is possible that damage can occur to individual fuel elements as well as to the whole core.

Important aspects of the POS analysis are the following:

- All plant operating modes and specific outage types are considered;
- Plant conditions which are important for the PSA are divided into mutually exclusive POSs based on operational plant system configurations and their unique impacts on plant response;
- For each POS all important conditions that may affect the core/fuel damage frequency are defined;
- POSs are grouped in a consistent manner such that any POS in the group may be represented by the characteristics of the POS selected as the POS group representative;
- For each POS group the important attributes are well characterized (e.g. the relationship between decay heat level, reactor water level and pressure, the systems available for decay heat removal, etc.);
- For multiunit PSAs the possibility that each reactor unit may be in a different POS at the time of the initiating event need to be considered and a represent set of combinations of POSs are selected consistent with plant operations and maintenance practices.

4.2. POS ANALYSIS TASKS AND THEIR ATTRIBUTES

The main tasks for the PSA element ‘POS Analysis’ are listed in Table 4.1. Tables 4.2-A through 4.2-D present the description of general and special attributes for these tasks.

TABLE 4.1 MAIN TASKS FOR POS ANALYSIS

Task ID	Task Content
OS-A	Identification of POSs
OS-B	POS grouping
OS-C	Estimation of POS frequencies and durations
OS-D	Documentation

TABLE 4.2-A ATTRIBUTES FOR POS ANALYSIS: TASK OS-A ‘IDENTIFICATION OF POSs’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
OS-A	The POS analysis uses a structured, systematic process to identify and define a complete set of plant operational states to be analysed in the PSA for each reactor unit within the scope.		COMMENT: In most cases such parameters as decay heat, primary temperature and pressure, etc. are changing in time even within a POS. It is impractical to reflect such changes in the PSA model; therefore it is generally acceptable to consider the worst parameters to be used for the entire POS duration.
OS-A01	A representative set of plant operational modes is analysed, including operation at different power levels, at-power refuelling, shutdown, refuelling outages, and other controlled shutdowns such as forced and planned maintenance.		COMMENT: Unplanned or forced maintenance shutdowns refers to those outages which result from failure of components which do not immediately challenge plant safety, for example failure of two standby diesel generators, unavailability of an electrical train, unavailability of a standby auxiliary feed train, etc. Unplanned maintenance shutdown start from at-power conditions and are typically grouped into three types determined by their final stable state in which the repair is conducted; i.e. hot shutdown, cold shutdown without draining, and cold shutdown with draining of the RCS. Planned maintenance shutdowns can also generally be grouped into the same three maintenance outage states; i.e. hot shutdown, cold shutdown without draining, and cold shutdown with draining of the RCS.
	OS-A01-S1	*Forced outages resulting from safe short term accident sequences at-power are also considered.*	*RATIONALE: In Level 1 PSA for the at-power POSs, plant evolutions are typically modelled for the early part of the accident sequences until a safe stable state is assured for at least 24 h. The PSA would need to consider additional post-accident POSs in order to model potential core/fuel damage risk beyond 24 h.* *COMMENT: Long duration outages following safe short term accident sequences (designated as OK on an the accident sequence event trees) are grouped by their final stable state in which accident recovery and repair is possible; e.g. low pressure recirculation, high pressure recirculation, feed and bleed cooling or shutdowns without control rod insertion. Most of these types of outages are of relatively low frequency and could be grouped into one or several POSs.*
	OS-A01-S2	*For multiunit PSAs, a representative set of combinations of POSs for each unit is selected such that the most likely combinations are accounted for.*	*RATIONALE: As evidenced in the Fukushima Daiichi accidents, all reactor units may be in different POSs at the time of an initiating event. Hence different combinations of POSs need to be considered. For a large number of units on a single site, it may be*

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	The selected combinations include at least the one with all reactors in operation at full power and one for each reactor unit in a LPSD POS.	*impractical to consider all possible combinations of POSs.* *COMMENT: While simplifications to the POS combinations may be necessary certain PSA applications may require that more POS combinations be considered. Some combinations may be eliminated due to plant operational practices, e.g. not normal to have two units in refuelling at the same time. Each combination of POSs may have a unique potential for each single unit and multiunit initiating event.*
OS-A02	For each identified POS, plant specific documentation and records, are reviewed and the characteristics of the POSs are defined in terms of unique combinations The combination of all POSs covers the entire stable operation and transition states. Characteristics include, but are not limited to: • operating modes; • RCS configurations; • location of the fuel; • range of plant parameters; • activities that change the above; and • containment (confinement) status	COMMENT: Examples of what could be considered for the characteristics listed include but are not limited to the following: • Operating modes or operational conditions as defined in plant Technical Specifications; • RCS configurations such as closed, opened to the containment (confinement) via gas removal system or opened (the reactor head removed) and whether temporary RCS penetrations are installed and their differential pressure capability, presence of vessel internals (which in some plants changes the decay heat removal mechanism from natural circulation cooling to forced circulation on the RHR system); and decay heat removal mechanisms, such as steaming or residual heat removal; • Location of the fuel (e.g. in the core, in the fuel pool, in the transfer tunnel, etc.); • Range of plant parameters, e.g. power level or decay heat level, average reactor coolant temperatures, pressures, and water level; • Activities that may lead to changes in the above parameters; e.g. drain down, filling and venting, dilution, fuel movement, and/or cooldown; • Containment (confinement) status (intact, open). Depending on plant type and design, other characteristics may also be important COMMENT: Plant specific documentation includes Technical Specifications, normal shutdown, refuelling and start-up procedures, etc. Plant records include recent outage plans and records, maintenance plans and records, operations data, trip history, control room logbooks, and thermal hydraulic data such as refuelling outage time to boil and time to core/fuel damage calculations, etc.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		COMMENT: System alignments, component unavailabilities due to maintenance, or major tests and containment (confinement) status could all be characteristics of the POS. However if during a POS there is no restriction on when the planned maintenance must start then the POS need not use the start of such planned maintenance activities as a POS characteristic. As such, these would be considered as conditional probabilities during the POS and not POS characteristics. On the other hand, if planned maintenance must start at a specific time or condition within the POS (e.g. train changing) then the start of such planned maintenance may appropriately be considered as an additional characteristic in defining the POS (this is not typical). COMMENT: The decay heat level associated with each POS is determined for use in defining and applying success criteria and the timing for operator actions. When the decay heat is the only variable during a specific time period (i.e. configuration is the same) then this could be considered a single POS.
OS-A03	Known plans for future plant operation (e.g. the next refuelling outage) are reviewed to ensure the POS identification remain valid and appropriate.	COMMENT: The known plans may be in written form, or may be extracted by way of the interviews. COMMENT: Experience from similar plants could be used in defining POSs for the plant with limited operational history. COMMENT: For example, specific POSs might need to be introduced if at least, one of the following aspects is identified: – POSs that were not previously encountered; for example, if a PWR did not previously have a hot mid-loop POS in its history, but will have this state in the next refuelling outage; – Configuration is allowable and was observed at similar plants but was not considered in the POS definition; – Early entry into a POS, results in substantially higher decay heat; or later entry into a POS, resulting in substantially lower decay heat.
	OS-A03-S1 *One time or specific known activities is accounted for in the assessment*	*RATIONALE: Typically important for configuration management during long outages.* *EXAMPLE: Steam generator replacement.*

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
OS-A04	Additional characteristics of the POSs are defined for each representative plant transition POS in terms of the relevant and capable SSCs, considering the ability of each system within a POS to mitigate applicable initiating events and to prevent core/fuel damage and large release.	COMMENT: The characterization process is iterative with the development of subsequent PSA tasks such that the initial POS characterization may change. For example, as the success criteria and data are developed it may be found that early in an outage an alternate decay heat removal system may be unavailable for the duration of a particular POS due to the decay heat being higher than the capacity of the system. Further, maintenance activities may or may not be a reason to subdivide a POS. To the extent that protected trains are employed while permitting maintenance on the other trains, then separation of a POS to distinguish changes in the protected train is a natural way to facilitate sequence frequency quantification. However, when planned maintenance involving different trains of equipment occurs randomly within a POS, then there is no need to subdivide the POS. COMMENT: Some examples of POS characteristics include system actuations, alignments, system success criteria, reliability/availability of systems, and the status of containment (confinement). EXAMPLE: – Main transformer isolated; – Service water system cross-tie open; – Steam supply to turbine driven auxiliary feedwater pump isolated; – Flood or fire barrier doors open; – Halon systems disabled.
OS-A05	Appropriate plant personnel (e.g. operations, maintenance, engineering, safety analysis, and outage planning) are interviewed to determine if any potential POS of past or future plant transition POSs has been overlooked.	RATIONALE: Interview of experienced plant personal may give additional knowledge on real plant behaviour and may help to identify POSs overlooked. COMMENT: Information from interviews conducted at similar plants may also be used but is not a substitute for plant specific interviews if an operating plant is under consideration.

TABLE 4.2-B ATTRIBUTES FOR POS ANALYSIS: TASK OS-B ‘POS GROUPING’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
OS-B	The POS analysis justifies all grouping of POSs to reduce the complexity of the PSA.	
OS-B01	POSs appearing in the same plant transition mode (e.g. cooldown mode, start-up mode) with similar plant response, success criteria, effect on operability, operator performance and relevant mitigating systems, are grouped such that all specific features impacting plant risk are included in the POS group.	COMMENT: Forced/unplanned outages are not combined together; a forced outage scenario POS need to be chosen to represent all potential causes of a forced outage; e.g. a turbine trip outage to hot standby, a loss of main feedwater outage requiring cold shutdown but without draindown, an RCS leakage for outages involving cooldown to cold shutdown with RCS draining, etc. COMMENT: For unplanned maintenance outages, three unplanned outage scenario POSs need to be chosen to represent all potential unplanned outages; i.e. hot shutdown, cold shutdown without draining, and cold shutdown with draining of the RCS to effect repairs. COMMENT: Grouping of the POSs is an iterative task, the judgement as to which features of a POS impact plant risk need to be confirmed after every iteration of the model quantification.
	OS-B01-S1 *Further grouping of POSs for each reactor unit in a multiunit PSA may be required to keep the combination of POSs to be modelled to a manageable level. Such further grouping is done so as not to mask the potential for initiating events that impact multiple reactor units concurrently*	*RATIONALE: It is expected that a multiunit PSA would be performed following the completion of single unit PSAs for each reactor on the site. Insights regarding the risk significant POSs from the single unit PSAs can be used to inform judgments to support further grouping. However, such grouping needs to be done in a manner that enables the potential for multiunit initiating events to be identified.* *COMMENT: Because initiating event selection and initiating event frequencies are in general POS dependent it is important that POS grouping be done in a manner that does not mask the potential for a multiunit initiating event.*
OS-B02	The POS grouping is checked to ensure that POSs with different plant response impacts (i.e. those with different success criteria) or those that could have more severe radionuclide release potential remain separated.	RATIONALE: This aspect may be important for subsequent Level 2 PSA. COMMENT: POS grouping need to be reviewed when information from the Level 2 PSA is available.
OS-B03	POSs that are used for those brief time periods involving activities (operational or maintenance) that lead to initiating events that are	RATIONALE: In this context, “demand-based” means an initiating event that is linked to a specific activity as opposed to occurring randomly in time over the POS

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	“demand-based” are separated from those that are time-based.	duration. EXAMPLE: In a PWR, the activity for drain down to midloop has been associated with historical events related to over-draining while lowering RCS level. This need to be modelled as a separate POS associated with the drain down activity and not grouped with other POSs. The intent of separating periods involving demand-based initiating events from other POSs is to avoid having to approximate the demand-based initiating event as one that is time-based. Dropped loads, such as dropping of the reactor head, need to be considered as demand-based.
OS-B04	If POSs are combined into groups, the most severe or constraining characteristics (with respect to core/fuel damage) of any POS within the group are chosen for the combined group.	COMMENT: The selection of the representative characteristics for a POS should consider the applicable initiating events for the POS. For example, LOCA initiators may be best represented by conditions within the POS when the RCS level is the lowest, while losses of heat removal may be best represented by conditions early in the POS, when the decay heat is the highest.
OS-B05	The POS groupings based on the results of the analyses within task OS-B is compiled and justified by iterative review.	COMMENT: Judgement as to the adequacy of the grouping to reflect the plant risk need to be confirmed upon every iteration of the model quantification.

TABLE 4.2-C ATTRIBUTES FOR POS ANALYSIS: TASK OS-C ‘ESTIMATION OF POS FREQUENCIES AND DURATIONS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
OS-C	The POS analysis determines the fraction of time in a calendar year spent in each modelled POS. These fractions may be estimated in terms of the average frequency and duration of each POS.		
OS-C01	The frequency and duration of POSs are determined based on a review of relevant plant specific records (such as operating profile, trip history, outage plans, maintenance records, logbooks) and, as appropriate, the frequency of forced outages assigned to each identified safe, stable state from the plant specific at-power PSA.		EXAMPLE: The frequency of a refuelling outage could be once in 18 months, with duration of 30 days. Duration data need to be developed using the requirements in the data analysis section. For forced outages due to short term accident sequences, there is likely no experience data on which to estimate the duration for the POS representing repair. Such durations will instead have to be estimated based on expert judgment. The applicable records are typically represented by the most recent data. However, future planned plant operation may differ from past practice, for example, by conducting a hot midloop repair. Another example is that the most recent outage may consist of unusual activities such as replacement of the reactor vessel head that would not be expected in a typical outage.
	OS-C01-S1	*The frequency and duration of POSs are determined based on a review of operational experience of similar plants with the same refuelling programme, generic PSA studies, design requirements, planned refuelling procedure, or other sources of information.*	*COMMENT: This SA is applied for new NPPs or NPPs with changed refuelling programmes.*
	OS-C01-S2	*The specific duration of POSs is determined based on an actual planning.*	*COMMENT: This attribute is applicable to a situation-specific outage or configuration risk management application and requires a detailed review of outage schedules and/or interviews with plant outage schedule planning personnel.*
	OS-C01-S3	*The frequency of post-accident POSs associated with forced outages resulting from safe short term accident sequences at-power is defined as a sum of frequencies of non-core/fuel damage accident sequences. The duration of these post-accident POSs is also determined*	*COMMENT: The duration of such outages are defined as the average time to return to power after forced outage based on observed experience from the plant under investigation, industry wide experience and or expert judgment in absence of other information. The time required to return to power in case of transient events could be available from experience; however, for the LOCAs-type events leading to forced outages experience is very limited and expert judgement need to be used.*

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	OS-CO1-S4	*For multiunit PSA it is necessary to estimate the probability or fraction of time that is spent in each modelled combination of POSs for each reactor unit. These estimates account for plant operational and maintenance practices.*	*RATIONALE: A separate multiunit PSA model will be needed to account for each modelled combination of POSs. Each applicable combination of POSs effectively represents the POS for the multiunit site. The probability or fraction of time spent in each modelled POS combination must be known to support quantification of multiunit initiating events and accident sequences.* *COMMENT: Some combinations may be eliminated due to plant operational practices, e.g. not normal to have two units in refuelling at the same time. It is not expected that the POS fractions for each reactor unit will be independently combined.*
OS-C02	The durations for each POS group are obtained as the sum of the durations of POSs included in the group.		COMMENT: As results from different risk sources, such as power and non-power operation or internal/external hazards, are combined, the durations are calculated as a fraction of a calendar year. COMMENT: The sum of all POS groups durations is generally equal to one calendar year COMMENT: This attribute may not be applicable for configuration risk management application.
OS-C03	Any changes to future plans or upcoming POS schedules are reviewed to ensure that the POS durations and assumed plant conditions remain valid.		COMMENT: Shorter outages often mean POSs are entered sooner with higher decay heat levels. The higher decay heat may affect the success criteria of a system or component and may result in a new POS.

TABLE 4.2-D ATTRIBUTES FOR POS ANALYSIS: TASK OS-D ‘DOCUMENTATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
OS-D	Documentation and information storage is performed in a manner that facilitates peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the assumptions made and their bases	
OS-D01	The following aspects of the POS analysis process are documented (a) identification of the plant transition modes, their average durations and average frequencies; (b) the process and criteria used to identify each POS; (c) the description of each POS; (d) the defining characteristics of each POS; (e) the process and criteria used to group POSs; (f) the applicable durations and average frequencies of POSs; (g) the defining characteristics of each POS grouping; (h) specific interfaces with other PSA tasks for traceability, and to facilitate configuration control when interfacing tasks are updated; (i) records of interviews (i.e. plant crew, schedule, planning, etc.) and collection of operating experience; (j) for multiunit PSAs the basis for the selection of POS combinations to be modelled and for estimating the fraction of time spent in each combination.	COMMENT: It is recommended to present information on POS durations, configurations and parameters in transparent and visualized manner in the form of tables, graphs and logical diagrams.
OS-D02	The sources of model uncertainty and related assumptions associated with the POS analysis are documented.	COMMENT: Model uncertainty usually relates to factors that do not have a parametric uncertainty. For example: assumed initial conditions for POS
OS-D03	All the underlying data (with uncertainty), information sources and analyses are documented.	

5. PSA ELEMENT ‘HE’: HAZARD EVENTS ANALYSIS

5.1. MAIN OBJECTIVES

The analysis of hazard events refers to the process of starting with a consideration of all possible hazards to the plant and taking it to the point where the specific events that will be incorporated into the PSA model have been determined and their frequencies determined. In order to do this, there needs to be an understanding of the difference and relationship between hazards, hazard groups, hazard events, and initiating events. In accordance with SSG-3, this section treats the following types of plant hazards:

- Internal hazards, including, but not limited to:
  - Internal fires
  - Internal floods
- External hazards, including
  - Seismic
  - External flood
  - High winds
  - Human-induced hazards

The section covers the following aspects of the hazards analysis.

- Identification of the hazards to be considered;
- Screening hazards of low potential risk at the specific site;
- Defining the hazard events to be included in the detailed PSA;
- Defining scenarios for internal fires and floods;
- Determining the frequency of the hazard events.

“Hazard group” refers to a collection of hazards that are assessed in the PSA using a common approach, methods, and data, while a “hazard” is the specific phenomenon that puts the plant at risk. A hazard group may consist of a single hazard (e.g. internal fires or seismic events) such that the hazard group and hazard are synonymous,[4] or multiple hazards (e.g. an internal-events hazard group, which includes transients and loss of coolant accident (LOCA) hazards; or a high-wind hazard group, which includes hurricane, tornado, and straight-wind hazards). In this context, the hazard is the phenomenon; the hazard event is an occurrence of the phenomenon of a specific severity that could possibly result in a plant trip and, in many cases, other damage. The initiating event is the specific plant perturbation that challenges plant control and safety systems.

[4] In theory, if every individual hazard had to be analyzed using a different approach, method, or data, then there would be no rationale to have hazard groups. However, this is not the case in reality. There are multiple individual hazards that can be analyzed using the same approach, data and methods, so grouping allows them to be analyzed in an integrated fashion and to meet each attribute in a similar manner.

In general, there is a range of hazard events associated with any given hazard, and, for analysis purposes, the range can be divided into bins characterized by their severity. Hazard events of different severity can result in different initiating events.

The terms "hazard event" and "initiating event" are not synonymous. Rather, a hazard event is identified as the cause of an initiating event by virtue of the effect it has on the plant. The assessment of the effect on the plant defines the reason for the plant trip as well as any additional failures, and provides the starting point for the analysis of the plant response. Therefore, in keeping with the definition of initiating event, for the occurrence of a given hazard event, the initiating event (or events, as more than one outcome may be possible) is (are) a perturbation to the steady state operation of the plant that challenges plant control and safety systems whose failure could potentially lead to core/fuel damage. For example, consider the earthquake hazard group, which involves only one hazard, i.e. earthquakes are the hazard and also the hazard group. This hazard (earthquakes) can be defined in terms of a range of seismic events (e.g. 0.1g, 0.3g, 0.5g, >0.75g) and their associated spectral shapes and time histories.

- A manual scram may be an initiating event for the 0.1g earthquake;
- A loss of off-site power (LOOP) is often assumed as the initiating event for the 0.3g and 0.5g earthquakes;
- A LOCA may be the initiating event for very large (>0.75g) earthquakes.

These assessments would be made based on an assessment of their impact on the plant. For example, for a 0.1g seismic event, the likelihood of any physical damage resulting in an automatic trip is small; for 0.3g and 0.5g seismic events, the most likely effect may be damage to the switchyard or the transmission system; and for a >0.75g seismic event, in addition to a LOOP, there may be a significant likelihood of failure of vessel or piping anchorage. A [hazard] event can be associated with multiple initiating events (each with a conditional probability of occurrence), so that a 0.3g seismic event might result in a manual scram, a LOOP, a LOCA, or a combination of a LOOP and a LOCA, each with an associated conditional probability, which, when combined with the [hazard] event frequency, provides the corresponding initiating event frequency.

It is even possible that a [hazard] event would not result in an initiating event (i.e. there would be no perturbation of the plant operation). For example, a plant may automatically trip (initiating event), may be manually tripped (initiating event), or may continue (no initiating event) to operate through a hurricane event. These examples highlight why the distinction between "hazard event" and "initiating event" is important and must be maintained.

The hazard events analysis is a highly iterative, multipurpose task, which provides the basis for expanding the PSA beyond the baseline of internal events and ensures completeness of treatment of all the hazards that can potentially contribute to the frequency of core/fuel damage. The risk profile can be incomplete and distorted if hazards that provide a significant[5] contribution to the total core/fuel damage frequency are omitted.

Alternately, there is great potential for expenditures of effort through detailed analysis of hazards that do not improve the understanding of the dominant contributors to core/fuel damage frequency.

Therefore, the identification of which hazards do not provide a significant contribution to the total core/fuel damage frequency is also important. Since internal events are the baseline for any PSA, this Chapter does not apply to internal events. The identification of hazard events associated with internal events is accomplished starting with Chapter 6.

The main objectives of the hazard events analysis are as follows:

- to identify a complete set of the hazards that have the potential to cause any initiating events applicable to the type of reactor[6] (i.e. interrupt normal plant operation and that require successful mitigation to prevent core/fuel damage), so that no significant contributor to core/fuel damage is omitted;
- to screen out hazards whose contribution to plant risk is small, so that analysis effort is not applied in an unproductive manner;
- to group hazards to facilitate the efficient definition of hazard events, modelling of plant response and hazard event frequency assessment while providing sufficient resolution regarding modelling of accident sequences;
- for multiunit PSAs, to facilitate the identification and grouping of hazards in a manner that enables the distinction to be made between initiating events impacting single reactor units independently and multiple reactor units concurrently.
- to define the range of hazard events that can be caused by the unscreened hazards in each hazard group;
- to address the treatment of correlated hazard events; and
- to provide estimates for the frequencies of the hazard events using information available and associated estimation techniques.

Important aspects of the HE analysis are the following:

- Hazard identification is correct and complete;
- Hazard screening is done using defined criteria and methods;

[5] There are many ways to define the meaning of "significant" when referring to the contribution to core/fuel damage frequency. Screening criteria have been defined in the attributes below that provide a reasonable practical limit on what should be considered "significant" hazards.

[6] The intent here is to start with a complete list of all hazards that could cause an initiating event at any reactor of the given type at any location (site). Screening certain hazards based on site-specific considerations is done later. This is made clear by the attributes.

- Hazard event definition is correct and complete (i.e. that the PSA model will include all of the hazard events that have a significant contribution to core/fuel damage frequency in a realistic manner);
- Hazards are grouped in a consistent manner such that any associated hazard events developed for the group have the same or less impact on plant SSCs as the hazard event used to represent that group for further modelling;
- Methods used for the estimation of the hazard event frequencies are clearly distinguished for the cases when:
  - Estimation is based on plant specific or generic, or both kinds of statistical information. When generic statistical information is used, estimation will take into account site-specific conditions in the application of that information.
  - Estimation for rare events, which is based on expert judgment or use of specific methods (e.g. use of applicable physical models, etc.);
- Uncertainties in the hazard event frequencies are understood, evaluated, accounted for, and documented.

5.2. HAZARD EVENTS ANALYSIS TASKS AND THEIR ATTRIBUTES

The main tasks for the PSA element ‘HE Analysis’ are listed in Table 5.1. Tables 5.2-A through 5.2-M present the description of general and special attributes for these tasks.

TABLE 5.1 MAIN TASKS FOR HE ANALYSIS

Task ID	Task Content
HE-A	Identification of potential hazards
HE-B	Hazard screening and final hazards list identification
HE-C	Characterization of hazard events for all hazards
HE-D	Characterization of hazard events for internal fires
HE-E	Characterization of hazard events for internal floods
HE-F	Characterization of hazard events for seismic
HE-G	Frequency of hazard events for all hazards
HE-H	Frequency of hazard events for internal fires
HE-I	Frequency of hazard events for internal floods
HE-J	Frequency of hazard events for seismic
HE-K	Fire scenario development
HE-L	Flood scenario development
HE-M	Documentation

TABLE 5.2-A ATTRIBUTES FOR HE ANALYSIS: TASK HE-A ‘IDENTIFICATION OF POTENTIAL HAZARDS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-A	A list of potential hazards is defined that is as complete as possible using different methods and applicable sources of information.	
HE-A01	The list of potential internal and external hazards includes consideration of generic hazards from international sources of data.	COMMENT: There are a number of sources of lists of hazards that have been developed for design requirements and PSAs. These sources are useful in developing an initial list of hazards to consider. EXAMPLE: The following references listed in the reference section of this report are useful sources of lists of hazards: [3, 5, 15, 23-34].
HE-A02	The list of potential hazards is augmented by a review of hazards considered in past PSA.	RATIONALE: Review of what hazards other plants have included in their PSAs can help to identify hazards that may be missed otherwise.
HE-A03	The list of potential hazards is augmented by a review of the plant safety analysis report and/or any siting studies and site environment assessments.	RATIONALE: These reports generally include comprehensive site assessments of site conditions that can be used to identify site-specific hazard considerations.
HE-A04	Credible correlated hazard groups for the site are defined. Two types of correlated hazards (induced hazards and combined hazards), are considered: – Induced hazards result from the case where the occurrence of the initial hazard creates conditions that result in a second hazard being caused to occur closely in time; – Combined hazards result from the case where the occurrence of the hazard has multiple manifestations such that a secondary effect often accompanies the primary effect. In addition consideration is given for credible combinations of independent hazards occurring simultaneously.	COMMENT: The general concept can be thought of as follows. Combined hazards are always correlated to some extent. There is always a possibility that they can appear together because they are inextricable manifestations of a single cause. Induced hazards are those that may or may not be correlated at any particular site depending on the conditions. They could either occur together or not. It is important to be thorough and imaginative in the possible correlations in order to assure completeness. EXAMPLES: An example of an induced hazard that may be encountered during the hazard screening process is high winds in combination with a forest fire. The high winds themselves can affect plant systems (such as HVAC, off-site power) while it may also be that camping nearby is common and these winds may induce a fire by scattering hot embers from forest fires. These then are not independent events, but the correlation may not be applicable at a given site (for example, no forest). The Fukushima Daiichi event was an induced hazard. Seismic events can be accompanied by tsunamis, but at many sites that correlation is not possible. Even at sites where such a correlation is possible, it is still possible to have an earthquake without a

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		tsunami or a tsunami without an earthquake (that affects the site). Another earthquake example would be earthquake-induced landslide for sites in the vicinity of steep slopes. An example of combined hazards is hurricane, for which the primary concern is the high winds. Hurricanes are always accompanied by precipitation, and so this correlation must always be considered. There are other possible manifestations that may have to be considered on a site-specific basis (e.g. surge, missiles). The only question is whether the precipitation can be intense enough that it can result in localized flooding that further compromises plant systems. EXAMPLE: Hazards occurring during a long hot summer period, prolonged external flood, etc. are an example of credible combinations of independent hazards.
HE-A05	The list of potential hazards is augmented by a review of operating experience.	RATIONALE: Most generic lists of hazards were developed years ago (even if they are currently included in more recent documents). Hazards that are not included in these lists (in particular internal plant hazards and human-induced hazards), may have been experienced at nuclear plants more recently than when these lists were developed. EXAMPLES: Most countries have requirements that occurrences that could impact plant operations be reported to the regulatory authority (e.g. Licensee Event Reports (LERs) in the US). These sources are generally publically available. As an example, occurrences caused high temperatures, forest fires, lighting impact, high wind combined with low temperatures and snowing, service water plugging by seaweed and others were reported from WWER operational experience.
HE-A06	Site-specific investigation and walkdowns and visual confirmation is conducted to identify plant specific hazards that are not accounted for by the previous attributes.	RATIONALE: Plant and site specific characteristics could add hazards that are not on any of the generic lists and also have not been otherwise considered. Although this is becoming less and less likely as time and experience go on, there is still a need to consider the possibility. COMMENT: It need to be noted that it is not possible to confirm the site-specific hazards list while a plant is in the design or construction phase. Therefore, while performing a PSA for a plant in design, walkdowns are effective only at the end of construction.

TABLE 5.2-B ATTRIBUTES FOR HE ANALYSIS: TASK HE-B ‘HAZARD SCREENING AND FINAL HAZARDS LIST IDENTIFICATION

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-B	The list of potential hazards is screened in order to eliminate hazards that are not potentially significant.	COMMENT: This task and the associated attributes do not apply to internal fire, internal flood, and seismic. As a practical matter, there are no techniques or criteria that will allow these hazards to be screened and a PSA in accordance with the attributes in other sections of this TECDOC is performed. This PSA effort may include screening of specific hazard scenarios per the hazard group attributes. COMMENT: The term “potentially significant” is meant to ensure the screening process accounts for uncertainty at this stage of the analysis. One approach is the use of “demonstratively conservative” analysis measured against an established goal.
HE-B01	The list of potential hazards are arranged in groups where each hazard in the group shares a common approach, methods, and data,	COMMENT: The creation of hazard groups is a tool to aid the efficient analysis of each hazard in the group. Each hazard is still analysed and screened separately, but the approach to doing so has common features. Hazard groups may have a single hazard or multiple hazards. EXAMPLES: Turbine generated missiles have little in common with other hazards considered in PSAs. Therefore, it is typical that they are in its own hazard group. Straight winds, tornados, and hurricanes have many common features, in particular the data sources and design information relevant to analyzing them. Therefore, it is typical that these would be placed in a single hazard group called “high winds.” COMMENT: For the hazards groups that include several hazards the representative hazard for the group should have the most restrictive features of each hazard in the group. The grouping of the hazards needs to be performed after the screening process is completed. EXAMPLE: This is not always as simple as it seems. The representative hazard may differ over the frequency range of interest. This may need to be addressed during the hazard analysis. For example, for high winds the lower wind speed frequencies may be dominated by straight winds, the middle range by hurricanes, and the upper range by tornados. This would need to be considered. This does not mean that the hazards cannot be grouped, but rather that care needs to be taken to properly select the

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		representative hazard event characteristics for each level of severity within the group. Of course, if the wind speed data is historical and it aggregates all data (regardless of source of wind speed), this is covered and the selection of the representative event becomes simple.
HE-B02	The necessary information relative to each hazard group is obtained	EXAMPLES: Information collection for the hazard group “high winds” could include: – Meteorological information on maximum credible wind speeds for various wind events (both average and gust); – Any available information on return intervals for various different magnitudes of the above events; – Location and characteristics of items that could become wind-generated missiles (e.g. utility poles); – Location and design of any wind breaks or missile shields that would protect structures from damage; – Design capacity of structures for resistance to wind forces (maximum gust and maximum sustained wind). Information collection for the hazard group “transportation accidents” could include: – Identify all airports within 34 kilometres of plant site. For those airports, provide estimates of the yearly number of take-offs and landings, typical flight paths, and type of aircraft. The take-off and landing crash rate may be significantly different from the in-flight crash rate; – Identify common flight paths of aircraft in the vicinity of the plant site for aircraft not in take-off or landing. Provide estimates of number and type of aircraft using those flight paths each year; – Generic crash rate data for the aircraft of interest; – Information on automobile and rail traffic on site, including type of vehicle and contents. Limit to large vehicles capable of damaging structures and equipment by direct impact or vehicles containing explosive or hazardous material. Include the effect of expected construction activities during operations;

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		– Information on automobile and rail traffic near the site where the vehicle contains explosive or hazardous material. Definition of "near the site" need to be based on whether a resulting explosion could generate hazardous force at the site or a release of hazardous material could generate dangerous concentrations on the site; – Design capacity of structures for exposure to explosion (maximum peak overpressure and overpressure time history). This information also applicable to evaluation of nearby facility accidents; – Design features to prevent ingress of hazardous gasses into plant buildings (e.g. intake filtration systems). This information also applicable to evaluation of nearby facility accidents and hazardous material release from on-site storage.
HE-B03	Qualitative screening criteria applied to each hazard within each hazard group to determine if the hazard can be screened out from further analysis are defined in the way that only risk negligible hazards are screened out. If all hazards in a hazard group can be screened, then the entire hazard group can be screened. These criteria are restrictive such that that they can be justified to be applied to individual hazards without consideration of possible correlated hazards (correlated hazards are the subject of a later attribute).	COMMENTS: The following qualitative screening criteria are typically applied: a) The occurrence of the hazard will not lead to an initiating event and/or degradation of a safety system. This criterion is applied only in cases where the conclusion is independent of the severity of the hazard (i.e. where any severity of the hazard will not lead to an initiating event). For that reason, for external hazards this criterion is only applied to hazards that are not applicable to the specific plant (e.g. cannot occur close enough to the plant to affect it). b) The hazard is slow to develop and there is sufficient time to prevent the hazard from affecting the plant and it can be shown that it is feasible within the time available to prepare and implement a response to mitigate the effects of the hazard with high confidence. c) The hazard has been included in the definition of another hazard. EXAMPLES: The following are examples of the application of each criterion: For criterion "a", it would be possible to screen out tsunami for a plant located on a river or cooling pond well inland from the coast. Note that where a hazard can cause degradation but does not directly result in an initiating event or require a plant trip, consideration needs to be given to the possibility that an initiating event could occur during the time period when the degraded condition exists. It may be possible to address this through application of quantitative screening, or it may be necessary to include in the PSA.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		For criterion "b", it would be possible to eliminate low lake level for a plant that has a separate cooling pond where the lake is simply the primary source of make-up to the cooling pond and the cooling pond has sufficient capacity to provide cooling for many days without make-up. A drop in lake level such that it could not be used for make-up would allow sufficient time to apply other sources of make-up to the pond regardless of regional conditions. For criterion "c", certain individual hazards associated with external flooding could be combined into a single external flooding hazard if the source data for the flooding analysis is an integrated data set of historical data for water levels at the site. In such case, the hazard is not so much being screened as it is being subsumed in a broader analysis.
HE-B04	If further qualitative screening is performed, additional qualitative screening criteria are applied to hazards that cannot be screened under HE-B03 only if they do not have any correlated hazards (i.e. they are probabilistically independent of all other remaining hazards).	COMMENTS: The following qualitative criteria are typically applied. a) The maximum possible severity of the hazard is of lesser damage potential than the design basis hazard event for another hazard that affects the same systems, structures, and components in the same way. This is applied by conducting an evaluation of plant design bases in order to estimate the resistance of plant structures and systems to a particular hazard. d) The hazard has a significantly lower mean frequency of occurrence than another hazard for which the plant has been designed; taking into account the uncertainties in the estimates of both frequencies, and the hazard could not result in worse consequences than the consequences from the other hazard. RATIONALE: These two screening criteria have been used in the past, and are generally valid. However, when the consideration of correlated hazards is taken, these criteria may result in screening hazards that, when taken in conjunction with the potential for concurrent hazards, should not be screened. EXAMPLES: The following are examples of the application of each criterion. Note that for both these examples it is assumed that a site-specific assessment was performed and it was determined that the screened hazard did not have any correlated hazards. For criterion d, the plant has been designed for a far upstream dam break that would cause a flood level of 5 meters at the site. Because of the topography around the site,

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		the maximum possible flood height that can result from a slow increase in water level (e.g. from extremely intense precipitation, rapid snow melt, etc.) is three meters (that is, the volume of water required to be generated from these other sources to exceed three meters at the site is clearly in excess of what is possible). Therefore, these other flooding hazards can be screened. For criterion e, the plant has a design basis for lake level increase up to 2 meters. If this level is exceeded, the only affected area is the service water pump house. The frequency of this design basis event has been estimated as 1E-4/year. Another hazard that would only affect the service water pump house is debris clogging the inlet. The frequency of this event is estimated as 5E-6/year. Because debris clogging cannot have worse consequences than increase in lake level, and the frequency is significantly lower, debris clogging can be screened.
HE-B05	The entire hazard group or specific hazard of certain intensity is screened out only when it is confirmed that the screening criteria can be applied for all correlated hazards involving the hazard under consideration.	RATIONALE: The impact of the correlated hazards can be much more severe than the impact of the individual hazard EXAMPLE: The impact of high winds of certain intensity and external flood of certain level might be negligible for plant safety when considered individually, but can be extremely severe when considered in combination.
HE-B06	When quantitative screening criteria are applied to both individual hazards that could not be screened qualitatively and also to the identified correlated hazards to screen them from further detailed analysis of the estimated impact of the hazard to the plant risk. In the selection of quantitative screening criteria; the guiding principle is to ensure that individual and correlated hazards that screen out, if subjected to detailed realistic assessment, would not make a significant contribution to the total aggregated risk for the risk metrics used in the PSA. The following criteria are typically applied. **Based on design basis hazard event core/fuel damage frequency and large early release frequency** 1. An individual hazard can be screened from further detailed analysis if: (a) the plant has a design basis for the hazard (i.e. there is a	RATIONALE: The first two quantitative screening criteria are based on the concept that an SSC designed for a specific design basis hazard event will not fail when subjected to that specific event severity and that design criteria are sufficiently conservative that the SSC has margin above that severity (i.e. the severity will have to exceed the design basis hazard event severity and there is no “failure cliff” just above that severity). The numerical screening criteria for correlated hazards is set at one order of magnitude below that for individual events because the SSCs, while they may be designed for each event, are not designed for both events at the same time and so the margin is potentially much lower. The last two criteria require more analysis because they can be applied to cases where there is not specific design basis hazard event for the hazard. The intent in the use of these criteria that the screening analysis be sufficiently bounding or conservative to ensure that if the hazards were subjected to detailed realistic analysis, the contribution to the total aggregated risk would not be significant. These criteria are somewhat more

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	defined design basis hazard event) and (b) (frequency of the design basis hazard event) x CCDP/CFDP (CLERP) < α% of the internal events CDF/FDF (LERF), Where: CCDP/CFDP (CLERP) is calculated assuming all SSCs that are not designed for the design basis hazard event fail; α - the parameter of the screening criteria representing the contribution to the overall CDF/FDF (LERF) of the individual hazard. 2. Correlated hazards can be screened from further detailed analysis if (a) the plant has a design basis for **both** hazards and (b) (frequency of the correlated design basis hazard events) x CCDP/CFDP (CLERP) < β% of the internal events CDF/FDF (LERF). Where: the plant CCDP/CFDP (CLERP) is calculated assuming all SSCs that are not designed **either** design basis hazard event fail; β - the parameter of the screening criteria representing the contribution to the overall CDF/FDF (LERF) of the correlated hazard. **Based on overall core/fuel damage frequency** 3. An individual hazard can be screened from further detailed analysis if a bounding or demonstrably conservative estimate of CDF/FDF (LERF) over the full range of hazard event severity is less than α% of the internal events CDF/FDF. 4. Correlated hazards can be screened from further detailed analysis if a bounding or demonstrably conservative estimate of CDF/FDF (LERF) over the full range of hazard event severity is less than 10% of the internal events CDF/FDF (LERF). The calculated values that result from the quantitative screening process are retained in the results of the PSA	restrictive in the analytical sense because in the absence of a design basis for the hazard there can be no prescribed threshold for the occurrence of damage to an SSC. Either the hazard frequency must be so low that the design of the SSCs does not really matter or some analysis of plant response must be performed in order to support a position that the plant can handle the hazard sufficiently. However, the order of magnitude difference between the criterion for an individual hazard versus correlated hazards is not required in this case because the CDF estimate is not just for the design basis hazard event, but rather includes beyond design basis hazard events. Therefore, the CCDP/CFDP would already account for the impact of the correlated hazards more thoroughly than under criteria 1 and 2. Therefore, in some cases it may be beneficial to apply these criteria even where a design basis exists. If the hazard has the potential to “couple” core/fuel damage to large early release (that is, increase the probability of a large early release given core/fuel damage significantly above what it would be for internal events), then the LERF criterion should also be applied. It would be possible to relax these criteria by requiring more rigorous analysis, but at that point the analytical requirements would exceed what could reasonably be called screening and it would be more productive to proceed to incorporating the hazard into the PSA as defined in HE-C and HE-G and the other hazard PSA attributes in the rest of this publication. COMMENT: With regard to criteria 1 and 2 parameters α and β need to be defined taken into account overall CDF/FDF (LERF) and number of hazards applicable to the site and the installation ensuring that the contribution is sufficiently low both in absolute and relative terms and relevant regulatory requirements are satisfied. Typical ranges for α and β: $1\leq\alpha\leq10$; $\beta\leq1$. COMMENT: With regard to criteria 3 and 4, the assessment of CDF/FDF addresses four aspects; (a) hazard analysis; (b) plant system and structural response analysis; (c) evaluation of plant systems and structures fragility; and (d) plant system and sequence analysis. Achieving a bounding or demonstrably conservative analysis does not require that each of these four aspects is bounding or demonstrably conservative, only that when taken together the answer is. This affords flexibility to determine the most efficient analytical path for the screening calculation.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
			COMMENT: It is noted that sometimes other risk metrics may ultimately be quantified as part of the PSA. While it is possible to use these other risk metrics in the screening process, it is unlikely that their use would result in different screening insights, so the use of CDF/FDF and LERF is sufficient. The one exception is when a multiunit risk metric is needed. In such case the special attribute below would apply.
	HE-BO6-S1	*For multiunit PSAs the screening of hazards meets one of the following criteria.* *5) The individual hazards or correlated hazards do not have the potential to cause a multiunit initiating event.* *6) An individual hazard or correlated hazards if subjected to detailed realistic analysis would not make a significant contribution to the selected multiunit PSA risk metrics, e.g. SCDF/SFDF, SLERF, SRCF, or SCCDF.*	*COMMENT: Note that loss of off-site power is example of an initiating event that has a high potential for impacting multiple units concurrently. Hence any external hazard that may cause a loss of off-site power should not be screened out unless Criterion 6) can be applied. It is expected that individual hazards or correlated hazards that can be screened out from the single reactor PSAs using Criteria 1) through 4) would also satisfy Criteria 5) or 6) of this special attribute and so could also be screened out from the multiunit PSA, however the analyst should perform a check to be sure this is the case.*
HE-B07	Confirmatory assessment, reviews, and visual inspections are conducted to support the screening analysis results. Confirmation is made that the SSCs credited for the design basis hazard event or in the estimation of core/fuel damage frequency are actuality designed, installed, and maintained in such a manner that the credit given for them in the screening analysis is justified.		RATIONALE: Experience with detailed PSA of major hazards such as internal fire, internal flood, and seismic has shown that the actual conditions in the plant do not always conform to the expectations from the various documents examined in the course of developing a technical position. It is therefore necessary to field validate the key design inputs that support the screening conclusions.

TABLE 5.2-C ATTRIBUTES FOR HE ANALYSIS: TASK HE-C “CHARACTERIZATION OF HAZARD EVENTS FOR ALL HAZARDS”

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-C	The specific hazard events that are to be considered in the PSA are defined in terms of the parameters and characteristics that will best support the determination of the response of the SSCs to occurrence of the hazard.	COMMENT: These attributes apply generically to all internal and external plant hazards. There are additional attributes that apply specifically to internal fire, internal flood, and seismic (HE-D, HE-E, HE-F) COMMENT: A hazard event is described in terms of the specific levels of severity of impact that a hazard can have on the plant. For example: an internal flood event would be expressed in terms of the specific flood source and its local impact, such as the resulting water levels in affected plant areas, or the extent of the area subjected to spray; a seismic event would be expressed in terms of spectral acceleration and associated spectral shape; a transient event would be expressed in terms of the plant systems affected by the event.
HE-C01	The hazard events are defined in a logical fashion to represent all ranges of possible hazard severities. Identification of hazards includes a review of plant specific experience, plant-unique information as well as a comprehensive review of generic sources.	COMMENT: Some hazards are best suited to the definition of discrete events and others as continuous distributions. Even in cases where a continuous distribution could be developed, the use of discrete points on that distribution will best support modelling and quantification. COMMENT: In practice the ranges of the hazards above certain severity for which all SSCs assumed to fail are included in the single hazard event (e.g. seismic hazard with magnitude >3 PGA). EXAMPLES: Aircraft crash. Aircraft come in various types and sizes. In general it makes sense to create hazard events that combine aircraft that are close in weight, speed, wingspan, and type of operation in order to come up with a set of specific hazard events to analyse. External flooding: Although the severity of external flooding events is clearly a continuous distribution, it is usually most efficient to define discrete events in terms of critical flood heights (the heights at which plant systems are impacted by site flooding; e.g. h1, h2, h3) and define the hazard events in those terms (h1<=HE1<h2, h2<=HE2<h3, h3<=HE3). Heavy Load Drop: These hazard events would be defined as discrete since the items

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		that could be dropped have specific characteristics as to shape, mass, etc. and are specific to the plant operations.
HE-C02	If an established operating basis hazard event or administrative shutdown lower limit below which the facility is not required to shut down for a hazard exists, the lower end of the severity range for defining hazard events in the PSA is established at the severity of the operating basis hazard event or administrative shutdown limit. In the absence of such established limits, an analysis is performed to determine the hazard severity below which a plant trip would not be demanded by the reactor protection system.	RATIONALE: Given the margin inherent in designing for a specific hazard, SSCs would not be expected to have any significant probability of failure at the operating basis hazard event severity or below any administrative limit that would require plant shutdown and inspection. Therefore, the CCDP/CFDP for events of severity below these hazard event severities are not expected to be significantly different than for internal events, and the internal events are expected to have a much higher initiating event frequency.
HE-C03	Where possible, the upper end of the severity range for hazard events is established at the physical limit of the hazard.	EXAMPLES: Aircraft crash: Upper limit cannot exceed the largest aircraft that can potentially hit the plant. External flooding: If the plant is on a lake formed by a dam, upper limit cannot exceed the height of the dam.
HE-C04	If grouping of hazard events is performed, it is performed in a way not grouping together hazards with potentially different effect on the equipment and/or initiating different plant response. Grouped hazard events are bounded by the worst case impacts within the group.	COMMENT: Grouping of hazard events may be useful for frequency calculations and to reduce the number of events to be analysed.
HE-C05	Correlated hazard events are defined by starting with the hazard events for the primary hazard and using a structured process for relating the secondary hazard (whether defined as induced or combined). For each defined hazard event of the primary hazard, one secondary hazard is included in the definition of the correlated hazard event. The severity of the second hazard is limited to only one, which is selected conservatively.	RATIONALE: There needs to be a limit to the added complexity of treating correlated events to focus on those most likely to be important to plant risk. To try to assess all the possible severities of a secondary hazard that could occur as a result of the first hazard event is not warranted given the uncertainties involved and the fact that the frequency of the correlated hazard event will be less than the frequency of the primary hazard event by itself. Similarly, the consideration of combinations of more than two hazards together would be expected to have low enough frequency as to not be worth pursuing. COMMENT: This is perhaps the most difficult task in the hazard PSA process. It is most helpful in this case to prepare a matrix containing all of the defined hazard events shown on one axis and all retained hazards shown on the other. For each

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
			defined hazard event (which will constitute the primary hazard), judge whether it is possible for another hazard to be correlated and define the correlated hazard severity to be considered.
	HE-C05-S1	*Several severity levels are defined for the second hazard based on a conditional probability distribution for the possible severities of the second hazard given the severity of the first hazard.*	*RATIONALE: For certain applications conservative definition of the severity of the second hazard may not provide sufficient risk insights,*
HE-C06	Hazard events (both individual and correlated) are evaluated as to whether they can affect multiple units at the same site.		COMMENT: If it is determined that a hazard event can affect more than one unit, this need to be included in the definition of the hazard event. It may be that this is always the case (e.g. a seismic event) or it may be that it will only occur part of the time (e.g. and aircraft crash would depend on the direction). In the latter case, both single unit and multiunit hazard events would be defined.

TABLE 5.2-D ATTRIBUTES FOR HE ANALYSIS: TASK HE-D ‘CHARACTERIZATION OF INTERNAL FIRE EVENT’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-D	A list of fire events for internal fire hazards is defined for all POSs which is as complete as possible.	DEFINITION: Internal Fire Event is an event brought about by the occurrence of an internal fire, and which directly or indirectly causes an initiating event and may further cause safety system failures or operator errors that may lead to core/fuel damage or large early release. Internal fire events are generally defined in terms of location, fire source, fire rate, oxygen ingress, propagation pathways and potential extent of damage. RATIONALE: Some fire events can only occur during specific POSs, may be more likely, or have a higher heat release rate (HRR) during specific POSs; and this may lead to the need of POS-specific fire event analysis. EXAMPLE: The welding activities that are the significant cause for fires are usually performed during shutdown POSs. Therefore, the conditions for the fire hazard analysis should consider shutdown specific factors, like disabled fire detection, the availability of larger combustible materials, or different fire compartment definition. EXAMPLE: See the NRC NUREG/CR-7114 [35] for how fires may change during shutdown. In general, the following major impacts from the Fire event assessment are observed: 1) Some fires are much more likely during shutdown; 2) Fires may be much larger in HRR; and 3) Plant partitioning affecting the extent of propagation can be much larger. Lesser impacts would be inoperability of fire detection and suppression, which can be maintained at any time for most systems.
HE-D01	Plant specific information required for the internal fire event definition and analysis is collected to support the fire event definitions: a) Cable routes of the plant, including raceways, conduits, trays and barriers; b) Equipment layout in the different rooms; c) Equipment and cable failure modes potentially induced by fire; d) Fire damage criteria; e) Data on fire events;	RATIONALE: Most of the information supporting the internal fire event definitions is plant specific (or equipment specific) and cannot be taken from generic information sources. COMMENT: Not all of this information will be needed for the fire hazard definition; however, the data collection should cover all these items to support the whole PSA. COMMENT: Multiple damage criteria may be established for the same equipment or cables. For example, a simple minimum damage temperature can be used for initial model development and for non-significant fire scenarios, and a more sophisticated time/temperature correlation may be used for significant fire scenarios. All of the

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	f) Human actions in the event of a fire; g) Fire loads in compartments; h) Fire protection procedures.	criteria used need to be justified. COMMENT: Equipment failure modes potentially induced by fire may include failure to operate, fail-as-is, or spurious operation. COMMENT: In the case of PSA for basic design stage of the plant this attribute is not applicable. Apply special attribute HE-D01-S1 instead.
	HE-D01-S1 *In PSA for basic design stage the following information is applied for fire event definition:* *a) Any information available at design stage from the list in HE-D01;* *b) For the missing information realistic assumptions are made and documented. The assumptions may be based on the experience gained in sister or similar plants if they exist.* *OR* *The fire PSA is based on the assessment of the availability of Safe Shutdown Equipment if already declared at design phase,*	*COMMENT: In design stage of a plant the information needed to support the internal fire PSA is not complete or simply not yet available. Any missing information needed to develop the fire hazard definitions are documented in the assumptions, which can later be used in the uncertainty and sensitivity analysis.*
HE-D02	The buildings and structures included in the PSA are defined and are partitioned into distinct physical analysis units that would substantially contain a fire that may occur, so called fire compartments or fire zones, which are examined individually. Fire compartments/zones are characterized by: a) Their physical boundaries (walls, ceilings/floors, doors, dampers, penetrations, etc.); b) The fire protection features , like fire alarms, fire detection and fire suppression systems; c) The fire resistance (fire rating) of the barriers surrounding the compartment; d) The components and cables located inside the fire compartment; e) Adjacent fire compartments;	COMMENT: Cables for non-safety equipment credited in the fire PSA may not be easily routed, especially for Balance of plant equipment such as Feedwater and Condensate. It may also be clear that performing the time-consuming effort to route the cables in detail may provide minimal reduction in the estimated plant fire risk. Assumed routing may need to be performed for this equipment, and documented in the fire PSA. Assumed routing need to be based on plant specific information, taking into account the equipment location, cable end location such as a power supply or control station, and the logical or likely routing for the cable. The Fire PSA should also assume that components that do not have cable routing are failed in their worst possible failure mode. In the context of a PSA for internal fires, a fire compartment could be a well-enclosed room that is not necessarily surrounded by fire resistant barriers, but would substantially contain a fire that may occur (i.e. the separation from other fire

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	f) Ventilation paths (ducts) that may connect the fire compartment to be analysed with non-adjacent fire compartments and their fire dampers; g) The fire load (e.g. type, amount, whether protected or unprotected, location, local distribution and whether permanent or temporary); h) Potential ignition sources (e.g. type, amount, location); i) Procedures for control of combustible material; j) Occupancy level (i.e. the possibility of detection of the fire by personnel); k) Accessibility of the location (e.g. for the fire brigade); The criteria used for the definition of fire compartments are justified and documented.	compartments is represented as separation by distance or by non-rated barriers that would not be subject to a high heat load). COMMENT: Physical boundaries can be stationary passive (e.g. wall), movable passive (e.g. hatch or closed door) and active (fire damper). The probability that the boundary will fail depends highly on the barrier type, number and location of penetrations, and the size/location of a possible fire.
HE-D03	Rationale for the number of hot shorts included in the circuit analysis is justified. The approach ensures that risk significant combinations of equipment involved in spurious operation are included in the fire PSA.	COMMENT: The number of hot shorts considered in the fire PSA circuit analysis can vary, depending on the importance of the equipment and the probability of the hot short.
HE-D04	A list of equipment for each fire compartment is established including equipment required for each POS and/or cables whose fire induced failure, including spurious operation, that may: a) Lead to an initiating event; b) Affect the ability of safety functions to mitigate an initiating event (frontline systems, support systems and control systems), including additional equipment failure identified in the detail circuit analysis such as common power supply failure due to missing or improperly configured electrical overcurrent protective device coordination; c) Affect operator actions after the occurrence of an initiating event induced by a fire (type C human interactions).	RATIONALE: Such an equipment list is necessary to perform the fire impact analysis to evaluate the potential consequences of a fire in the fire compartment. The applicable initiating events for each fire event are identified per the requirements of IE-A. COMMENT: Equipment and cables should include support equipment/cables such as power supplies, interlock circuits, instrumentation, and support systems such as cooling water, HVAC and others. Failure modes for associated cables and circuits should include all significant failure modes, such as inter-cable shorts, intra-cable shorts, multiple shorts to ground, and shorts to ground. COMMENT: Scope of the containment (confinement) function would depend on whether the PSA includes LERF, Large Release or another release metric.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	HE-D04-S1	*A list of equipment for each fire compartment is established including equipment required for each POS and/or cables whose fire induced failure, including spurious operation that may affect containment (confinement) function, such as containment isolation or cooling.*	*COMMENT: This attribute applies to additional containment functions that are beyond those that are required to prevent core/fuel damage.*
	HE-D04-S2	*A list of equipment for each fire compartment is established including equipment required for each POS and/or cables whose fire induced failure (including spurious operation) may lead to a failure of operator actions or result in an undesired operator action that impacts a credited function.*	*COMMENT: See also SA HR-E07-S1*
HE-D05	Raceway fire wraps or other passive fire barrier elements or active fire barrier elements are identified.		

TABLE 5.2-E ATTRIBUTES FOR HE ANALYSIS: TASK HE-E ‘CHARACTERIZATION OF INTERNAL FLOOD EVENTS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-E	A list of flooding events for internal flood hazards is defined which is as complete as possible for all POSs.	DEFINITION: Internal flood event is an event brought about by the occurrence of an internal flood, and which directly or indirectly causes an initiating event and may further cause safety system failures or operator errors that may lead to core/fuel damage or large early release. Internal flood events are generally defined in terms of location, flood source, flow rate, potential spray, pathways and potential extent of damage. RATIONALE: Some floods can only occur during specific POSs, and this may lead to the need of POS-specific flood analysis. EXAMPLE: The system drainage activities are potential causes for internal floods and usually performed during shutdown POSs. Therefore, the conditions for the flood hazard analysis should consider POS-specific factors, like ongoing drainage activities, or human errors during maintenance.
HE-E01	Plant specific information required for the internal flood event definition is collected to support the flood event definitions: a) Possible sources of flooding: pipes, valves, pumps, internal tanks, pools, reservoirs, heat exchangers, connections to open-ended sources (e.g. sea, lake, river), multiunit shared systems or structures, etc.; b) Possible flooding mechanisms for each POS including breaks, leaks, rupture, tank overfilling, spurious or desired actuation of a spray system (e.g. the containment spray system or the fire extinguishing system) or human error during operation or during maintenance related activities (e.g. wrong positioning or inadvertent opening of a valve); c) Characteristics of the flood: capacity (depending on whether the source of flooding is a closed or open system), flow rate, temperature and pressure, presence or possible production of steam;	COMMENTS: 1) Most of the information supporting the internal flood event definitions is plant specific (or system specific) and cannot be taken from generic information sources. 2) Source of flooding may be equipment not associated with safety related or energy production systems. For example, some incidents were originated by leaks in toilets. 3) Not all of this information will be needed for the flood hazard definition; however, the data collection should cover all these items to support the whole PSA. COMMENT: In the case of PSA for basic design stage of the plant this attribute is not applicable. Special attribute HE-E01-S1 need to be applied instead. COMMENT; Characterization includes the flood type, flood size and rate including a range of flow rates, capacity of each source, and the temperature/pressure of each source. These characteristics may vary for each POS (e.g. as the plant shuts down, a steam source may become cooler or not be applicable, depending on the plant condition).

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	d) Flooding related alarms, leak detection systems, capacity of draining systems and flooding related protection for components (such as equipment trip signals); e) Critical flooding heights of components relevant to PSA and room dimensions in the flood compartments.	
	HE-E01-S1 *In PSA for basic design stage the following information is applied for flooding hazard event definition:* *a) Any information available at design stage from the list in HE-E01;* *b) For the missing information realistic assumptions are made, and the assumptions are based on the experience gained in sister or similar plants if they exist.* *OR* *The flooding PSA is based on the assessment of the availability of Safe Shutdown Equipment if already declared at design phase,*	*COMMENT: In design stage of a plant the information needed to support the internal flooding PSA is not complete or simply not yet available, therefore the needed but missing information need to be somehow "created" making assumptions.*
HE-E02	The identification of each flood source includes the propagation path from the source to its potential area(s) of accumulation.	COMMENT: The areas of accumulation may depend on the failure location, and the failure of boundaries or other flood prevention features.
HE-E03	Plant walkdowns are performed to: a) verify the accuracy of information obtained from drawings and other sources of plant information, including the location of SSCs; b) the flood source and location, including flooding pathways; c) to obtain necessary information on spatial interactions for analysis of the damage effects from each potential source of internal flooding, including the effects of spray; d) verify mitigation features located in each flood compartment, such as drains, flood barriers, shields (for spray), etc.	COMMENT: While performing a PSA for a plant in design walkdowns are effective only by the end of plant construction.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-E04	The buildings and structures are partitioned into distinct physical units which will contain the flood events, which are examined individually. Flood compartments are characterized by: a) Their physical boundaries (walls, doors, penetrations, etc.); b) The flood protection features , like flood/level alarms, flood detection and drainage systems; c) The flood resistance of the barriers surrounding the flood compartment; d) The components, including electrical cabinets, located inside the flood compartment e) Adjacent flood compartment and the connections to these areas; f) Ventilation paths (ducts) that may connect the flood compartment to be analysed with non-adjacent flood compartments (potentially important for steam propagation); g) Potential flood sources (e.g. type, maximum amount of water to be released, length of pipelines and volume of tanks, pressure in the system with flood source, location); h) Occupancy level (i.e. the possibility of detection of the flood by personnel); i) Accessibility of the location.	
HE-E05	For multiunit sites flood compartments with shared systems, components or flooding sources are included in the flooding PSA.	
HE-E06	The criteria used for the definition of flood compartments are justified.	
HE-E07	Qualitative screening is performed only for fire/flood compartments or scenarios that have no impact on equipment or operator actions.	COMMENT: Operator response need to be considered here only if the indication is available in the control room and the fire/flood source can be reliably isolated considering both system reliability and operator response. Operator actions need to be proceduralized, with sufficient training, staff and time to ensure the action is highly reliability given the most challenging fire/flood that may occur in the compartment. COMMENT: Fire/flooding mitigation (e.g. mitigation to prevent unacceptable flood

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		levels or isolate ventilation system) typically is not credited in the qualitative screening.
HE-E08	If qualitative screening is applied to reduce the number of fire/flood compartments, then it is performed in a way not screening out fire/flood hazard events with low likelihood, but with potentially significant consequences or fire/flood hazard events with the potential for propagation to other compartments with fire/flood susceptible equipment. The availability of the barriers on the propagation pathways is considered for each POS.	COMMENT: Quantitative or qualitative screening may involve POS specific screening, based on the credited equipment for the POS and status of the barriers. EXAMPLE: During shutdown POSs hermetic doors closed during power operation might be intentionally opened and should not be considered as a barrier for fire/flood propagation.
HE-E09	A list of equipment for each flood compartment is established including equipment required for each POS that may: a) lead to an initiating event; b) affect the ability of safety functions to mitigate an initiating event (frontline systems, support systems and control systems); c) affect operator actions after the occurrence of an initiating event induced by a flood (type C human interactions); d) Affect containment (confinement) function, such as containment isolation or cooling.	RATIONALE: Such an equipment list is necessary to perform the flood impact analysis to evaluate the potential consequences of a flood in each area. COMMENT: Equipment should include support equipment such as power supplies, electrical cabinets, interlock circuits, instrumentation, and support systems such as cooling water, HVAC and others. Scope of the containment (confinement) function would depend on whether the PSA includes LERF, large release or another release metric.
HE-E10	When performing this analysis, POS-specific configurations are taken into consideration	RATIONALE: During shutdown, it is uncommon for flood mitigating features to be in an impaired state. Doors may be propped open, drainage paths blocked, and barriers may be removed. This could result in different, and greater, propagation paths.

TABLE 5.2-F ATTRIBUTES FOR HE ANALYSIS: TASK HE-F ‘CHARACTERIZATION OF HAZARD EVENTS FOR SEISMIC’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-F	The approach to hazard events for seismic is established and the hazard events are defined.	
HE-F01	The characterization of hazard events for seismic has all the attributes of HE-C and the additional attributes of this section	
HE-F02	The approach to the characterization of seismic hazard events uses parameters that allow complete characterization of the hazard event (e.g. peak ground acceleration).	COMMENT: It is most common to discretize the seismic hazard in bins expressed by ranges of zero period peak ground acceleration in the horizontal direction in the free field along with the associated seismic response spectrum. COMMENT: The seismic events are defined as ranges of acceleration of interest starting at the level of interest for the potential onset of damage to the point at which the frequency of the seismic event is low enough that the residual risk contribution is small. Therefore, the seismic event definitions are identical for all POS.
HE-F03	The lower bound severity for the hazard events for seismic is selected such that earthquakes less severe than this are not expected to cause damage.	RATIONALE: Since general plant transients have relatively high frequency, the occurrence of earthquakes that would do no more than cause the plant to shut down (either automatically or manually, for example, an operating basis earthquake, which will lead to automatic or manual shutdown) but do no other damage will not significantly add to plant risk. It could even be argued that earthquakes that only cause loss of off-site power and cause no other damage will also not contribute significantly to overall risk from loss of off-site power, but care must be taken here because recovery of off-site power after an earthquake is unlikely. COMMENT: If the lower bound is set higher than the level likely to cause only a loss of off-site power, it need to be shown that this does not contribute significantly to the frequency of an unrecovered loss of off-site power from other causes.
HE-F04	The severity for the hazard events for seismic is included in the definition of the upper bound seismic hazard event with the severity for which SSCs performing safety functions assumed to be lost (see HE-C01).	COMMENT: The upper bound severity could be associated with a frequency of 1% of internal events CDF/FDF or lower to assure that the overestimated risk above this level could not exceed 1% of CDF/FDF even if the CCDP/CFDP for that severity is essentially 1.0.
HE-F05	The characterization of hazard events for seismic includes correlated events involving the concurrent occurrence of a second external hazard	COMMENT: Seismic events can cause any number of other effects, including tsunami, dam failure, and landslides.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	affecting the site. The correlated events to consider are developed by a plant specific and site specific review.	
HE-F06	The definition of hazard events for seismic includes correlated events involving the occurrence of an additional internal hazard within the plant (e.g. as the result of internal fire or internal flooding). This can be in addition to the second site hazard discussed in HE-C04.	COMMENT: The possibility of internal flooding concurrent with a seismic event is a rather straightforward consideration since each flood source identified in the internal flooding PSA (even if it was screened) can be evaluated as to whether there is a seismic failure mode that need to be considered. The question of seismic induced fire is more complex. Key points to keep in mind are: • An ignition source that does not suffer a functional failure due to earthquake will not cause a fire; • The occurrence of a fire is not certainty if an ignition source is damaged; • Only fires that would add to the earthquake damage are potentially important; • Ignition sources not included in the fire PSA (unique to seismic) would need to be considered. One example could be a storage cabinet containing flammable materials. This would generally not be considered as an ignition source in a fire PSA (although it could be a secondary combustible). A seismic event could cause the cabinet to fall, be damaged, spill flammable material, and ‘self ignite.’ COMMENT: At the time of development of this TECDOC, methods for PSA for seismically-induced internal hazards have not reached an adequate level of maturity to fully meet this attribute.

TABLE 5.2-G ATTRIBUTES FOR HE ANALYSIS: TASK HE-G 'FREQUENCY OF HAZARD EVENTS FOR ALL HAZARDS'

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-G	The specific hazard events that have been defined are analysed to determine their frequency.	COMMENT: These attributes apply generically to all internal and external plant hazards. There are additional attributes that apply specifically to internal fire, internal flood, and seismic (HE-H, HE-I, HE-J).
HE-G01	The determination of the frequency of each hazard event is performed using site specific and plant specific information, except where noted in Fire (HE-H) and Flood (HE-I), which is based on a combination of generic and plant specific data. The information used is current, and relevant to the current design and operation of the plant and to the current conditions around the site.	COMMENT: New facilities or changes to facilities near the plant, changes in transportation patterns, changes to types and schedules for heavy load movements may have an impact on the frequency of hazard event (e.g. comparing to the frequency determined during construction phase or later assessments).
HE-G02	The estimation of the mean frequency and the other parameters considers existing calculations of the mean hazard frequency of the design basis hazard, hazard modeling, and recent site data, as appropriate.	COMMENT: Recent data might include, for example, the annual site maximum wind speeds, aircraft activity in the vicinity, or precipitation data for the site or region.
HE-G03	The determination of the frequency is expressed in terms of a continuous hazard curve or as a series of discrete events, as appropriate.	RATIONALE: The various hazards that may be evaluated are not all suited for the typical approach of a hazard curve because the parameters of interest may not be continuous in nature. EXAMPLES: There are several obvious cases where the use of a hazard curve is not appropriate. ***Aircraft crash***. The parameters of interest are generally mass, wingspan, and speed. These are not continuous, but rather associated with broad general classifications of aircraft (for example, general aviation, small commercial, large commercial, small military, large military). It is most common in this case to establish a representative aircraft that bounds the class in terms of damage potential and to determine the frequency of impact on a class specific basis. This approach would be generally used for all types of transportation accident. ***Nearby facility accident***. An explosion at a nearby facility would also not be expected to have a hazard curve for the overpressure due to explosion. There would be specific explosion sources, and each would have a specific calculated overpressure and a discrete frequency calculation.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-G04	Hazard event frequencies that are determined based on fault tree analysis are developed using the attributes for such analyses from IE-E03 and IE-G01.	EXAMPLE: The determination of the frequency of heavy load drop could be developed by building a fault tree model for the failure of the crane and operator errors that could result in dropping the load on equipment of concern.
HE-G05	Hazard event frequencies that are based on the use of expert judgment are developed using a formal expert elicitation process.	COMMENT: This is necessary in cases where there is insufficient data and also there are no established phenomenological models. One source of guidance on the approach to the use of expert elicitation is NUREG/CR-6372 [36]. Although the details of this document are focussed on seismic hazard, the general guidance on the approach is applicable to any application of expert judgment.
HE-G06	Plant operating state (POS) specific hazard event frequencies are calculated taking into account the fraction of time the plant is at specific POS For multiunit PSAs, hazard event frequencies that are dependent on the combination of POSs are calculated taking into account the probability of the POS combination.	RATIONALE: For the computation of annual average core/fuel damage frequency/large early release frequency it is essential to preserve the total hazard event frequency per calendar year of average plant operation (one full calendar year of experience for one reactor). In order to do this when determining total annual plant CDF/FDF (or LERF), which includes contributions from events occurring during power operation as well as during other plant operating states, the calculation of the contribution for each operating state must account for the fraction of the year that the plant is in that operating state. When the standard activities are not conducted annually (for example, 18 month refuelling schedule) it is necessary to normalize to the average amount of time each year (for example, if there is one 30 day refuelling outage every 18 months, there will be two outages (60 days) every three years, or an average of 20 days each calendar year). EXAMPLES: There are two possible generic classes of hazard event, those that are applicable to all operating states and those that are applicable to only certain operating states. These are handled differently. Assume that the total frequency is calculated as number of observed (or estimated) occurrences/number of years since commercial operation. Case 1 – Applicable to POS Fire in room “X”. This can occur at any time. If the frequency is 0.01/calendar-year, then this must be preserved through all operating states in proportion to the time in that state. If the average availability of the plant is 0.9, then the frequency of the fire for the at-power PSA is 0.009/year, and the remainder would be similarly apportioned to the various non-power states. Case 2 – Applicable to selected operating states. Turbine Missile. This can only occur during conditions considered in the at-power PSA. If the frequency is 1E-5/calendar-

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		year, as it can only occur during power operation the plant availability is inherently included and so the frequency for the at-power PSA is 1E-5/year. The frequency of this hazard for all operating states of the non-power PSA (when the turbine is not operating) is 0, which preserves the yearly total.
HE-G07	Hazards frequencies for external hazards are derived using information collected for the particular hazard in the region around the site or, when not available or sufficient, in the wider regions.	RATIONALE: Historical records for the site might not be sufficient to construct hazard curve with reasonable uncertainties. Therefore, all available sources of information need to be used in the statistical treatment process. COMMENT: The hazard frequency assessment utilizes all available relevant information from governmental records, meteorological local and regional stations, historical records and any evidence available on the occurrence of the events.
HE-G08	Applicability analysis of the data is performed to address changes in site or regional conditions that could impact the hazard frequency. Data found to be inapplicable is either ignored or adjusted for the changes.	RATIONALE: For many external hazards, local changes can affect the likelihood of hazard events. This could include new buildings or cities, canals, and dams. It can also include changes in local operational strategies. EXAMPLE: If a dam was built ten years ago along a river and it is used to control water flow and level, then data on flooding from more than ten years ago would either need to be ignored or calculations would have to be performed to show what the flood level would have been with the dam in place. Similarly, if the river banks had been raised to build a town, resulting in narrowing of the river at that point, similar considerations would have to be included. COMMENT: In some cases the number and extent of changes that would affect a particular hazard are so extensive that adjustment of past data would be virtually impossible. In such cases, detailed analytical models (such as simulations) could be used.
HE-G09	The hazards frequency are verified against observed historical events	COMMENT: Statistical data treatment that is based on available records for relatively short observation time may come up with the hazard curve that predicts extremely low or extremely high frequency for high magnitude events. Verification of such curve against observed events may help to understand the bias and uncertainty of the hazard curve. EXAMPLE: For the NPP site X in 2011 based on statistical records on the 130 years on the level of the river at the site the hazard curve for external floods has been constructed using available records and extreme values distribution type 1. The

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		frequency of the flood event which reaches elevation of 99 m above sea level was shown to be 1E-6 1/year. However, based on the records from 17-th century it was verified that the flood elevation did reach 99 m. This information was used to adjust the hazard curve and derive distributions that produce frequency of the external flood in the range of 1.5E-3 1/year for the flood elevation 99 m.
HE-G08	Whether hazard curve or discrete hazard event frequencies are developed, uncertainty is taken into account.	
HE-G09	Uncertainties in each step of the hazard analysis identified in HE-C and HE-G tasks are propagated and displayed in the final quantification of hazards estimates for the site.	

TABLE 5.2-H ATTRIBUTES FOR HE ANALYSIS: TASK HE-H ‘FREQUENCY OF INTERNAL FIRE EVENT’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-H	Frequency of fire events in individual fire compartments is assessed based on relevant generic industry and plant specific evidence for each POS.	RATIONALE: Frequency analysis of fire events has all of the attributes of HE-G, and the additional attributes of this section. Task described here is related to a Probabilistic Safety Hazard Analysis (PSHA). See references TECDOC-724 [19] and SSG-9 [34].
HE-H01	Estimation of the ignition frequency for fire compartments is performed for fire compartments that survive the qualitative screening (impact screening) process.	COMMENT: The ignition frequency is NOT equal to the fire event frequency. The ignition is the beginning of the process, and analysis taking into account the fire propagation and fire effects should show that it can develop into fire event. For screening purposes at the early phases, the ignition frequency can conservatively be used as the fire event frequency.
HE-H02	The frequency of ignition associated with ignition sources are calculated based on generic fire frequency data updated with plant specific data using a suitable process per the applicable requirements of IE-G. A plant-wide consistent methodology is used to estimate the fire frequency of each fire compartment or scenario using an appropriate apportionment method. A non-zero fire ignition frequency is assigned to all fire compartments for each POS.	COMMENT: Acceptable systematic methods includes for instance: Bayesian updating of applicable generic fire frequencies.
HE-H03	The frequency of ignition accounts for POS specific factors.	COMMENT: Fire frequency is impacted by factors such as the amount of maintenance, occupancy and storage of combustibles. Increases of these factors can result in higher ignition frequencies for both fixed and transient fires. However, normally operating equipment may be stopped during shutdown, resulting in lower fixed fire frequencies for some equipment or equipment types.
HE-H04	The analysis of the fire event frequencies reflects a range of fire intensities and durations that can be used to estimate the probability of the fire event damaging equipment or causing a PSA initiating event.	COMMENT: Fire events most commonly involve a fire event that can vary in intensity and duration. The fire frequency curve used in the PSA should account for the likelihood of the range of intensities and/or duration.
HE-H05	The estimated fire intensities (heat release rates) account for POS specific factors.	COMMENT: Heat release rates for transient fires may be larger during specific POSs due to increased storage of combustibles during or prior to an outage.
HE-H06	Estimation of the fire frequency takes into account potential human errors causing fire during specific modes of operation.	RATIONALE: The possibility of such human errors is different in the different operational modes; therefore, this difference needs to be taken into account.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		COMMENT: Human-induced fires include transient fires and welding cutting, or other “hot work” fires.
HE-H07	Fire frequencies are estimated as a mean with statistical uncertainty intervals for all unscreened fire scenarios.	
HE-H08	Uncertainties in each step of the fire hazard analysis identified in HE-D and HE-H tasks are propagated and displayed in the final quantification of fire hazards estimates for the plant.	

TABLE 5.2-I ATTRIBUTES FOR HE ANALYSIS: TASK HE-I ‘FREQUENCY OF INTERNAL FLOOD EVENT’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-I	Frequency of flood event in individual flood compartment is assessed based on relevant generic industry and plant specific evidence for all POSs.	Frequency analysis of flood events has all of the attributes of HE-G, and the additional attributes of this section
HE-I01	Estimation of the flood frequency for flood compartments is performed either before screening for all flood compartments, or at the beginning of the quantitative screening process for the most important flood compartments that survive the qualitative screening (impact screening) process	RATIONALE: IE-G provides guidance for the use of either generic or plant specific data (depending on the plant specific experience), or more commonly; the combination of generic and plant specific data using a Bayesian process or similar. The requirements from IE-G are supplemented below with flood specific considerations.
HE-I02	The generic information used for flood frequency estimation includes generic plant experience, pipe, tank and other component rupture failure rates. The applicability of the applied generic data sources is justified.	COMMENT: The application of generic data may require the collection and use of plant specific design information, such as pipe lengths and size, operating parameters, and other aspects affecting flooding frequency.
HE-I03	Estimation of the flood frequency takes into account potential human errors during maintenance and testing causing flooding during specific modes of operation.	RATIONALE: The probability of human errors may be different in each operational mode; therefore this difference needs to be taken into account. EXAMPLE: Possible human-induced flooding: – Water hammer events leading to pipe breaks; – Overfilling tanks; – Diversion of flow through openings created to perform maintenance; – Inadvertent actuation of fire suppression system.
HE-I04	If engineering judgement was applied for the estimation of flood frequency, plant specific information is used as the basis for the engineering judgement including data related to human-induced mechanisms potentially leading to flooding.	COMMENT: Plant specific operational experience, design information, and operating parameters need to be considered when estimating frequencies using engineering judgment. For example, operating pressure, temperature and flow rate can be important aspects of both flood frequency and the potential impact.
HE-I05	Flood Frequencies are estimated as a mean with statistical uncertainty intervals for all unscreened flood scenarios.	
HE-I06	Uncertainties in each step of the flood hazard analysis identified in HE-E and HE-I tasks are propagated and displayed in the final quantification of flood hazards estimates for the plant.	

TABLE 5.2-J ATTRIBUTES FOR HE ANALYSIS: TASK HE-J ‘FREQUENCY OF HAZARD EVENTS FOR SEISMIC’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-J	The hazard events for seismic that have been defined are analysed to determine their frequency.	COMMENT: The probabilistic seismic hazard analysis has all of the attributes of HE-G, and the additional attributes of this section
HE-J01	A comprehensive database is established that reflects site specific information on: – Geological, seismological and geophysical data; – Local site topography; – Geotechnical and geophysical site properties; – Location and geometry of all credible earthquake sources in the region and historical data on earthquakes associated with this source, including expressions of aleatory and epistemic uncertainty in the characteristics of each source.	
HE-J02	If available, an existing probabilistic seismic hazard analysis (PSHA) is used. A check is performed of the database (HE-G01) to determine whether any new information about the site seismology or geology since the PSHA was performed.	COMMENT: If there is no new information regarding the site, then the existing PSHA can be used as is. If there is new information, then this information is used to update the PSHA in a way that achieves the other attributes in this section.
HE-J03	All credible seismic sources from the database that could affect the PSHA are incorporated in the update or creation of the PSHA.	
HE-J04	The PSHA addresses: – All credible mechanisms governing estimates of vibratory ground motion that can occur at a site; – Regional and site-specific geological, geophysical, and geotechnical data, and historical, instrumental and paleoseismicity seismicity data (including strong motion data); – Effects of local site response; – Current attenuation models in the ground motion estimates.	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-J05	Uncertainties in each step of the seismic hazard analysis identified in HE-F and HE-J tasks are propagated and displayed in the final quantification of seismic hazard estimates for the site.	COMMENT: Both aleatory and epistemic uncertainty need to be identified, evaluated and included in the analyses (e.g. uncertainties in the seismic source characterization, uncertainties in characterizing the ground motion propagation, uncertainties in the local site response, etc.)

TABLE 5.2-K ATTRIBUTES FOR HE ANALYSIS: TASK HE-K ‘FIRE SCENARIO DEVELOPMENT‘

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-K	Fire scenarios are developed for each fire compartment, including multicompartment fires, based on the impact analysis, and scenario screening is performed.	COMMENT: The development of the fire scenarios is integral with the fire frequency analysis. The ignition source grouping, target grouping, and other simplifications performed during the scenario development will affect the assigned fire frequency.
HE-K01	Impact analysis is performed in order to determine whether the fire affecting the equipment in the fire compartments can cause plant disturbance and/or degradation of safety functions. Impact analysis includes the potential impact on exposed structural steel from large combustible sources, where applicable.	RATIONALE: The impact analysis can significantly reduce the number of fire compartments to be included in the PSA. COMMENT: Impact analysis would include the component/cable failure due to fire or explosion, as well as the impact due to smoke and soot. The impact analysis will also consider the potential impact on manual and automatic suppression. COMMENT: Where exact cable routing has not been established or cables are routed with assumed cable routing the scenario impact should assume damage to these cables in a conservative manner.
HE-K02	The potential multicompartment fires are identified taking into account all possible failures of fire barriers between fire compartments.	RATIONALE: Though the frequency of multicompartment fires may be lower than that of a single compartment fire they may cause more severe consequences, due to a higher number of potentially affected equipment.
HE-K03	Qualitatively screening may be performed for fire compartments, multicompartment fires or scenarios having no impact on equipment in the fire PSA, and do not cause an initiating event. Additional screening criteria for multicompartment fire scenarios can be developed that ensure the contribution of the screened physical analysis unit combinations are of low risk significance.	COMMENT: Screening of an individual compartment should include consideration of the individual compartment screening criteria, and the multicompartment screening criteria. For example, if a fire in a compartment does not affect fire PSA equipment or cause an initiating event, but can spread to another compartment which can affect PSA equipment or cause an initiating event; the compartment does not initially screen qualitatively. COMMENT: Screening criteria for multiple compartment scenarios might consider that the spreading of fires from one compartment to another does not fail additional equipment, including equipment relied on for operator actions, or cause a new initiating event.
HE-K04	Fire scenarios are developed for each un-screened fire compartment, including multicompartment fires, based on the potential damage of the fire. Risk significant fire compartments include those fire scenarios that will characterize the fire risk for the compartment.	COMMENT: Fire scenarios for the main control room should include both abandonment scenarios as well as scenarios leading to loss of function. COMMENT: Where multiple scenarios are identified in a risk significant fire

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		compartment, scenarios should include a range of fire intensities and target damage/impact such that the risk of each significant fire compartment is characterized. The level of detail included in the analysis need to be commensurate with the relative fire risk importance of the fire compartment and scenario.
HE-K05	Grouping of fire scenarios includes group of ignition sources and component targets such that the fire PSA analyses the fire compartment in a realistic manner commensurate with the risk of the fire compartment and fire scenario.	COMMENT: Grouping for fire scenarios involves grouping of fire ignition sources and grouping of targets, in order to simplify the Fire PSA scenario analysis. It is un-realistic to analyse all ignition sources individually, or analyse all target damages as separate scenarios, since this would result in millions of scenarios for a the unscreened fire compartments. COMMENT: The general approach for ensuring risk is accurately characterized is: a) dominate scenarios involve little to no grouping, b) risk significant scenarios involve some grouping, and c) non-risk significant scenarios involve grouped ignition sources and targets without limitation. However, the physical layout and fire characteristics of the scenario are taken into account in the scenario development, which may resulting in grouping being used in dominate and risk significant scenarios. For example, if multiple ignition sources with similar characteristics are the same distance below an important target; then grouping of the ignition sources is reasonable since running separate scenarios would not change the risk results. Grouping may also be affected by the uncertainty in the fire scenario characteristics. Because fire ignition frequencies and fire modelling characteristics can be highly uncertainty, it may be that changing the grouping may improve our fire PSA base results, but significant increase our uncertainty. Thus the simplifications in grouping as well as our simplifications in fire damage modelling take into account the certainty of the modelling, typically with some conservative bias. Therefore, key to the grouping approach is whether changing the grouping will have a significant change in the final Fire PSA results, including CDF/FDF as well as uncertainty.
HE-K06	Dominant fire scenarios are analysed using multiple heat release rates, considering fire growth, steady burning, fire decay, and with multiple fire suppressions times accounting for the likelihood of each influencing factor in the scenario frequency.	RATIONALE: Fire Modelling would include assessment of fire growth, burnout, decay, time to damage, and effectiveness of fire protection/suppression using a multipoint fire intensity model.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-K07	The effectiveness of raceway fire wraps other passive fire barrier elements, or active fire barrier elements credited in the analysis of fire scenarios are evaluated.	COMMENT: Damage to a credited fire barrier due to a high energy event need to be considered in fire scenarios, where applicable.
HE-K08	Factors influencing the fire intensity, timing or extent of the impact for each scenario shall be quantified and incorporated into the plant response model.	COMMENT: Scenario impact should include damage to cables where exact cable routing has not been established, or cables with assumed cable routing. RATIONALE: Detailed fire modelling is typically performed for risk significant scenarios (when the modelling more accurately assesses the timing and extent of damage). Fire Modelling would include assessment of fire growth, burnout, decay, time to damage, and effectiveness of fire protection/suppression.
HE-K09	The effectiveness, reliability and availability of any fire protection features credited in the PSA are evaluated. Dependencies between detection, automatic suppression and manual suppression are evaluated and included in the PSA.	RATIONALE: Credited fire protection features may include detection, suppression, and active fire barriers such as fire dampers or self-closing doors. Review of plant maintenance records is required to ensure the estimated availability of the fire suppression or protection feature is properly assessed in the model. Effectiveness of the fire suppression is demonstrated by ensuring the fire can be detected and suppressed prior to target damage, and there are no impacts from blockages or pocket effects.
	HE-K09-S1 *Fire protection features credited in risk significant fire scenarios are estimated using plant specific availability data.*	
HE-K10	When assessing the effectiveness of fire protection features as part of the impact analysis, POS-specific configurations are taken into consideration	RATIONALE: During shutdown, it is not uncommon for fire protection features to be in an impaired state. Doors may be propped open, suppression systems disabled, and barriers removed or inoperable. This could result in different, and greater, propagation paths.
HE-K11	Severity factors are applied to the risk significant fire event scenario frequencies that represent the likelihood the equipment or cables are damaged without suppression. The severity factors are independent of other factors, such as the non-suppression probability.	COMMENT: Severity factors may not be applicable to all fire frequencies or all scenarios, depending on the data and modelling for the fire event. For example, high energy arcing faults are often times assumed to have a set damage zone, and no severity factor is applied. Additionally, some fire PSA approaches use a single damage zone, given failure or success of automatic and manual suppression, and severity factors may not be applicable to this type of approach. COMMENT: Determination of the severity factor involves estimating the damage

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		criteria of the target, either a set temperature or thermal response (typically used for detailed fire modelling), and represents the fire characteristics (size, growth, decay, etc.) and probability needed to exceed the damage criteria.
HE-K12	Analysis of the damaging fire event frequencies includes the estimation of a non-suppression probability for each fire scenario. Non-suppression includes the consideration of both manual and automatic suppression capability, with dependency accounted for in the analysis, when both are credited.	COMMENT: Non-suppression probabilities are applied when the time to damage is estimated for a given scenario, or when automatic suppression is evaluated as effective in preventing target damage.
HE-K13	The probabilities of developing into a multicompartment fire are assessed, and the frequencies of multicompartment fires are determined. Analysis includes evaluation of factors affecting multicompartment scenarios including factors discussed in HE-K02 to HE-K12 above.	EXAMPLE: The supporting deterministic fire propagation analysis shows, that given failure of a fire barrier forming the border of the fire compartment the developed fire can propagate into the neighbour fire compartment causing a multicompartment fire.
HE-K14	If fire barriers are credited, an evaluation for barrier effectiveness, reliability and availability for each POS is provided.	COMMENT: If a barrier is included in the plant fire protection programme as a credited barrier, effectiveness review is limited to PSA scenarios that potentially exceed the fire rating or damage the barrier, such as scenarios involving a high energy event. COMMENT: If a barrier is included in the plant fire protection programme as a credited barrier, effectiveness review is limited to PSA scenarios that potentially exceed the fire rating or damage the barrier, such as scenarios involving a high energy event. COMMENT: During shutdown, some fire barriers are typically temporarily removed as well as some automatic fire suppression systems being disabled.
HE-K15	If quantitative screening is applied to reduce the number of fire scenarios, fire compartments or multicompartment fires to be modelled in the PSA, then it is applied such that the cumulative risk contribution of screened fire scenarios is small for all POSs.	COMMENT: Based on the fire ignition frequency estimates and the equipment potentially affected by a fire in the fire compartment, the quantitative screening may be performed assessing the contribution of the fire compartment to the core/fuel damage frequency. COMMENT: The quantitative screening does not mean screening out of the analysis It means screening out from further investigations and the estimated CDF/FDF values need to be a part of the final results. RATIONALE: The quantitative screening can significantly reduce the number of

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		fire compartments to be analysed in detail in the PSA. COMMENT: Quantitative or qualitative screening may involve POS specific screening, based on the credited equipment for the POS.
HE-K16	Quantitative Screening does not screen out fire events with low fire frequency, but with potentially significant consequences.	
HE-K17	Include unscreened fire scenarios in the fire PSA plant response model. The model is capable of determining fire-initiated conditional core/fuel damage probabilities (CCDP/CFDPs) and conditional large early release probabilities (CLERPs) for various fire scenarios, and capable of determining the significant contributors to the fire-induced risk for all fire-significant POSs.	COMMENT: The plant response model is constructed consistent with the equipment identified in HE-D03. The fire PSA plant response model includes fire-induced initiating events, both fire-induced and random failures of equipment, fire-specific as well as non–fire-related human failures associated with safe shutdown, accident progression events (e.g. containment (confinement) failure modes), and the supporting probability data (including uncertainty).
HE-K18	Develop the fire PSA plant response model so that systems and equipment that were included in the internal-events PSA but are not included in the Fire PSA and that are potentially vulnerable to fire-induced failure, are failed in the worst possible failure mode for each POS, including fire-induced spurious operation.	COMMENT: The final Fire PSA model should not fail any risk significant equipment failed per this requirement (not credited), unless it can be demonstrated that additional modelling or cable tracing will not impact the results for each POS.
HE-K19	Plant walkdowns are performed to verify the accuracy of fire event information obtained from drawings and other sources of plant information, potential fire impacts, and to obtain necessary information on spatial interactions for analysis of fire propagation from each potential fire source and damage to potential equipment or cables, including equipment/cables in adjacent compartments.	RATIONALE: Walkdowns are necessary to confirm any plant partitioning credited in the definition of fire compartments, as well as to determine the spatial interactions such as the distance between the source and the targets (equipment or cables), location of fire detection/suppression, the potential ignition of secondary combustibles, and other fire event specific information. COMMENT: Separate walkdowns need to be performed at shutdown to support PSA assumptions and modelling for shutdown POSs. COMMENT: While performing a PSA for a plant in design walkdowns are effective only by the end of plant construction.

TABLE 5.2-L ATTRIBUTES FOR HE ANALYSIS: TASK HE-L ‘FLOOD SCENARIO DEVELOPMENT‘

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-L	Flood scenarios are developed for each flood compartment, including multicompartment floods, based on the impact analysis, and scenario screening is performed.	COMMENT: The development of the flood scenarios is integral with the flood frequency analysis. The flood scenario grouping, target grouping, and other simplifications performed during the scenario development will affect the assigned flood frequency.
HE-L01	If grouping of flooding sources was done in the PSA, it was performed in a way not grouping together flooding sources with potentially different effect on the equipment in the flood compartment, and/or initiating different plant response. Grouped flooding sources are bounded by the worst case impacts within the group.	COMMENT: Grouping of flooding sources may be useful for frequency calculations and to minimize the number of flooding events to be analysed.
HE-L02	Impact analysis is performed in order to determine whether the flood affecting the equipment in the flood compartment can cause plant disturbance and/or degradation of safety functions for all POSs. In the impact analysis the following aspects are considered: a) Components affected by internal flooding take into account elevations, barriers, doors and drains. The potential for drain blockages or failure of floor drains (e.g. failure of check valves, piping or seals) is considered; b) The impact of submergence, spray, pipe whip, jet impingement, condensation, humidity, or temperature concerns, including the susceptibility of components to these mechanisms; c) The possibility of floodwater spreading from one area to another is assessed, including consideration of a barrier failure. Barrier failure may include random failure or structural failure due to flooding loads. Justification for barrier effectiveness is provided; d) All possible routes for the propagation of floodwater is taken into consideration for each flooding source; e) The location, including the elevation of cabinets, terminal boxes for cables for safety related components and other sensitive equipment is identified.	RATIONALE: The impact analysis can significantly reduce the number of flood compartments to be included in the PSA. COMMENT: Propagation can occur through a number of pathways, such as through non-rated doors, drains, hatchways, or open penetrations between areas. COMMENT: Operator mitigation may result in preventing damage or limiting the overall damage for the flood. COMMENT: Justification for barrier effectiveness may include the use of qualified barriers, or additional review that shows whether the barrier will delay, restrict, or prevent the propagation of floods to adjacent areas. For Shutdown POSs, barriers may be removed or disabled. COMMENT: Justification for components remaining functional following impact from submergence, spray, etc. need to be justified by test, operational date, engineering analysis or expert judgement using a formal expert elicitation process. COMMENT: Spurious actuations (hot shorts) are not normally considered for flooding PSA, other than the change of state due to loss of electrical power.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	The potential impact of flooding on plant operation is assessed.	
HE-L03	Engineering calculations are performed as needed to determine the flood rate, time to damage susceptible equipment, and the structural capacity of components, structures or compartments.	
HE-L04	For multiunit sites with shared systems or structures, potential multiunit impacts of internal flooding on SSCs and plant initiating events are considered and analyzed. The number and combination of reactor units and related operational modes affected by the flood are identified.	COMMENT: Multiunit impacts may include damage to components shared between plants, components in an adjacent unit credited in the flooding PSA following a cross-tie, or causing a potential initiating event in the adjacent unit.
HE-L05	The flood event with no impact, including impact from flooding, sprays or propagation, can be qualitatively screened out of further investigation.	RATIONALE: A flood compartment may not damage any components/cabinets; however, flood propagation may cause damage to credited components. Therefore screening of the area without proper consideration of flood propagation may lead to omitting of risk significant flood scenarios.
HE-L06	The analysis of the flood frequencies includes the estimation of the probability of developing from flood initiator into a flood affecting the equipment and/or causing a PSA initiating event”.	RATIONALE: The flood frequency includes both the system failure (e.g. pipe break) and failure of mitigation features that result in preventing damage or limiting the overall damage for the flood, as identified in hazard definition for each compartment. Mitigation includes both automatic flood mitigation systems (e.g. drains, detection, barriers, etc.) and manual mitigation features (e.g. operator shutdown of a pump, given an alarm) in the estimation of the flood event frequency.
HE-L07	The probabilities of developing into a multicompartment flood are assessed, and the frequencies of multicompartment floods are determined. Analysis includes evaluation of factors affecting multicompartment scenarios including factors discussed in HE-I02 to I05 above.	COMMENT: The frequency of a multicompartment flood potentially considers additional mitigation that result in preventing damage or limiting the overall damage for the flood.
HE-L08	If flood barriers are credited, an evaluation for barrier effectiveness and availability for each POS is provided.	COMMENT: During shutdown, some flood barriers are typically temporarily removed.
HE-L09	If quantitative screening is applied to reduce the number of flood scenarios, then it is performed in a way not screening out flood hazard events with low flood frequency, but with potentially significant consequences. Quantitative screening is also applied such that the	COMMENT: Quantitative or qualitative screening may involve POS specific screening, based on the credited equipment for the POS.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	cumulative impact of screened flood scenarios is small for all flooding-significant POSs.	
HE-L10	Include unscreened flood scenarios in the flood PSA plant response model. The model is capable of determining flood-initiated conditional core/fuel damage probabilities (CCDPs/CFDPs) and conditional large early release probabilities (CLERPs) for various flood scenarios, and capable of determining the significant contributors to the flood-induced risk for all flood-significant POSs.	COMMENT: The plant response model is constructed consistent with the equipment identified in HE-E. The PSA plant response model includes flood-induced initiating events, both flood-induced and random failures of equipment, flood-specific as well as non–flood-related human failures associated with safe shutdown, accident progression events (e.g. containment (confinement) failure modes), and the supporting probability data (including uncertainty).
HE-L11	Plant walkdowns are performed to verify the accuracy of flood event information obtained from drawings and other sources of plant information, potential flood and spray impacts, and to obtain necessary information on spatial interactions for analysis of flood propagation from each potential source and damage to potential equipment, including equipment in adjacent compartments.	RATIONALE: Walkdowns are necessary to confirm any plant partitioning credited in the definition of flood compartments, as well as to determine the spatial interactions such as the height above the floor for the targets (equipment), location of level alarms, and other flood event specific information. COMMENT: Separate walkdowns need to be performed at shutdown to support PSA assumptions and modelling for shutdown POSs. COMMENT: While performing a PSA for a plant in design walkdowns are effective only by the end of plant construction.

TABLE 5.2-M ATTRIBUTES FOR HE ANALYSIS: TASK HE-M ‘DOCUMENTATION‘

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HE-M	Documentation and information storage is performed in a manner facilitating a peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the methods used, assumptions made, and their bases.	
HE-M01	The following aspects of the hazard event analysis process are documented: **I. Hazard identification, screening, and hazard event definition** - Hazard definition; - The procedure of searching the specific hazards, including: - generic lists of hazards - the analysis performed for searching plant-unique and plant specific hazards; - The approach for assessing the completeness and consistency of hazards with the plant specific experience, industry experience, other comparable PSAs, and generic initiating events; - The process used to identify applicable flood sources; - The qualitative or quantitative criteria for screening out hazards or scenarios; - The list of hazards screened out and screened in; - The basis for grouping and subdividing hazards and resolving whether the hazard events involve single reactor or multiple reactor units; - Documentation of the internal flood plant partitioning and the definition of flooding compartments; - The basis for any plant partitioning analysis in limiting hazard damage; - The basis for defining hazard events; - The plant equipment, including cables, potentially damaged by	RATIONALE: Underlying assumptions for fire scenarios includes the characteristics of the ignition source, characteristics of the damage targets, any applied severity factors, and any applied non-suppression probabilities. Characteristic of target damage includes consideration for target damage criteria, whether generic or plant specific, and damage mechanisms included in each scenario. COMMENT: Determination of the severity factor involves estimating the damage criteria of the target, either a set temperature or thermal response (typically used for detailed fire modelling), and represents the fire characteristics (size, growth, decay, etc.) and probability needed to exceed the damage criteria. COMMENT: Review of plant events will result in the identification and screening of events involving smoke, sparks or heat which are not considered challenging fires. Documentation of the screening process is needed to ensure plant specific fire frequencies are developed consistent with the generic fire data. COMMENT: The list of assumptions and justifications needs to be comprehensive and cover all such assumptions that are used to demonstrate that an attribute has been achieved. This will allow the reviewers and future users to understand the basis of underlying assumptions that drive the hazard event analysis.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	the hazard event; - The cable selection and location process including assumed cable routing and electrical distribution system overcurrent coordination; - The defined plant initiating events analysed in the PSA for equipment damaged from the hazard event. These include both single unit and multiple unit initiating events caused by the hazard events; - Any walkdowns performed in support of plant partitioning or hazard event definition; - The final list of hazard events, and for multiunit PSAs a delineation of whether each initiating event impacts each reactor unit and each combinations of reactor units **II. Hazard event frequencies assessment:** - The model used to evaluate the frequency of each hazard event; - The process for computing the hazard event frequencies that accounts for the fraction of time spent in each POS and for multiunit PSAs, each modelled combination of POS; - The process and results for analysing fire scenarios including supporting information for scenario selection, underlying assumptions, scenario descriptions, and the conclusions of the quantitative analysis - Assumptions related to fire detection, or automatic or manual fire suppression; - Basis for any severity factors, including damage criteria for targets and fire characteristics needed to exceed the damage criteria; - Sources for generic estimates and justification for the choice of particular generic data source(s); - The plant specific data, including the periods, for which plant specific data were gathered for each hazard, and the criteria for	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	screening plant events not included in the plant specific data; - Justification for exclusion of any data; - The rationale for any uncertainty distributions used for frequency estimations; - Estimated frequencies, including the characterization of uncertainty; - Any walkdowns performed in support of hazard event frequency estimates; - Sources of uncertainty related to plant partitioning associated with the hazard, identification and characterization, hazard grouping, frequency estimates, and scenario analysis; - Assumptions made in the analysis and their justification (engineering judgment, specific analysis, statistical information, etc.).	
HE-M02	The sources of model uncertainty and related assumptions associated with the hazard event analysis are documented.	
HE-M03	All the underlying data and information sources and analyses are documented and stored.	

6. PSA ELEMENT ‘IE’: INITIATING EVENTS ANALYSIS

6.1. MAIN OBJECTIVES

The initiating events analysis is a highly iterative, multipurpose task, which provides the basis for the PSA and ensures its completeness. The risk profile can be incomplete and distorted if important initiating events (IEs) are omitted or incorrectly included in the IE groups.

The main objectives of the initiating events analysis are as follows:

- To identify for each POS group a reasonably complete set of the events that interrupt normal plant operation and that require successful mitigation to prevent core/fuel damage, so that no significant contributor to core/fuel damage is omitted;
- To group initiating events to facilitate the efficient modelling of plant response and initiating events frequency assessment while providing sufficient resolution regarding modelling of accident sequences (events included in the same group have similar mitigation requirements, or are bounded by the limiting mitigation requirements for the ‘representative initiating event’ for the group);
- For multiunit PSAs, a systematic method for resolving the impact of each initiating event on each reactor unit and each combination of reactor units considered in the multiunit PSA;
- To provide estimates for the frequencies of the initiating event groups using information available and associated estimation techniques.

Important aspects of the IE analysis are the following:

- Initiating event definition is correct and complete;
- Initiating events are identified taking into account all plant configurations possible at power operation and POSs;
- IEs are grouped in a consistent manner such that any event in the group has the same or less demanding mitigation requirements than initiating event chosen as the IE group representative for further modelling;
- Methods used for the estimation of the IE frequencies are clearly distinguished for the cases when:
  - Estimation is based on plant specific or generic, or both kinds of statistical information
  - Estimation is based on SSC models (mainly refers to system initiators and includes checking system failures and heavy load drops which may create an initiating event)
  - Estimation is based on HRA models (mainly refers to non-power POSs)

  - Estimation for rare events, which is based on expert judgment or use of specific methods (e.g. structural mechanics analysis, etc.)

- Uncertainties in the IE frequencies are understood, evaluated, accounted for, and documented.

6.2. INITIATING EVENTS ANALYSIS TASKS AND THEIR ATTRIBUTES

The main tasks for the PSA element 'IE Analysis' are listed in Table 6.1. Tables 6.2-A through 6.2-G present the description of general and special attributes for these tasks.

TABLE 6.1 MAIN TASKS FOR IE ANALYSIS

Task ID	Task Content
IE-A	Identification of IE candidates (preliminary identification of IEs)
IE-B	IE screening and final IEs list identification
IE-C	IEs grouping
IE-D	Collection and evaluation of generic information for IE frequencies assessment
IE-E	Collection of plant specific information
IE-F	IE frequencies quantification
IE-G	Documentation

TABLE 6.2-A ATTRIBUTES FOR IE ANALYSIS: TASK IE-A ‘IDENTIFICATION OF IE CANDIDATES’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-A	A list of initiating events for internal events, internal hazards, and external hazards for all POS is defined which is as complete as possible.	COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered.
IE-A01	IE definition is clear and covers any plant disturbances that require mitigation to prevent core/fuel damage.	COMMENTS: 1) The following IE definition is generally used: “IE is an event caused by plant equipment failures and/or human errors which could directly lead to core damage (fuel damage) or challenges normal plant operation and requires successful mitigation to prevent core damage (fuel damage)”. 2) The initiating events identified typically include, but are not limited to the following: – Reactivity insertions; – Transients of various types; – Loss of off-site Power; – Loss of coolant accidents (LOCAs), including maintenance induced LOCAs and cold overpressure-induced LOCAs for shutdown POSs; – Interfacing systems LOCAs; – Steam generator tube ruptures; – Support system initiators; – Loss of inventory; – Fuel handling errors; – Spent fuel pool loss of heat sink; – Loss of shutdown cooling and – Heavy load drops. 3) The need to include different types of LOCAs is POS-dependent, e.g. if the reactor vessel head is off, drain down events may be assumed to dominate pipe break LOCAs. 4) On multiunit sites, an accident on another unit that progresses to the point of

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		declaring a general emergency and/or site evacuation, with the potential for release and site contamination need to be considered as a potential initiating event on each unit on the site. This is one way, in which a multiple reactor accident may result from initiating events that only impact a single unit.
IE-A02	All POSs with power and non-power operation are considered together with their interlocks and system configuration. IEs applicable to specific configurations are identified.	RATIONALE: Systems configuration, interlocks and requirements for plant shutdown may be different for the same plant operating on different power levels. This may lead to the appearance of additional IEs and/or to changes in the boundary conditions of the IEs, which were identified for different POS. EXAMPLES: At some plants (e.g. WWER-440 NPPs) the following differences related to POSs exist: 1) Event involving boron dilution due to erroneous connection of a disconnected loop is possible only at a lower than nominal power level. 2) Trip of 3 MCPs leads to reactor scram only at power level below 75% from nominal. 3) Trip of the last operating turbine leads to immediate reactor scram only when the plant operates at power level below 75% from nominal. 4) Plant configuration (in particular secondary side arrangements) differs significantly while the unit operates at 50% and 100% power level (one and two turbines).
IE-A03	A structured, systematic process for identifying initiating events is employed in each POS. The following methods for identification of potential IEs are used: 1) Analysis of lists of IEs from PSAs for similar units: Lists of IEs developed in PSAs for similar units are reviewed in order to identify potential IEs applicable to the investigated unit. 2) Analysis of generic lists of IEs: The lists of IEs from generic sources (e.g. generic lists from IAEA, US NRC, EPRI, etc.) for similar units are reviewed in order to identify potential IEs applicable to the investigated unit.	RATIONALE: Use of only one or a subset of the methods listed in IE-A03 may not provide a complete list of initiating events due to inherent limitations of each method. COMMENTS: 1) For specific applications the use of a subset of the methods may provide a list of IEs sufficient to deal with the application. This should include at least: – Previous PSAs lists for similar units; – Operational experience of the unit under consideration and similar units. 2) IEs are conditional on the POS. Many initiating events for at-power conditions may also apply to POSs with the RCS at high pressure. 3) Special emphasis is placed on review of plant transition POSs (e.g. reducing water

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	3) Analysis of operational experience: Operational experience of the unit under consideration and similar units is reviewed in order to identify events that happened in the past. The experience on plant specific initiating events is reviewed to assure that the list of challenges accounts for the plant experience. Experience and analyses at similar plants are reviewed to assess whether the list of challenges included in the model accounts for the industry experience. 4) Deductive analysis (e.g. master logic diagram, heat balance fault trees, etc.). A step-by step consequential analysis is performed in order to identify events, which could lead to core damage or require mitigation actions. 5) Inductive analysis (e.g. Failure mode and effect analysis). Systematic evaluation of each system is performed to assess the possibility of an initiating event occurring due to a failure of the system, e.g. detailed model of system interfaces including fault tree development and/or failure modes and effects analysis (FMEA) to assess and document the possibility of an initiating event resulting from individual systems/ system train/equipment failures. All systems, which failures may bring disturbance in plant operation (e.g. normal operation, front-line and support systems) are reviewed, with the exception of those, which were already identified as the source of IEs based on other analysis. The analyses are performed after system models were developed. 6) Lists of DBA and BDBA are reviewed.	level to mid-loop for PWRs and hydro testing for BWRs) and maintenance activities (including plant realignments in preparation for maintenance) during shutdown POSs to identify IEs unique to these operating conditions. 4) Special emphasis need to be placed on identifying cases where the loss of a support system can cause the change of state of a component that in turn will result in an initiating event for the specific POS. For example, this can be a result of the failure position of the component on loss of support system being designed to be a safe state for a plant trip from full power, but would cause an initiating event in the non-power POS.
IE-A04	Initiating events resulting from multiple failures in each POS and requiring different mitigation strategy are included, in particular those that can result from a common cause.	RATIONALE: Events, caused by multiple equipment failures may be significant in terms of risk even if the IE frequency is low. See also Table 12.2-D, general attribute DF-D01.
IE-A05	The plant operations, maintenance, engineering, and safety analysis personnel are interviewed to determine if any potential initiating events for any POS have been overlooked. Interview information from similar	RATIONALE: Interview of experienced plant personal may give additional knowledge on real plant behaviour and may help to identify IEs overlooked with the

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	plants is also used.	use of methods listed in IE-A03.
IE-A06	System or equipment failures or combinations of these are screened in each POS to see whether they represent either a unique IE, which needs separate treatment or represent a contributing IE to an IE group. Dependencies between system initiators and post-trip functions need to be identified in this process. All system initiators that at the same time result in safety function failures or degradation are identified.	COMMENT: These types of events are known as common cause initiators or system initiators. A Common Cause Initiator (CCI) is an initiating event (e.g. causing a transient or requiring manual shutdown during plant operation) and at the same time degrading one or more safety functions that may be needed to mitigate consequences of the accident. EXAMPLES: Failure modes, which disrupt normal operation are: - Normally operating pumps: failure to run; - Standby pumps: inadvertent start-up/failure to start; - Safety/relief valves: inadvertent opening; - Normally closed bus breaker: inadvertent opening. Typically, the control and protections systems, electric power supply system, service water system or other support systems are sources for unexpected CCIs, where the plant's transient experience cannot provide information. The following are the main areas for identification of CCIs: Loss of process control. An analysis of the process control includes both measurement and control of process parameters. A large number of parameters exist in the plant, which are used to supervise and control the plant, power, level, pressure, flow, temperature, humidity, etc. Loss of some parameters may cause (or require) a plant trip and functionally degrade one or more safety systems, e.g.: - Erroneous level measurement in the reactor vessel; - Spurious isolation signals. Loss of power supply. Some failures in the power supply which may cause (or require) a plant trip and functionally degrade one or more safety systems, e.g.: - Loss of external power; - Loss of specific AC or DC bus bars. Loss of auxiliary systems. Some failures within auxiliary systems may cause (or

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		require) a plant trip and functionally degrade one or more safety related systems, e.g.: - Loss of instrument air; - Loss of cooling water. Component failures in safety systems. Component failures in safety systems may degrade safety functions, and may also be a requirement for a plant shut-down (Technical Specification rules).
IE-A07	Events caused by operator errors are identified and evaluated.	COMMENT: For power operation usually events caused by operator errors are assumed to be taken into consideration in IE frequencies estimated on the basis of operational experience. However, for certain applications implicit consideration of IEs caused by operator errors may hide the impact of changes in plant maintenance and operational practice. This is particularly important for the common cause initiators because of the potential dependency between the errors associated with the initiating event and those actions required to respond to the event. For non-power POS there are some initiators directly caused by human errors and which frequency is quantified using HRA methods. IEs caused by human failure events are particularly common for events during shutdown. Human failure induced initiating events can be identified by analysing the operating procedures and practices applicable for each POS.
IE-A08	Initiating events caused by equipment damage during refuelling process, heavy load lifting and transportation are considered as hazards induced IEs and are analysed for each POS.	COMMENT: Potential heavy load (e.g. RPV head, spent fuel cask, concrete shielding blocks) drops are analysed in the areas having the potential to damage systems required to perform the safety functions or having the potential to directly result in mechanical damage to fuel assemblies. EXAMPLES: Some plants (e.g. WWER-440) have open areas in the turbine hall where decay heat removal systems are located which are vulnerable to heavy load drops. Particularly applicable for the plants with at-power refuelling (i.e. CANDU, RBMK, AGR, MAGNOX, vessel type heavy water reactor).
IE-A09	Initiating event precursors in each POS and run-back events for power operation modes (also called house-load turbine operation) are reviewed for the purpose of IE identification.	RATIONALE: Review of IE precursors and run-back events may help to identify IEs overlooked with the use of methods listed in IE-A03 and provides a partial basis for quantifying their frequencies

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		COMMENTS: 1) A run-back event is an event, which does not result in a plant trip if plant run-back systems are successful. 2) A precursor for an IE is a kind of trigger event, which alone does not represent an initiating event, but together with other events may cause an IE. A special analysis may be necessary to model these events in the PSA IEs, e.g. an IE event tree. EXAMPLE: Turbine trips, main coolant pump trip, main feedwater pump failure etc. have to be considered taking into account the availability of automatic capabilities, e.g. for power reduction, to avoid a reactor scram.
IE-A10	Events that have occurred during POSs other than the one being examined (e.g. during power operation) are identified and examined on the applicability for all POSs of interest (e.g. for a shutdown POSs).	RATIONALE: The IEs have occurred at different conditions may have a potential to occur during POS considered. These events need to be included in the list of IEs, unless it is justified that the IE cannot physically occur during POS analysed. However, the use of these events in data treatment needs to be made with care.
IE-A11	Administrative (orderly) shutdown caused by different reasons (e.g. failure of single or multiple trains of front-line or support systems) is included in the list of IEs for power operation. These IEs are reviewed in order to avoid double counting in shutdown PSA.	RATIONALE: Administrative shutdown for certain reasons may cause risk significant accident sequences. Exclusion of IEs of this type may hinder certain applications (e.g. those ones dealing with exemptions to TS, justification for continued operation, etc.) EXAMPLE: Administrative orderly shutdown due to requirements of TS (e.g. exceeding the AOT after a failure of the emergency feedwater pump identified at periodical test).
IE-A12	Multiunit site initiators are identified and included in the list of IEs as ‘Multiunits initiators’.	RATIONALE: An IE may be caused by system/equipment failures at another unit at the multiple unit site. These IEs could not be identified with the use of methods listed in IE-A03; however they may be significant contributors to the risk in particular to those multiple units plants with shared equipment and resources (spare parts, repair staff, cooling water, diesel fuel, etc.), .Some dependencies such as shared diesels, switchyards, transformers, heat exchangers, etc. are evident and usually analyzed while performing a PSA. Particularly important are subtle interactions that have the potential to result in the simultaneous unavailability of safety systems at adjacent units following a long term accident. Common cooling water and diesel fuel inventory is of utmost importance. Other important points are the ability to control the accidents occurred simultaneously at several units as well as availability of spare parts and

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		repair staff for several units simultaneously. Allocation of available resources may be a very useful PSA application. EXAMPLE: For the multiunits plant when two or more units share the same building (e.g. turbine hall) IEs occurred at one unit may affect normal operation of the other unit. For a multiunit site, the potential spreading of a hazard like seismically induced fire to other units should also be considered in the analysis. COMMENTS: Multiunits initiators may include the events occurred both at the nearby units and at the unit under consideration. The main feature of these initiators that they affect several units either by causing the disturbance on the nearby unit or by sharing common equipment. The last feature is important for IE grouping task (See Table 6.2-C, general attribute IE-C06). Multiunits initiators are of particular importance when they are caused by external or internal hazard events, or by failures in any common support systems.
IE-A13	The events dealing with failures of individual support systems (or trains) that can cause a plant trip are included in the list of IEs for power operation POSs.	COMMENT: Failures of support system train(s) that may cause an initiating event at-power need to be included in the IE list in addition to the failure of the whole system. If only the failure of the whole support system is included in the IE list as a single most conservative event, the frequency of such events may be underestimated.
IE-A14	In identification of initiating events, temporary alignments during maintenance, that could either influence the likelihood that failures cause an initiating event, or could increase the severity of the effect on plant safety functions that would result from such an event are accounted for each system.	RATIONALE: These routine but temporary alignments are very common and very important during shutdown and may be associated with IEs caused by human failure events or related to different boundary conditions imposed by the temporary alignments.
IE-A15	Each internal and external hazard event that was defined under HE-C through HE-F is related to one or more of the identified initiating events that can result from the occurrence of the hazard event. If the hazard event cannot be related only to the initiating events identified through the other attributes in IE-A, then additional initiating events are defined.	COMMENT: The use of "initiating event" in this attribute could refer to an individual initiating event or an initiating event group, as appropriate. Consideration of the relationship between the hazard and the initiating events may require that an initiating event group be re-defined in order to properly address the hazard. COMMENT: In general, it is expected that most hazard events can be related to the internal initiating events identified.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		EXAMPLES: - Fires can cause reactor trip, loss of off-site power, support system transients, various size LOCAs, etc., but in general do not cause unique initiating events. Seismic events, on the other hand, can cause initiating events not covered in the internal events analysis and that cannot be modelled using just the internal initiating events; - Collapse of the turbine building from a seismic event could result in simultaneous main steam and feedwater line breaks that are not bounded by either of the individual internal events). COMMENT: The correspondence of hazard event to initiating event may not be one-to-one. The analyst must consider that there may be a conditional probability that the hazard event may lead to different initiating events. EXAMPLE: A particular fire event may lead to loss of off-site power, but there may be a conditional probability that it leads to a primary PORV LOCA due to a hot short. COMMENT: The PSA should initially assign the identified initiating event conservatively, and provide refinement in the identified initiating events for significant scenarios. The PSA should not overly simplify the identified initiating events (e.g. all scenarios involving a specific hazard are assumed to be a single or small group of initiating events). COMMENT: The potential list of IEs caused by a hazard event generally includes most of the internal events IEs, unless the IE cannot be caused by the hazard event. A simplified IE approach assuming a reactor trip followed by hazard-induced loss of a system in place of analysing the IE (e.g. reactor trip followed by loss of component cooling water versus loss of CCW IE) should not be used unless the simplified approach results in no significant impact on the hazard event PSA results. COMMENT: The modelling of the relationship between the hazard event and the initiating events can be done in more than one way. The conditional probability of each initiating event given the hazard event can be calculated directly and combined with the hazard event .frequency to determine the hazard-induced initiating event frequency. Alternatively, it can be handled within the systems logic by modelling the initiating events as consequential failures following a hazard-induced reactor trip.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		Either approach will work as long as the Boolean logic and frequency is properly preserved and there are ways to extract the contribution of each initiating event from the results.
IE-A16	Detailed impact analysis is performed in order to determine what kind of initiating event is caused by the SSCs affected by the hazard.	COMMENT: For most hazards, the impact analysis will focus only on loss of function for a piece of equipment. However, certain hazards can result in spurious equipment actuations, most notably internal fires, but also possibly in seismic (due to relay chatter). Other hazards may also have the possibility of such effects. COMMENT: This attribute is applicable only to PSA of hazards.
IE-A17	Where a particular hazards event can cause several initiating events defined in the internal events PSA simultaneously, the most severe initiating event from the standpoint of success criteria is used as the representative initiating event and the other events are treated as consequential failures.	EXAMPLE: The same fire could cause both a small LOCA (through spurious opening of a head vent valve, for example) along with a loss of AC power (through damage to AC power or control circuits. In this case, the fire-induced initiating event is a small LOCA (because the plant response to mitigate the event is more restrictive. The additional loss of AC power is a consequential failure that will be handled by the system logic models of the support systems. The question is what initiating event needs to be taken as consequence of the hazard.
IE-A18	Include potential initiating events resulting from fires in the main control room, including fires that result in a loss of function or lead to a control room abandonment	RATIONALE: The special effects of a fire in the main control room have to be included into the fire PSA taking into account the specific features associated with this location. Specifically, the initiating event in this case may be either loss of function or abandonment of the control room due to habitability when the actual damage caused by the fire would not cause any equipment failures that would cause plant trip.
IE-A19	For multiunit PSA there is a separate list for initiating events that may impact two or more reactor units concurrently.	

TABLE 6.2-B ATTRIBUTES FOR IE ANALYSIS: TASK IE-B ‘IE SCREENING AND FINAL IES LIST IDENTIFICATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-B	All the identified events for internal events, internal hazards and external hazards for all POS are subject to a screening analysis in order to screen out events not applicable for the unit under consideration and compile a final list of IEs.	COMMENT: Attributes related to screening under IE-B are not applicable to hazard PSAs, as the relevant screening should already be performed under the task of definition of hazards. COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered
IE-B01	The events are screened out from the list of IEs and eliminated from further consideration only if compliance with one of the following criteria is justified: a) The event does not lead to the IE as defined in the PSA. b) The event does not correspond to the scope of the PSA. c) The frequency of the event is less than the truncation value related to the accident sequence frequency, and the event does not involve an ISLOCA, containment (confinement) bypass, or reactor pressure vessel rupture. For these events the truncation value is at least one order of magnitude lower than the truncation value accepted in the PSA. d) The resulting reactor shutdown during at-power POS is not an immediate occurrence. That is, the event does not require the plant to transfer to shutdown conditions until a defined amount of time has elapsed, the condition is detectable before plant systems are required to respond, and there, is a high degree of certainty (based on supporting calculations), that the condition can be detected and corrected before normal plant operation is curtailed (either administratively or automatically).	RATIONALE: The events should not be screened out if a potential for a high Level 2 contribution is recognized. COMMENT: There are various means to implement item d. One approach would be to establish a bounding probability of failure of the operators to detect and correct the problem, with consideration of the difficulty of correction, and show that the resulting initiating event frequency is low.
	IE-B01-S1 *Events with frequency below the truncation value are revisited in the screening process and retained in the list of IEs to identify a wider range of possible hazards.*	*EXAMPLE: Changes in plant test and maintenance practice may impact the frequencies of these IEs. Exclusion of IEs of this type may mask their potential importance for certain applications.*
IE-B02	IEs, the frequencies of which need to be assessed by FT modelling or other reliability methods, are identified (e.g. support system failures,	RATIONALE: Fault tree (reliability) modelling allows properly taking into account support or auxiliary system dependencies and comprehensively accounting for

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	CCI, failures of lifting equipment, etc.).	different causal mechanisms to estimate IEs frequencies.
IE-B03	Potential cases of double counting of initiating events to be analysed in both internal event PSA and hazard analysis are avoided.	EXAMPLE: Feedwater line ruptures are usually considered as a potential flooding mechanism. In this case the events need to be excluded from the internal event PSA if they are considered in the internal hazard PSA model or internal event PSA model need to be re-developed and re-quantify to incorporate flooding consequences. Another example of flood mechanisms is ruptures of service or circulating water pipes. Internal (fires) and external hazards can be implicitly taken into consideration in the definition of internal initiating events such as loss of off-site power or loss of the grid. However, when the IEF are evaluated as a part of a hazard PSA, the frequency estimation need to be revised and duration analysed to remove contributions to the internal events PSA frequency.

TABLE 6.2-C ATTRIBUTES FOR IE ANALYSIS: TASK IE-C ‘IE GROUPING’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-C	IEs are grouped in separate groups with similar mitigation requirements for all IEs in the group in order to facilitate an efficient, but realistic estimation of the CDF/FDF. The different IE groups are characterized by different impacts on plant performance, safety functions, single vs. multiple reactor impact, and possibilities for recovery.	COMMENT: IEs are grouped in a separate group if it is important for a specific application.
IE-C01	A structured, systematic process for grouping the initiating events is used. The accident progressions and success criteria are identified for each of the IE (available thermal hydraulic analysis and expert judgment are used). (See also Sections 7 and 8).	RATIONALE: Grouping can be performed only based on similarity of the accident progression and success criteria of all the events included in the group.
IE-C02	Grouping of initiating events is justified.	RATIONALE: Meeting of the required conditions ensures that any specific feature of the IE included in the group was not treated in an optimistic manner and therefore no potential insights of the PSA are overlooked. COMMENTS: It is recommended that Initiating events are grouped in a single group only when the following can be assured: - Events have the same safe and unsafe end states and lead to a similar accident progression in terms of the plant response, success criteria, timing, and the effect on the operability of relevant mitigating systems and operators performance; or - Events can be subsumed into a group and bounded by the worst case impacts within the ‘new’ group Events that involve multiple reactor units a separated from those that impact single reactor units in a manner that avoids double counting. COMMENT: 1) Those IEs that have significantly different environmental impact or could have a more severe radionuclide release potential are grouped separately from other initiating event categories. EXAMPLE: Such initiators as interfacing systems LOCA, SG tube ruptures, high-energy steam line breaks outside containment (confinement) are usually modelled as a

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
			separate groups. 2) A grouping valid for one POS may not be appropriate for another POS.
	IE-C02-S1	*IE with a relatively low frequency, but more severe accident progression and more demanding success criteria (comparing to the other IEs in the group) is included in a separate IE group.*	*RATIONALE: For certain applications a more realistic representation of the plant response is required.*
	IE-C02-S2	*If the signals for actuation of at least one mitigation system are different for different IEs, these IEs are included in separate groups.*	*RATIONALE: For certain applications a more realistic representation of the plant response towards IEs with different signals for systems actuation and operation is important.* *EXAMPLE: SLOCA and pressurizer steam leak may have different signals for actuation of HPECC pumps (e.g. low pressure and low level in the pressurizer for SLOCA and only low pressure in the pressurizer for a pressurizer leak).*
IE-C03	IEs are included in separate groups if different operator actions or conditions for operator actions in terms of information available, time windows, environmental conditions, and procedural requirements exist.		EXAMPLE: Events requiring ISLOCA isolation need to be considered separately for each ISLOCA path if different isolation possibilities are available.
IE-C04	Plant specific thermal hydraulic analyses supporting accident sequence modelling and success criteria definition for the representative IE in each group are performed. In case the success criteria for frequent events included in the group are much less severe than success criteria for the representative IE, the events are grouped differently.		RATIONALE: This attribute helps to avoid excessive conservatism.
IE-C05	Each single unit common cause initiator and each multiunit common cause initiator are considered as a separate group.		RATIONALE: Grouping of this type of events could mask the insights for certain applications.
IE-C06	'Multiple units initiators' affecting systems/equipment shared among several units are considered as separate groups.		RATIONALE: The capacity of mitigation systems and resources availability may be significantly different when more than one unit are affected by the IE (see IE-A12).
IE-C07	The IEs, for which the strategy of accident mitigation depends on the place of their origination (e.g. different possibilities for leak isolation or different impact on operation of other equipment), are considered in		EXAMPLES: 1. For some plants, where LOCA isolation is possible, LOCA in isolable and non-isolable parts can be considered.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	separate groups unless the impact is bounded by the worst-case location.	2. For steamline breaks outside and inside containment (confinement), the environmental conditions important for operation of other equipment may be significantly different.
IE-C08	A list of IE groups is compiled. Representative IEs for further modelling of each IE group are selected. The strictest features in terms of accident progression and success criteria of an IE included in the group are assigned for the representative IE.	COMMENT: The hypothetical IE that combines the worst success criteria of all IEs in the group may be constructed for further analysis.

TABLE 6.2-D ATTRIBUTES FOR IE ANALYSIS: TASK IE-D ‘COLLECTING AND EVALUATING GENERIC INFORMATION FOR IE FREQUENCIES ASSESSMENT’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-D	Generic information required to perform the internal events IE frequencies assessment for all POS is collected. Generic information is evaluated regarding its applicability. Applicable generic sources are selected for each IE/IE group.	COMMENT: Generic information is needed when plant specific data is not available, as well as for the purpose of Bayesian updating. COMMENT: If the scope of the PSA does not include LPSD POS, then these do not have to be considered
IE-D01	Generic information required for the IE frequency estimation is collected in order to account for a broader experience. While doing this: a. The sources of generic data and the process of the derivation of generic IE frequencies estimates are identified and described. The IE definitions and boundary conditions are evaluated in the view of consistency with the events determined in the IE Screening and the final IE List Identification. b. Generic information is traced to the primary source to avoid inadvertent double counting of information and assure that no information from the plant is contained in the generic information. This is important from the viewpoint of consistent Bayesian updating.	RATIONALE: Applicability of data from plants of different design need to be investigated and boundaries of the IEs in the generic source need to be compared with plant specific IEs boundaries COMMENTS: For example the following generic information data is required: a) Number of IEs versus plant operational time; b) Frequencies of IE for rare events; c) Description of the methods used and conditions under which generic information was obtained; d) Unit type where data came from (i.e. plant design); e) IE definition and boundary conditions in generic sources; f) POS to which IE recorded is related.
IE-D02	The collection and evaluation of generic information include an understanding and assessment of the applicability and uncertainty in the original data.	RATIONALE: Information on the uncertainty of generic data supports the decision on the applicability of the generic data for Bayesian updating with plant specific data.
IE-D03	The generic information collected is evaluated in order to identify the information applicable for a specific IE and/or IE group.	RATIONALE: In case applicability of generic data to the plant specific IEs is not justified, special consideration need to be given to the possibility to apply the Bayesian updating process.

TABLE 6.2-E ATTRIBUTES FOR IE ANALYSIS: TASK IE-E ‘COLLECTING OF PLANT SPECIFIC INFORMATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-E	Plant specific information required to perform IE frequencies assessment for internal events, internal hazards, and external hazards for all POS is collected in accordance with the IEs lists described in the attributes of the task IE-B and IE grouping outlined in the attributes of IE-C.	COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered
IE-E01	Plant specific operational information in accordance with the IEs lists referenced in the attributes of the tasks IE-B and IE-C is collected.	RATIONALE: Plant specific events are collected in order to provide information, which is plant specific and reflects plant design and operational features.
IE-E02	The database containing information on events and plant operational history is created and plant specific information is collected.	COMMENT: Duration of a POS may be important for estimation of frequencies of the IEs of certain duration (i.e. LOOP IE). COMMENT: The following is an example of the type of information to be collected in the database. - Number of IEs for each IE group; - Number of precursors for the IEs; - Number of run-back events; - POS data; - Duration of IE (e.g. for off-site power); - Time period of data collection; - Description of the event.
IE-E03	When system/reliability models for initiating events frequency assessment are used, the appropriate system/component information is collected.	
IE-E04	When collecting information for internal hazards and external hazards initiating event assessment, the information required to assess the fragility/damage criteria for SSCs for the hazard is collected (see also DA-G).	

TABLE 6.2-F ATTRIBUTES FOR IE ANALYSIS: TASK IE-G ‘IE FREQUENCIES QUANTIFICATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-F	Frequency of individual IE and/or IE group for internal events, internal hazards and external hazards for each POS is assessed based on relevant generic industry and plant specific evidence. Where feasible, generic and plant specific evidence is integrated using proven methods to obtain plant specific IE frequency estimates. IE frequency estimation is accompanied by a characterization of the uncertainty.	COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered
IE-F01	Initiating event frequencies are calculated taking into account the fraction of time the plant is at a specific POS, usually on a “per calendar year” basis. In other words, the initiating event frequency assigned to a particular POS takes into account both the expected hourly rate of occurrence of the initiator while in a particular POS and the duration of the POS. For demand based IEs, the frequency in an average year that each POS is entered is accounted for. For single reactor unit PSAs, frequencies are estimated on a reactor calendar year basis, whereas for multiunit PSAs, frequencies are estimated on a site calendar year basis.	RATIONALE: When initiating event frequencies are calculated on a “per calendar year” basis, the core/fuel damage frequencies calculated for different POS are additive: the total core/fuel damage frequency is the sum of the core/fuel damage frequencies of the relevant POS. For multiunit PSAs, quantifying the initiating event frequencies on “per site calendar year” basis accomplishes the same objective.
IE-F02	Realistic IE frequency estimates are calculated using Bayesian updates where feasible. Prior distributions are selected as either non-informative, or representative of variability in industry data.	
IE-F03	For rare initiating events, the industry generic data is used with account for plant specifics.	RATIONALE: Use of Bayesian updating with zero plant specific statistics need to be performed with care in order to avoid double counting of the exposure time potentially accounted in industry generic data. COMMENT: ‘Rare event’ is an event that might be expected to occur once or a few times throughout the world nuclear industry experience.
IE-F04	For extremely rare initiating events an engineering judgment is used, augmented with applicable generic data sources and specific analysis (e.g. fracture mechanics methods, etc.).	RATIONALE: Use of any statistical analysis methods (i.e. the Bayesian updating) could not produce useful results for the ‘extremely rare’ events due to practical absents of statistical information. COMMENT: ‘Extremely rare event’ is an event that would not be expected to occur even once throughout the industry experience.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-F05	Generic and plant specific data are used in a justifiable manner. When the Bayesian approach is used to derive a distribution and mean value of IE frequency, the check is made that the posterior distributions derived are justified given the prior distributions and the plant specific evidence.	COMMENT: If the estimator for the mean value of a parameter based on plant evidence is outside of a 95% confidence interval around the median value of the prior distribution the applicability of that particular prior data and distribution need to be reconsidered regarding its applicability to the initiating event under consideration.
IE-F06	While using system models or HRA for initiating events frequency assessment: the system models or HRA computational methods are modified in such a way that the top event quantification produces a failure frequency rather than a top event probability as normally computed. When developing the system model the following aspects are taken into account: All relevant combinations of events involving the annual frequency of one component failure combined with the unavailability (or failure during the repair time of the first component) of other components are captured. - Probability of spurious actuation of the equipment and CCFs are considered and accounted for; - Spurious actuation of the equipment and passive failures not considered in the PSA model are included in the model; - Support system failures are included in the model (unless the support system is an own initiator); - Pre-accident human errors are included in the model; - Impact of nearby units is accounted for.	COMMENT: Standard fault tree quantification model provides estimation of probabilities over a specific time frame, but not frequencies RATIONALE: This attribute helps to avoid underestimation of IE frequencies for the IEs treated with the use of FT modelling technique. COMMENT: It is important to correctly model in FTs the following aspects of system operation: – Possibilities for recovery of the redundant equipment; – Mission time corresponding to actual system (component) operating time within a year, including CCF (e.g. 8000 h instead of 24 h used in the accident sequences analyses), etc.
IE-F07	Each likely system alignment or plant condition that could influence the likelihood that failures cause an initiating event, or magnify the severity of the challenge to plant safety functions that would result from such an event is accounted for in the PSA.	RATIONALE: Realignment of the equipment may lead to increase of the frequency of system failures causing the IE. EXAMPLE: At some plants during test of Reactor Protection System one system train is out of operation. During this period the system configuration (2 out of 3) changes (1 out of 2), which may lead to a significant increase in the frequency of spurious actuation of the reactor scram.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-F08	In the ISLOCA frequency analysis, those features of plant and procedures that could significantly influence the ISLOCA frequency are accounted for.	EXAMPLE: Absence of test possibility for one check valve in the sequence of two leads to a significant increase in the frequency of the ISLOCA event due to a high probability that the second check valve is in the failed state.
IE-F09	The frequency of IEs, for which the strategy of accident mitigation depends on the place of their origination (e.g. different possibilities for leak isolation or different impact on operation of other equipment), is estimated for the specific location taking into account geometrical characteristics of the NPPs pipelines.	EXAMPLES: 1) For some plants, where SLOCA isolation is possible, SLOCA in isolable and non-isolable part can be calculated by partitioning of the total frequency taking into account the length of the pipelines before and after the isolation valve. 2) For steam lines breaks, the frequency of the IEs occurred inside and outside containment (confinement) can be calculated by partitioning of the total IE frequency taking into account the length of the pipelines inside and outside containment (confinement).
IE-F10	Plant specific information is used in the assessment and quantification of recovery actions where available for IE frequencies estimation. These recovery actions are clearly defined in order to avoid double crediting in IE frequency assessment task and accident sequence modelling task.	RATIONALE: Use of generic information for quantification of the recovery action for IE frequency estimation may introduce excessive optimism/conservatism in the results due to non-accounting of plant specificity: 1) Absence/availability of relevant procedures. 2) Technical possibility for recovery action. 3) Plant-dependent time margins for the recovery actions. EXAMPLES: 1) Recovery action for closure of pressurizer safety valves after spurious opening is dependent on the actual cause of spurious opening and design of the control circuit of the valve. 2) Recovery of the off-site power is dependent on the site-specific external grid characteristics.
IE-F11	The results of the initiating event analysis are compared with generic data sources to provide a reasonableness check of the quantitative and qualitative results. The deviations from generic sources are resolved and/or explained.	COMMENT: If the estimator for the mean value of a parameter based on plant evidence is outside of a 95% confidence interval around the median value of the prior distribution the applicability of that particular prior data and distribution need to be reconsidered regarding its applicability to the initiating event under consideration.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-F12	Detailed fragility/impact analysis is performed in order to determine the probability of developing of the hazard into a PSA initiating event.		RATIONALE: The hazard itself is not an initiating event. It has to develop into an initiating event defined by the PSA in order to challenge the plant safety functions, and so there is a conditional probability that a given hazard event will result in a given initiating event (or events). This is usually evaluated by developing a logic model for the SSC failures that can lead to the hazard-induced initiating event and quantifying that model. Once this probability is determined, the hazard frequency determined under the task of hazard frequency quantification as discussed in HE-G, HE-H, HE-I and HE-J need to be multiplied by this probability to quantify the frequency of the hazard induced initiating event COMMENT: This attribute is applicable only to PSA of hazards.
	IE-F12-S1	*The detailed impact analysis for fire initiating events includes deterministic fire propagation calculations using qualified computer codes in order to reduce the unnecessary conservatism of the associated assumptions.*	*COMMENT: The reduction of the conservatism in the fire PSA enables specific applications (like risk informed fire protection)*

TABLE 6.2-G ATTRIBUTES FOR IE ANALYSIS: TASK IE-H ‘DOCUMENTATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-G	Documentation and information storage is performed in a manner facilitating a peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the methods used, assumptions made, and their bases.	
IE-G01	The following aspects of the initiating event analysis process are documented: **I. IE identification and grouping:** – IE definition; – The procedure of searching the specific initiating events, including: ○ Generic lists of IEs ○ The analysis performed for searching plant-unique and plant specific initiators ○ The approach for assessing the completeness and consistency of initiating events with the plant specific experience, industry experience, other comparable PSAs, and generic initiating events; – The rationale for screening out initiators; – The list of IEs screened out and screened in events; – The basis for grouping and subdividing initiating events including the basis for delineating multiunit initiating events; – The assumptions made to identify, screen out, and group IEs; – The list of IE groups and particular IEs assigned to the IE group; – A list of IE groups and particular IEs associated with each POS for each internal and external hazard. **II. Frequencies assessment:** – The model used to evaluate the frequency of each IE; – The process for computing the initiating event frequencies; – Sources for generic estimates and justification for the choice of	COMMENTS: - IEs frequencies mean, median, 5% and 95% percentile need to be assessed and documented. - Aging of the plant need to be investigated for time trends.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	particular generic data source(s); – The plant specific data, including the periods, for which plant specific data were gathered for each IE; – Justification for exclusion of any data; – The rationale for any distributions used for frequency estimations; – Estimated frequencies, including the characterization of uncertainty; – Potential time dependent aspects of the initiating event frequencies; – Key assumptions made in the analysis and their justification (engineering judgment, specific analysis, statistical information, etc.).	
IE-G02	The sources of model uncertainty and related assumptions associated with the initiating analysis are documented.	
IE-G03	All the underlying data and information sources and analyses are documented and stored.	
	IE-H02-S1 *The information from the IE analysis including the IE databases created is part of the PSA documentation. These data including the databases and the detailed background information is stored in a retrievable and accessible electronic form and format. Due to the amount of information arising from the IE analysis tasks electronic storage of this information is essential for many of the applications.*	*COMMENT: Electronic storage of IE database is essential for many applications.*

7. PSA ELEMENT 'AS': ACCIDENT SEQUENCE ANALYSIS

7.1. MAIN OBJECTIVES

The objective of the accident sequence (AS) analysis is to ensure that the response of the plant's systems and operators to an initiating event is reflected in the assessment of CDF/FDF in such a way that:

- Significant operator actions, mitigation systems, and phenomena that influence or determine the course of sequences are appropriately included in the accident sequence model and sequence definition;
- Plant specific dependencies due to initiating events, human interfaces, functional dependencies, environmental, and spatial impact, and common cause failures are reflected in the accident sequence structure;
- The individual function successes, mission times, and time windows for operator actions for each critical safety function modelled in the accident sequences reflects the success criteria evaluated in accordance with the attributes of Section 8 of this publication;
- End states are clearly defined to be either core/fuel damage[7] on one or more reactor units or successful prevention with the capability to support the interface between Level 1 and Level 2 PSA;
- The accident sequences are defined for the selected set of initiating events, POSs, and times that a POS can occur.

The important aspects of AS analysis are the following:

- Clear definition of success and non-success end states;
- Comprehensive list of key safety functions and systems performing the functions;
- Realistic accident progression identification;
- Clear presentation of AS models;
- Completeness of AS models;
- Justification for end states for all ASs.

7.2. ACCIDENT SEQUENCE ANALYSIS TASKS AND THEIR ATTRIBUTES

Table 7.1 lists the main tasks for the PSA element 'AS Analysis'. Tables 7.2-A through 7.2-E present the description of general and special attributes for these tasks.

[7] Although this publication is intended for light water reactors, most of the concepts and attributes are applicable to other reactor designs. For that reason it is worth noting here that for certain plant designs the concept of core/fuel damage as applied to light water reactors may not be applicable (e.g. reactors with homogeneous core or High Temperature Gas Cooled reactors). In such cases the term core/fuel damage should be replaced by an appropriate definition of "undesirable consequences" that is applicable to the reactor design.

TABLE 7.1 MAIN TASKS FOR AS ANALYSIS

Task ID	Task Content
AS-A	Selection of a method and provision of related tools for accident sequences modelling
AS-B	Definition of success and non-success end states and key safety functions
AS-C	Accident sequences progression identification and as models development
AS-D	Accident sequence success criteria definition
AS-E	Documentation

TABLE 7.2-A ATTRIBUTES FOR AS ANALYSIS: TASK AS-A ‘SELECTION OF A METHOD AND PROVISION OF RELATED TOOLS FOR ACCIDENT SEQUENCES MODELLING’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
AS-A	The task includes the selection of a method and provision of related tools for accident sequences modelling.	
AS-A01	The method chosen for accident sequence analysis provides for the possibility to explicitly model the appropriate combinations of system responses and operator actions that affect the key safety functions, accounting for changing plant conditions within a POS, for each modelled initiating event /IE group and provides a framework to support sequence quantification. The method supports graphical representation of the accident sequence logic (e.g. ‘event tree structure’).	RATIONALE: Graphical representation of the AS logic provides for the possibility to analyse and review AS models. This feature is of high importance for a number of applications. COMMENT: The accident sequence analysis need to be valid for the range of plant conditions within the POS.
AS-A02	For multiunit PSAs, in addition to the accident sequences already available from the single reactor PSAs, the method provides the capability to model the different possible responses to initiating events that involve two or more reactor units as well as those from a single reactor initiating event that adversely impacts one or more other units.	RATIONALE: Single reactor accident sequences have already been defined in the single reactor PSAs which are assumed to have been completed before the multiunit PSA is built. Accident sequences resulting from initiating events involving multiple reactor units need to be added for a reasonably complete set of accident sequences. In addition there may be additional multiple reactor accidents from single reactor accidents that progress into a multiple reactor accident due to a “domino effect”.

TABLE 7.2-B ATTRIBUTES FOR AS ANALYSIS: TASK AS-B ‘DEFINITION OF SUCCESS AND NON-SUCCESS END STATES AND KEY SAFETY FUNCTIONS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
AS-B	For each initiating event group for internal events, internal hazards, and external hazards for each POS the key safety functions that are necessary to reach a success end state are identified. Success and non-success end states are clearly defined.	COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered.
AS-B01	The success and non-success states are defined in a manner that provides the possibility to justify the achievement (non-achievement) of the success end state for each accident sequence with the use of available tools (e.g. thermal hydraulic analysis, tests and experiments, etc.). All end states are identified as success or non-success; no end state is undetermined.	RATIONALE: Undefined end states prevent the capability for a useful interpretation of the results.
	AS-B01-S1 *For accident sequences resulting from initiating events affecting multiple reactor units, the end states must account for the success and non-success end state status of all affected units.*	*COMMENT: An initiating event that impacts a combination of N reactors on the site may result in any possible combination of reactor end states ranging from all N reactors with successful end states to all N reactors with unsuccessful end states.*
AS-B02	For each initiating event group the key safety functions are identified. Systems and procedurally directed operator actions required to perform safety functions are identified for each IE group with account for availability of specific equipment and conditions for operator actions (e.g. information available for operator, acceptability for manually controlled equipment, time window, etc.). For each safety function, system models are developed with account for success criteria defined for specific IE group and AS.	
AS-B03	A justification for the achievement of stable success end state conditions is provided for each AS with account of all uncertainties associated with the applicable tools.	RATIONALE: Ignoring the uncertainties associated with the available tools used to justify achievement of the success end state may lead to loss of significant insight of the PSA.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	AS-B03-S1	*Justification for the achievement of the non-success end state conditions is performed with the use of 'best estimate' models and parameters of the applicable justification tools.*	*RATIONALE: Use of conservative parameters for justification of non-success end states may lead to excessively conservative consideration of certain ASs, bias the results and insights and make certain applications non-credible.*

TABLE 7.2-C ATTRIBUTES FOR AS ANALYSIS: TASK AS-C ‘ACCIDENT SEQUENCES PROGRESSION IDENTIFICATION AND AS MODELS DEVELOPMENT’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
AS-C	For each IE group for internal events, internal hazards, and external hazards for each POS the accident progression for all sequences is identified and justified. For each IE group the accident sequence models are developed. AS models explicitly address realistic plant behaviour in response to IE in terms of normal plant systems operation, operator actions, and mitigation systems that support the key safety functions necessary to achieve a stable safe state.	COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered
AS-C01	The end states of the accident sequences are achieved when either a ‘non-successful’ or “safe stable state“, where long term stable successful plant conditions have been reached.	COMMENTS: ‘Stable successful’ plant conditions are the conditions which may be maintained during and after the defined mission time with the set of equipment postulated to be operable for the specific accident sequence. The mission time may be different for different accident sequences and is specified as the post-IE occurrence time period that allows for long term measures to be put in place to maintain this state, e.g. to repair a failed safety system train. For shutdown PSA, boiling in the core with inventory makeup may represent a stable long term, steady state condition. EXAMPLE: The possibility to remove heat via the secondary side in an open mode using limited amount of water in the demineralized water tanks should not be considered as a successful stable end state.
AS-C02	The accident progression analysis is performed for each sequence until a safe, stable, long term condition is reached or until core/fuel damage occurs, in order to determine if there is a cliff edge effect beyond the mission time used in the PSA.	COMMENT: The cliff edge effect appears if small deviations in plant parameters that could give rise to severely abnormal plant behaviour or exhausting of safety system resources (e.g. cooling water, diesel fuel) could lead to dramatic change of safety function fulfilment. EXAMPLE: New WWER plants are equipped with long term hydroaccumulators to cope with LOCA for more than 24 h. Given a failure of all active safety systems the core is prevented from damaging in a passive way until hydroaccumulators become empty. After that the cliff edge effect appears.
AS-C03	Realistic and ‘applicable’ (i.e. from ‘similar’ plants) thermal hydraulic analyses are used to determine the accident progression parameters (e.g. timing, temperature, pressure). All normal operation and stand-by	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	systems, the operability of which may impact the accident progression are accounted for.		
	AS-C03-S1	*Plant specific realistic thermal hydraulic analyses are used to determine the accident progression for ASs.*	*RATIONALE: Use of thermal hydraulic analysis from similar units may produce results, which do not account for specific plant features influencing accident progression for specific sequences. The ASs constructed without taking into account plant specific features may not be appropriate for some PSA applications.*
AS-C04	Conservative assumptions are made when particular course of accident progression for specific ASs are not justified by supporting analyses (e.g. thermal hydraulic, fractural mechanics, reactivity analysis, etc.).		RATIONALE: This attribute is stated in order to avoid missing of potential insight due to lack of knowledge on actual plant behaviour. If safety significant insights cannot be achieved with the use of conservative assumptions, more efforts need to be taken to remove conservatism with appropriate justification.
	AS-C04-S1	*Plant specific realistic analyses are performed for specific ASs in order to obtain a realistic description and model of accident sequences.*	*RATIONALE: Use of conservative assumptions instead of realistic analysis may bias the benefits of certain applications aimed at improving/checking the influence of specific plant changes.*
AS-C05	The procedures are reviewed with engagement of plant operations and training personnel to confirm that the interpretation of the procedures and the expected responses are consistent with the existing thermal hydraulic analyses and plant operational practices. The accident sequence models are consistent with the plant specific emergency procedures, shutdown operating procedures, training simulator exercises, and existing thermal hydraulic analyses. In case of alternatives, the most restrictive accident progression is modelled. For accident sequences resulting from a multiunit initiating event the human dependencies and interactions associating with controlling and accident management of multiple units is considered.		COMMENT: Procedures for use during shutdown contain a significant amount of detail and cautions not normally included in normal operating procedures. The definition of the shutdown accident sequences must reflect all available sources of guidance to the plant operators.
	AS-C05-S1	*When existing procedures allow operator to follow different mitigation strategies, the accident sequence models account for all possible strategies. The likelihood of each strategy is estimated based on the results of interview with plant operators, actual plant experience, and training practice.*	*RATIONALE: Incomplete modelling of accident progression dealing with non-clear requirements of plant emergency procedures may bias the benefits of certain applications aimed at improving the accident procedures.*

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
AS-C06	For at-power operation POSs all accident sequences constructed based on the results of realistic thermal hydraulic analyses, where human interactions not considered in plant emergency procedures for the particular scenario are credited, the failure of those human interactions is assumed. (See also Table 10.2-E, general attributes HR-E01, HR-E03, and Table 10.2-G, general attribute HR-G05).		RATIONALE: Optimistic crediting the human interactions not described in the emergency procedures may mask the problems in the emergency procedures. COMMENT: However, the sequences with the human interactions assumed to be failed might remain in the accident sequences model to allow improvement of the emergency procedures focusing on those interactions that are beneficial for safety. COMMENT: Emergency procedures may be less detailed than accident sequence models in the PSA.
	AS-C06-S1	*For all accident sequences constructed based on the results of realistic thermal hydraulic analyses, which require human interactions not considered in plant emergency procedures for the particular scenario, additional investigations are performed to analyse the possibility to perform required actions (e.g. plant -specific thermal hydraulic analysis for specific sequences, interviews with plant operators, HRA, analysis of plant experience, simulator exercises, etc.)*	*RATIONALE: Realistic modelling of accident progressions dealing with non-clear requirements of plant emergency procedures helps to assess real benefits from improvements in emergency operating procedures.*
AS-C07	For low power and shutdown operation POSs all accident sequences constructed based on the results of realistic thermal hydraulic analyses, where human interactions not considered in plant emergency procedures for the particular scenario are credited, the failure of those human interactions is assumed or additional investigations are performed to assess the possibility to perform required actions (e.g. plant -specific thermal hydraulic analysis for specific sequences, interviews with plant operators, HRA, analysis of plant experience, simulator exercises, etc.).		RATIONAL: For low power and shutdown operation POSs emergency procedures are not detailed and do not provide specific guidance for human interactions for particular scenarios that are modelled in PSA. However, due to longer available time it might be possible to credit these human interactions, when their feasibility is assessed through plant specific thermal hydraulic analysis, interviews with plant operators, analysis of plant experience, simulator exercises, etc. COMMENT: For POSs with the containment (confinement) open, the ability to re-establish containment (confinement) integrity by closing the containment (confinement) entrances may not be dependent only on human interactions, but can be significantly affected by the initiating event (e.g. Loss of off-site power).
AS-C08	If emergency procedures permit performing an action, but the realistic t/h analyses demonstrate that the action imposes an adverse effect, the accident sequences nevertheless include those actions.		RATIONALE: Unjustified optimism need to be avoided in ASs modelling.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	AS-C08-S1	*If emergency procedures permit to perform an action but the realistic t/h analyses demonstrate that the action imposes an adverse effect, additional investigations are performed to assess the real operator response (e.g. interviews with plant operators, analysis of plant experience, simulator exercises, etc.) Both permitted action and action based on realistic operator response are included in accident sequence models.*	*RATIONALE: Realistic modelling of accident progressions dealing with non-clear requirements of plant emergency procedures helps to assess real benefits from improvements in emergency operating procedures.* *EXAMPLE: For the units with the possibility to isolated the primary circuit in case of LOCA event procedures may permit or even require isolation; however, realistic analysis confirm that this action may have adverse consequences in certain conditions.* *COMMENT: Human reliability analysis should consider the issue of incomplete or non-clear requirements of plant emergency procedures (See Section 10.2).*
AS-C09	The accident sequences possible for each initiating event group are developed. For each initiating event group, the accident sequences model is developed to a justifiable level of detail that the differences in requirements on systems and operator responses are captured. Diverse systems providing similar function are modelled separately if the choice of one system over another significantly changes the requirements for operator intervention or the need for other systems.		COMMENT: Accident sequences can be modelled at various levels of detail ranging from small functional level event trees, through system level event trees (commonly referred to as the small event tree approach with fault tree linking) to very large event trees that model support system and front line system status at the train level (the so-called Large Event Tree or Event Tree Linking approach). (See also Table 13.2-A, general attribute MQ-A01).
AS-C10	For each key safety function its dependence on the success or failure of preceding functions and the impact on accident progression are addressed.		COMMENTS: The dependence between operator-induced initiating events and recovery events is especially important. In some cases, operators are directed to control the rate of feed to match boil-off. Success of this action has two ramifications: (1) it may avoid the need to go to recirculation and (2) it adds heat to the containment (confinement) that may require containment (confinement) heat removal systems to operate. Failure to control flow (i.e. over feeding), leads to a need for recirculation, but may not require additional heat removal capability beyond the recirculation system EXAMPLE: The success of low pressure system injection is dependent on the success of RPV depressurization.
AS-C11	When developing accident sequences, the phenomenological conditions created by the accident progression including those caused by changing plant conditions within a POS or due to the unique site and plant impacts resulting from internal or external hazards that create additional		EXAMPLE: Phenomenological conditions include generation of harsh environmental effects, including temperature, pressure, debris, water levels, and humidity. The effects of these conditions could directly cause equipment failure, or might require procedural operator actions to prevent equipment damage (e.g. to temporary disable

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	phenomenological conditions are identified so that the effect on potential mitigating systems is properly accounted for The adverse impacts of radiological contamination of the site due to an accident on another unit are considered when modelling the plant and operator response to each unit on the site.	equipment). Examples of phenomenological conditions that could affect accident progression are the viability of recirculation from the containment (confinement) or the potential impact of reactor coolant boiling on the ability to close the containment (confinement). COMMENT: On the other hand, systems that might not be available at the start of a sequence due to the specific POS conditions could become available as plant conditions change, e.g. secondary passive heat removal system at new WWERs is initially unavailable during Cold Shutdown due to the lack of steam in steam generators, but as the RCS heats up it may become available.
AS-C12	If plant configurations and maintenance practices create dependencies among various system alignments, these configurations and alignments are defined and included in the model in a manner that reflects these dependencies.	
AS-C13	Events for which time phased dependencies might exist are defined and are included in ASs models appropriately.	EXAMPLE of time phased events include: AC power recovery, DC battery time dependent discharge, environmental conditions for operating equipment and the control room (e.g. room cooling), etc. During shutdown POSs two key time phased dependencies examples are: (1) initiation of PWR injection by gravity before reactor coolant boiling (boiling may negate elevation head for gravity injection) and (2) recovery of residual heat removal function before reactor coolant boiling to avoid pump cavitation.
AS-C14	If ATWS sequences are grouped and modelled as a single event tree, the most restrictive case is considered.	COMMENT: Many PSAs group ATWS sequences together and develop a model for the most restrictive case (e.g. LOOP, etc.)
	AS-C14-S1 *ATWS sequences are modelled as part of accident sequence model for each IE group. Specific analyses justify the possibility to prevent core/fuel damage for each ATWS sequence with successful end state.*	*COMMENT: For modelling of ATWS sequences the specific conditions which are in place for the related initiating event group are accounted for, as well as the conditions and events connected to a particular failure of the reactor shutdown function.*
AS-C15	When transfers between event trees are used to reduce the size and complexity of individual event trees the method for implementing an event tree transfer that preserves the dependencies that are part of the	COMMENT: If software being used for PSA is not capable of event trees linking, care must be taken that all boundary conditions of parent event tree top event are

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	transferred sequence is used. These include functional, system, initiating event, operator, and spatial or environmental dependencies.		transferred to subsequent event trees.
AS-C16	The consequences of successful operation of mitigating systems on accident progression are determined by considering the actual plant response.		EXAMPLES: 1) On receipt of a LOCA signal, three containment spray pumps start even though only one is required by the success criteria. If there is no directive to the operators to turn off pumps, or decrease flow, the increased flow will decrease the time of depletion of the tank shared by common spay and injection systems. Even if there is procedural direction to decrease flow, the possibility that the operators would fail to do so need to be taken into account. 2) Opening of all steam safety valves while only one is needed to prevent excessive pressure increase in the steam lines may lead to failure to reclose of several valves.
	AS-C16-S1	*Realistic plant specific analyses are made for specific ASs in order to verify whether the conditions for operator actions and operation of the specific equipment are achieved.*	*RATIONALE: Use of conservative assumptions instead of realistic analysis may bias the benefits of many applications aimed at improving/checking the influence of specific plant changes (e.g. hardware or procedures).*
AS-C17	Accident progression is discussed and 'agreed' with plant operators.		RATIONALE: Experienced plant operators could identify inconsistencies between PSA ASs models and actual plant behaviour in term of accident progression, system requirements, procedurally directed operator actions, etc.
	AS-C17-S1	*An expanded graphical representation of accidents progression (e.g. 'event sequence diagram') for IE groups is used to verify the AS models with plant operators.*	*RATIONALE: Graphical representation of accident progression helps non-PSA specialists to understand AS models.*
AS-C18	The accident sequence models for the identified initiating events for hazards are modified to reflect the dependence of the accident sequence on the effects caused by the hazard being analysed.		RATIONALE: In many cases the systems performing safety functions are affected by the hazard. If totally disabled, the relevant event tree need to be modified accordingly.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
AS-C18	The hazard events sequence models are developed for the hazard event in the control room, and the model takes into account hazard even-specific impacts.	RATIONALE: In the PSA for internal initiating event usually there is no such event tree model that can be applied to model the external or internal hazards in the control room. It is an initiating event special to the hazards; therefore special event sequence model need to be developed. COMMENT: For example fire-specific impacts to consider include: - Widespread effect of a fire in the main control room across multiple safety systems; - The potential for spurious actuation of systems and - The impact of fire in the main control room on operator actions including: a) The effects of fire and smoke b) The capability of features for fire detection and suppression c) The use of an alternative location for safe shutdown, taking into account aspects of accessibility and other possible limitations.

TABLE 7.2-D ATTRIBUTES FOR AS ANALYSIS: TASK AS-D ‘SUCCESS CRITERIA FOR ACCIDENT SEQUENCES’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
AS-D	The task includes the definition of accident sequence success criteria.	
AS-D01	For each initiating event group and for each accident sequence, the success criteria for safety related functions, operator actions, systems, and equipment are defined.	COMMENT: See attributes in Section 8.

TABLE 7.2-E ATTRIBUTES FOR AS ANALYSIS: TASK AS-E 'DOCUMENTATION'

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
AS-E	Documentation and information storage is performed in a manner that facilitates peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the methods used, assumptions made and their bases.	
AS-E01	The following aspects of the accident sequence analysis process are documented: - Graphical representation of each accident sequence for each IE group; - A description of the accident progression for each sequence or group of similar sequences; - The success criteria established for each initiating event category including the bases for the criteria; - Any assumptions that were made in developing the accident sequences, as well as the bases for the assumptions; - Existing analyses performed to define success criteria and expected sequence phenomena including necessary timing considerations; - System operation information to support the modelled dependencies; - Calculations or other bases used to justify equipment operability beyond its 'normal' design parameters and for which credit has been taken; - Justification for the non-loss of dependences if modelling simplifications were implied; - Treatment of accident sequences involving unsuccessful end states on two or more reactor units concurrently.	
AS-E02	The interfaces between Accident Sequence Analysis and other PSA tasks are defined and documented.	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	- The definition of hazard events in the Hazard Event analysis task; - The definition of initiating event category in the Initiating Event Analysis Task; - The definition of core damage and associated success criteria in Success Criteria Definition Task; - Key definitions of operator actions and sequence-specific timing and dependencies reflected in the accident sequence models in the HRA task for these actions; - The basis for the sequence and cutset quantification in the Level 1 Quantification and Results Interpretation Task; - A framework for an integrated treatment of dependencies in the initiating events analysis, systems analysis, data analysis, human reliability analysis, Level 1 quantification.	
AS-E03	The sources of model uncertainty and related assumptions associated with the accident sequence analysis are documented.	

8. PSA ELEMENT 'SC': SUCCESS CRITERIA FORMULATION AND SUPPORTING ANALYSIS

8.1. MAIN OBJECTIVES

The main objective of the success criteria formulation task is to determine for given initiating events what represents a successful or unsuccessful plant response and to translate this information into detailed plant system and operator action success criteria accomplished for each POS. Thermal hydraulic analyses simulating the course of accident sequence progression and other assessment means are used for this purpose. These analyses and assessments are called in this section supporting analyses for the success criteria formulation.

As a first task core or fuel damage or other unsuccessful accident sequence end states are defined in order to provide the basis for the derivation of detailed success criteria for safety related functions or human interactions. The description of the formulation of success criteria and of related attributes in this section is limited to success criteria required for a Level 1 PSA.

Success criteria regarding the plant response to initiating events are used to specify whether safety related functions meet the requirements to prevent damage to the core or mitigate significant releases of radioactivity. These safety related functions in terms of a PSA may be functions of operating systems, front line safety systems, I&C, support systems, structures, components, and operator actions. For operator actions success criteria are characterized by statements that certain actions are successfully carried out within a defined time window.

Success criteria are used to construct the logic PSA model, including for example the determination of boundary conditions for initiating events, of event tree branch point probabilities and probabilities for other events in the logic model. They also determine the required number of trains of a safety related system. Top-level safety related function requirements are translated into the requirements for systems performing that function, a process, which is continued down to support systems. Event tree branch point probabilities also may reflect operator actions with their specific success criteria, e.g. a time window. Other operator actions may be modelled at the system level. There is therefore a close connection between initiating events analysis, accident sequence analyses, human reliability analysis, systems analysis, and success criteria formulation.

8.2. SUCCESS CRITERIA FORMULATION AND SUPPORTING ANALYSIS TASKS AND THEIR ATTRIBUTES

Table 8.1 lists the main tasks for the PSA element 'Success Criteria Formulation and Supporting Analysis'. Tables 8.2-A through 8.2-C present the description of general and special attributes for these tasks.

TABLE 8.1 MAIN TASKS FOR SUCCESS CRITERIA FORMULATION AND SUPPORTING ANALYSIS

Task ID	Task Content
SC-A	Definition of overall and detailed success criteria
SC-B	Thermal hydraulic analyses and other assessment means supporting the derivation of detailed success criteria
SC-C	Documentation

TABLE 8.2-A ATTRIBUTES FOR SUCCESS CRITERIA FORMULATION AND SUPPORTING ANALYSIS: TASK SC-A 'DEFINITION OF OVERALL AND DETAILED SUCCESS CRITERIA'

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SC-A	Definition of the overall success criteria for the PSA and definition of the success criteria for systems, structures, components, and human interactions for internal events, internal hazards, and external hazards for all POS is performed in a manner which is consistent with plant features, procedures and operating practices.	COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered.
SC-A01	Definition of core/fuel damage or other unsuccessful accident sequence end states. Core or fuel damage is defined in terms of physical processes and phenomena and failure mechanisms, which may cause a substantial release of radioactive material from the reactor fuel.	COMMENT: For vessel type LWRs there are usually only two types of end states defined in terms of the Level 1 PSA: (1) Successful end states without significant core/fuel damage, and (2) Unsuccessful end states with core/fuel damage. For other reactor types, for example for channel type reactors, different levels of core or fuel damage are used to reflect scenarios where damage is limited to only one channel, a group of channels, to a portion of the core or extends to the entire core. COMMENT: For example the following information sources are used to derive the definition of core or fuel damage: - The available design basis information for a plant and related information, e.g. design basis accident analyses is used; - Available information on core or fuel damage mechanisms and phenomena for similar plants and from related experimental investigations is used.
SC-A02	The physical plant parameters (e.g. highest node temperature, core collapsed liquid level) and associated acceptance criteria or limit values (e.g. temperature limit, percentage of cladding thickness oxidized) to be used in determining core or fuel damage are defined. The parameters are selected in such a way that the determination of core or fuel damage is as realistic as practical and consistent with current best practices and knowledge. For the application of parameter acceptance criteria with the results of thermal hydraulic calculation a credible margin is specified, justified and used to take care of limitations of the computer codes, such as limitations in the sophistication of models, and	EXAMPLES: Parameters and associated acceptance criteria that are used in PSAs include: 1. BWR: Collapsed liquid level less than 1/3 core height or code-predicted peak core temperature > 2500°F (1370°C). 2. PWR: Collapsed liquid level below top of active fuel for a prolonged period, or code-predicted core peak node temperature > 2200°F (1200°C) using a code with detailed core modelling, or code-predicted core peak node temperature > 1800°F (1000°C) using a code with simplified (e.g. single-node core model, lumped parameter) core modelling, or code-predicted core exit temperature > 1200°F (650°C) for 30 min using a code with simplified core modelling.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	uncertainties in the results.	
SC-A03	The decay heat level associated with each modelled POS is determined for use in defining and applying success criteria and the timing for operator actions.	COMMENT: The decay heat level is defined based on average duration after reactor trip for a particular POS.
	SC-A03-S1 *The decay heat level is defined based on planning outage durations.*	*RATIONALE: The decay heat level associated with planned outage duration is essential for applications aimed at reducing outage duration Important.* *COMMENT: The trend toward shorter outages may mean that POSs are entered sooner after plant shutdown when decay heat levels are higher than might be experienced in past outages. The higher decay heat may affect the success criteria of a system or component and may therefore require a change in the characteristics of a POS even if the actual plant outage procedures are not changed. The known plans may be in written form, or may be extracted by way of the interviews.*
SC-A04	Success criteria for each of the safety related function are specified in the accident sequences for each initiating event group.	COMMENT: The formulation of success criteria at the functional level, system level, system train level and for structures and equipment is accompanied by a description of accident sequences, including references to the plants protective I&C and EOPs which primarily determine the plant systems response.
SC-A05	Systems capable of meeting the specified success criteria of safety related functions are identified together with associated operator actions if applicable. The success criteria for the safety related functions are translated accordingly to the systems and associated operator actions. From the level of systems, success criteria are continued to system trains if necessary and further down to the associated support systems. For multiple units plants the systems that are shared between units are identified, and the manner in which the sharing is performed should the units experience a common initiating event (e.g. LOOP). This includes operator actions as required and specified by plant procedures or operating practices.	COMMENT: As specified under other PSA tasks in this publication dependencies of front line systems on support systems and I&C are preferably modelled explicitly for example by means of transfers from support system trains to the equipment of the front line system which depend on a particular support systems. Depending on the design this requires formulation of success criteria for support systems as well. An example for this is a DC electrical power supply from two DC supply trains via separation diodes. Apart from these straightforward train dependencies on supports there are usually dependencies requiring additional analyses, for example room cooling requirements regarding the operation of safety related equipment during the mission time.
SC-A06	A mission time for the accident sequences is determined. The mission time is the time during which safety related functions are required to	COMMENT: As regards the additional evaluation or modelling carried out for sequences in which a safe, stable state has not been achieved by the end of the mission

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	work to achieve a safe stable state after an initiating event. Additional evaluation or modelling is carried out for sequences in which a safe stable state has not been achieved by the end of the mission time defined for the PSA.	time defined for the PSA, possible approaches include: a. Assigning an appropriate plant damage state for that sequence if this is useful and does not significantly hinder applications; b. Extending the mission time, and extending the affected analyses to the point at which conditions and parameters can be shown to reach acceptable values; c. Extending the mission time to reflect site and regional impacts that can cause the need for systems to operate longer in order to assure long term safe, stable conditions; d. Modelling additional system recovery or operator interactions for the sequence, in accordance with requirements stated in the systems analysis and HRA sections of this guide, to demonstrate that a successful outcome is achieved together with an assessment of the probability for success and failure of the additional events. COMMENT: It has been typical in internal events to use a mission time of 24 hours on the assumption that, if a safe stable condition is reached by that time there are usually a number of options for recovery available to maintain that state as long as there is no “failure cliff” shortly after that point in time. However, this may not be true of internal or external hazards, where the damage could require systems to operate much longer (for example, recovery of off-site power may take much longer).

TABLE 8.2-B ATTRIBUTES FOR SUCCESS CRITERIA FORMULATION AND SUPPORTING ANALYSIS: TASK SC-B ‘THERMAL HYDRAULIC ANALYSES AND OTHER ASSESSMENT MEANS SUPPORTING THE FORMULATION OF SUCCESS CRITERIA’

Task/ GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SC-B	Detailed success criteria and event timing that fully support for the quantification of risk metrics, and the determination of impact of success criteria on systems, structures, components and human interactions are developed for internal events, internal hazards, and external hazards for all POS by appropriate thermal hydraulic analyses and other assessment means.		COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered.
SC-B01	Applicable and proven computer codes are used for the modelling of the course of accident sequences and for the derivation of associated success criteria. Preferably and if available best estimate codes and models are used for this purpose and the plant and sequence model reflects the specific design and operational features of the plant. Best estimate models or analyses can be supplemented with plant specific or generic Safety Analysis Report or other conservative analyses applicable to the plant accompanied with a justification and an assessment of associated uncertainties.		COMMENT: For success criteria development it may be necessary to perform specific thermal hydraulic calculations for low power and shutdown POS.
	SC-B01-S1	*Applicable and proven computer codes are used for the modelling the course of all relevant accident sequences and for the derivation of associated success criteria. Best estimate codes and models are used for this purpose and the plant and sequence model reflects the specific design and operational features of the plant.*	*RATIONALE: Use of generic assessments may provide insufficient plant specificity for parts of the model affected by applications. Conservative assessments may cause masking effects hindering certain applications.*
SC-B02	Expert judgment is only used to assess the conditions or response of systems, structures and equipment in situations when there is a lack of available information, knowledge or analytical methods upon which a prediction can be based if it can be demonstrated that the variability and uncertainty potentially inherent in the assessment does not significantly impact on the PSA models and results.		

Task/ GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SC-B03	When defining success criteria; thermal hydraulic, structural, or other analyses and evaluations are used, which are appropriate to the POS definition and characterization as well as the hazard event and the event sequence being analysed. The level of detail in these analyses and evaluations is consistent with the initiating event grouping and accident sequence analysis tasks.	COMMENT: Success criteria determined for full power conditions are not always bounding for low power and shutdown states.
SC-B04	Analysis models and computer codes are used that have proven capability to model the conditions and phenomena of interest in the determination of success criteria and that provide results representative for the plant. Computer codes and models are only used within known limits of applicability.	
SC-B05	The plant model and parameters used for thermal hydraulic analyses are established in a way that provides a level of resolution that reflects the actual design and operational features of the plant. Parameter values (including setpoints, limit points, trigger values, entry and exit values for procedures, and sets of parameter values which are used for control functions) determine when operator actions are carried out and determine the function of safety related systems. In this respect the plant model and the model of related control system functions are supported by a detailed description including references to the plants protective I&C and EOPs. When specifying parameter values, uncertainties, variability, and delays for measuring and actuating devices and for actuated equipment are taken into account.	
SC-B06	The plausibility, reasonableness, and acceptability of thermal hydraulic, structural or other supporting engineering bases used to support success criteria is checked with appropriate methods.	COMMENT: Methods can include the following: a) Comparison of results with results of similar analyses performed for similar plants, accounting for differences in unique plant features. b) Comparison with results of similar analyses with other codes. c) Check by other means, e.g. simplified engineering calculations.

TABLE 8.2-C ATTRIBUTES FOR SUCCESS CRITERIA FORMULATION AND SUPPORTING ANALYSIS: TASK SC-C ‘DOCUMENTATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SC-C	The documentation is performed in a manner facilitating a peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the methods used, assumptions made, and their bases.	
SC-C01	The following aspects of the success criteria formulation and support analysis process are documented (a) Each of the success criteria and the supporting assessments, engineering bases, references and assumptions are documented in detail. (b) Conservative assumptions are described and documented including the rationale for using conservatism and an assessment of impacts. (c) A detailed and traceable description of condensation, grouping, binning, agglomeration, screening and simplification steps is given including justifications and an assessment of effects and which is consistent with the initiating event and accident sequence analysis tasks. (d) The basis for the success criteria development process is documented in a way, which is consistent with the initiating event and accident sequence analysis tasks.	COMMENT: The following is documented consistent with and not extensively doubling the information presented in the tasks for initiating events, accident sequence assessment, human interaction analysis and systems analysis: a) The definition of core / fuel damage used in the PSA including the basis for any selected parameters and parameter values; b) Calculations (generic and plant specific) or other references used to establish success criteria, and identification of cases for which they are used; c) Identification of computer codes or other methods used to establish plant specific success criteria; d) A description of the limitations (e.g. potential conservatisms or limitations that could challenge the applicability of computer code models in certain cases) of the calculations or codes; e) Identification of important assumptions used in establishing success criteria; f) A detailed and traceable description of condensation, grouping, binning, agglomeration, screening-out and simplification steps where used including justifications and impact assessment and consistent with the initiating event and accident sequence analysis tasks; g) A summary of success criteria for the safety related functions, systems and human interactions for each accident initiating event group; h) The basis for determining the time windows and other conditions for human interactions; i) The description of processes used to define success criteria for grouped initiating events or accident sequences.
SC-C02	The uses, rationale and background information for expert judgment is	RATIONALE: Applications may require redoing expert judgments, partially or as a

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	documented in a way which is traceable and reproducible. Uncertainties and variability in expert judgment are stated. The impacts or effects of these uncertainties and variability are assessed as part of the Results Analysis and Interpretation Task.	whole. Meaningful results and comparisons can only be achieved in such case if the expert judgment process including background information and justifications are sufficiently documented.
SC-C03	The rationale used in the application of success criteria for situations for which there is more than one technical approach, none of which is universally accepted as correct, is documented and the effects of using a particular approach is justified and impacts discussed.	
SC-C04	The sources of model uncertainty and related assumptions associated with the success criteria analysis are documented.	

9. PSA ELEMENT ‘SY’: SYSTEMS ANALYSIS

9.1. MAIN OBJECTIVES

The objectives of the systems analysis element are to identify and quantify the causes of failure for each plant system represented in the initiating event analysis and accident sequence analysis accomplished for each POS in such a way that:

- For each safety function in accident sequence models, system models are developed with account for success criteria.
- System-level success criteria, mission times, time windows for operator actions, different initial system alignments and assumptions provide the basis for the system logic models as reflected in the model. A reasonably complete set of system failure and unavailability modes for each system is represented.
- Human errors and operator actions that could influence the system unavailability or the system’s contribution to accident sequences are identified for development as part of the HRA element.
- Intrasystem dependencies and intersystem dependencies including functional, human, phenomenological, and common cause failures that could influence system unavailability or the system’s contribution to accident sequence frequencies are identified and accounted for.

9.2. SYSTEMS ANALYSIS TASKS AND THEIR ATTRIBUTES

Table 9.1 lists the main tasks for the PSA element ‘Systems Analysis’. Tables 9.2-A through 9.2-D present the description of general and special attributes for these tasks.

TABLE 9.1 MAIN TASKS FOR SYSTEMS ANALYSIS

Task ID	Task Content
SY-A	System characterization and system boundary definition
SY-B	Failure cause identification and modelling
SY-C	Identification and modelling of dependencies
SY-D	Documentation

TABLE 9.2-A ATTRIBUTES FOR SYSTEMS ANALYSIS: TASK SY-A ‘SYSTEM CHARACTERISATION AND SYSTEM BOUNDARY DEFINITION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-A	System characteristics including boundaries are defined for all systems, including support systems, needed for performing the functions identified in the accident sequence analysis.	
SY-A01	Plant information is collected to support the system model development. - Define system function during normal and accident conditions; - Establish system boundaries; - Identify interfaces with other systems; - Identify instrumentation and control requirements including operator interface; - Identify testing and maintenance requirements and practices; - Identify operating limitations such as those imposed by technical specifications; - Identify procedures for the operation of the system during normal and accident conditions, including specific planning guides, shutdown operating procedures for shutdown plant operational states; - Identify system configuration during normal and accident conditions, including temporary system alignments for shutdown plant operational states; - Identify system test and surveillance procedures; - Ascertain system operating history; - Ascertain system modification history.	EXAMPLES of information sources include: System P&IDs, one-line diagrams, instrumentation and control drawings, spatial layout drawings, system operating procedures, abnormal operating procedures, emergency procedures, success criteria calculations, the final or updated SAR, technical specifications, training information, system descriptions and related design documents, actual system operating experience and interviews with system engineers and operators.
SY-A02	Components required for system operation and the support systems interfaces required for actuation and operation of the system components are identified.	COMMENT: The boundaries of systems defined in a PSA may be different from the boundary used in the plant being analyzed.

TABLE 9.2-B ATTRIBUTES FOR SYSTEMS ANALYSIS: TASK SY-B: ‘FAILURE CAUSE IDENTIFICATION AND MODELLING’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-B	System models are developed for all systems included in Task A for internal events, internal hazards, and external hazards for all POS.	COMMENT: When considering hazard events included in the PSA, it is necessary to determine the additional SSC’s that have unique failure modes associated with the hazard, but were screened out in the internal events analysis because they did not have a credible random failure mode. COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered.
SY-B01	The system models include within the boundary the components required for system operation (as identified above), including interfaces as identified in SY-A02 (Table 9.2-A).	
SY-B02	Both normal and alternate system alignments are modelled.	COMMENTS: Depending on the modelling technique, a single system model may be constructed that addresses all alignments, or separate models may be developed for each different alignment. For a shutdown PSA past outages need to be reviewed to determine unique system operating states (e.g. temporary power or cooling) that need to be included in the sequence models.
SY-B03	System models are developed for all success criteria required in the accident sequence models.	COMMENTS: 1. Success criteria for all systems are developed according to Attributes in Section 8. 2. Depending on the modelling technique, a single system model may be constructed that addresses all success criteria, or separate models may be developed for each success criterion. EXAMPLES: a. Different success criteria are required for some systems to mitigate different accident scenarios: the number of pumps required to operate in some systems is dependent upon the accident initiating event. b. Success criteria for some systems are dependent on the success of another component in the system.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		c. Success criteria for some systems are time dependent. d. Changing decay heat with time, and after fuel reload may affect system success criteria.
SY-B04	In the PSA for internal flooding the loss of function of system containing the flooding source is considered if the system is disabled by the loss of inventory.	RATIONALE: Besides the unavailability of the flooding affected SSCs the loss of inventory in the flooding source may disable the function of the system the flooding source belongs to.
SY-B05	The boundaries of the components required for system operation match the definitions used to establish the component failure data.	EXAMPLE: A local control circuit for a pump does not need to be included explicitly in the system model if the control circuit is not shared with another component and the pump failure data used in quantifying the system model include control circuit failures.
SY-B06	A systematic method is used for identification of component unavailability and failure modes.	EXAMPLE is the use of FMEA.
SY-B07	Systems models are developed to include all component failure modes and unavailabilities that lead to failure to achieve system function as defined by the system success criteria except as excluded by SY-B18.	EXAMPLES of failure modes (not a comprehensive list): – Active component fails to start or to continue to run; – Failure of a closed component to open or to remain closed; – Failure of an open component to close or to remain open; – Active component spurious operation; – Plugging of an active or passive component; – Leakage of an active or passive component; – Rupture of an active or passive component; – Internal leakage of a component; – Internal rupture of a component; – Failure to provide signal (e.g. instrumentation); – Spurious signal/operation; – Pre-initiator human failure events[8];

[8] ‘Pre-initiator human failure event’ represents the failure of plant staff to perform correctly the required activities that causes the unavailability of the component, system, or function. These activities are usually dealing with test and maintenance.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		– Failure due to the particular application of “fail safe design” principle[9].
	SY-B07-S1 *Leakages/ruptures of passive components are included in the system models.*	*RATIONALE: Modelling of passive components failures (e.g. pipe segments) is useful for PSA applications dealing with optimization of ISI.*
SY-B08	When internal and external hazard events are part of the PSA, SSC failure modes unique to the hazard are identified.	COMMENT: This process may result in reviewing system drawings, general arrangements, isometrics, circuit and wiring diagrams, etc. in order to identify applicable induced failure modes. This attribute results in a supplemental list of events that will be added to the hazard equipment list to be considered as part of the fragility analysis. The fragility analysis may result in a determination that the susceptibility to the hazard event is low, in which case it would not be necessary to add the induced failure more to the model.
SY-B09	When hazard induced failures are included in the systems analysis models, these failures are added to the internal event fault trees.	COMMENT: It is generally easiest to first build the internal event systems model to create the overall systems and functions logic model. Adding the hazard-induced failures to this preserves the logic structure and creates an integrated model.
SY-B10	For seismic PSA, if any relays were identified as susceptible to relay chatter during the fragility analysis, their effects are assessed and added to the model.	COMMENT: It is not intended that every possible effect of the relay chatter be included in the model. It need to be determined whether the chatter can reasonably result in an impact to the model that results in a failure of a credited piece of equipment or requires an operator response to correct This determination is likely to require the performance of circuit response analysis.
SY-B11	When hazard-induced failures are included in the systems analysis models, for each basic event that represents a hazard-induced failure the model is constructed in such manner that the complementary “success” state can be properly accounted for during the quantification process in cases where the hazard-induced failure probability is high.	RATIONALE: It is common in the analysis of hazards that as the severity of the hazard increases, the probability of failures can approach (or reach) 1.0. In such cases, the complementary success state approaches zero. When approximations are used in the quantification process (e.g. the rare events approximation) failure to account for the low success probabilities generates false PSA results for sequences that are of very low frequency or impossible, but due to using approximations appear to be of high frequency.

[9] Failure of support systems might cause inadvertent change of the component state due to application of “fail safe design” principle.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-B12	If hazard-induced internal fires or floods are identified as part of the dependency and fragility analyses, the basic events and their effects are added to the model. The effects are assessed using the attributes given for the assessment of internal fires and floods.	RATIONALE: In order to properly assess the impacts of a seismically-induced internal fire or flood, it is necessary to develop the scenario in accordance with how it would be done for a random occurrence of the event. The attributes of HE-D and HE-E will logically apply.
SY-B13	The models include consideration to flow diversion as a result of component failures when the flow diversions that will fail a system or a train function as defined by the system success criteria. Exclusion of flow diversion failure modes from the model is justified by analysis.	EXAMPLES are: - Flow is diverted through recirculation lines; - Flow is diverted by round pumping due to pump failure and failure of check valve to reclose; - Flow is diverted through spuriously open overpressure protection safety relief valve in the system.
SY-B14	Unavailability for components due to testing and maintenance (both preventive and corrective) is included in the system models consistent with the actual practices and history of the plant for removing equipment from service. Restrictions on coincident unavailability of components/trains due to maintenance based on plant administrative practices such as Technical Specifications are addressed.	COMMENT: Unavailability to be considered include: – Unavailability caused by testing when a component or system train is reconfigured from its required accident mitigating position such that the component cannot function as required if an initiating event occur; – Maintenance events at the train level when procedures require isolating the entire train for maintenance; – Maintenance events at a sub-train level (i.e. between tag out boundaries, such as a functional equipment group) when directed by procedures. EXAMPLES of out-of-service unavailability to be modelled: – Train outages during a work window for preventive/corrective maintenance; – A functional equipment group removed from service for preventive/corrective maintenance; – A relief valve taken out of service; – Equipment intentionally taken out-of-service due to plant conditions (e.g. high pressure injection (PWR/WWER) with low reactor vessel pressure, automatic actuation of safety equipment) in some shutdown POSs; – Equipment that will not function given plant conditions (e.g. steam driven pumps at low reactor/steam generator temperatures) in some shutdown POSs; – Planned maintenance configurations and test alignments during the shutdown or in case of on-line maintenance.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
			COMMENTS: – The coincident maintenance on two redundant trains, if permitted, may be an important risk contributor, and this possibility needs to be considered; – Many systems are re-aligned, tagged out, have their automatic functions disabled, etc. in the process of going into an outage; – The capability to remove differing sets of SSCs for maintenance and testing is a unique characteristic of shutdown conditions. In some cases, due to the changes in maintenance configurations, additional POSs may need to be defined as output of the system analysis (see Section 4).
	SY-B14-S1	*The system models include the ability to turn test and maintenance contributions on and off.*	*RATIONALE: E.g. a Risk Monitor reflects actual configuration and maintenance activities and mean value maintenance unavailability are not used.*
	SY-B14-S2	*System models reflect the real maintenance situation with maintenance unavailability attributed to each train. Attributing all maintenance unavailability to one particular train is avoided.*	*RATIONALE: Certain applications will require train-specific modelling.*
	SY-B14-S3	*Symmetric models are developed to avoid overestimation of importance of some particular redundant components or trains and underestimation of others. Attributing the IE localization or challenges for equipment actuation to particular components from the set of redundant components is avoided.*	*RATIONALE: The applications dealing with ranking components in accordance with their importance measures require equal consideration of the possibility of an IE to occur in any of the redundant trains or loops and of the redundant components to operate when demanded.* *EXAMPLE:* – ***Non-symmetric model**: Steam line rupture is modelled as a rupture on a single selected SG (e.g. SG1) with the total IE frequency attributed to the steam line associated with SG1; in this case the effect of unavailability of the SG1 isolation valve will be overestimated and the effect of unavailabilities of equivalent isolation valves on other SGs underestimated.* – ***Symmetric model**: Steam line rupture is modelled as a rupture on any SG with the frequency partitioned equally between all SGs. In this case, importance measures of redundant components are not biased.*
SY-B19	Contributors to system unavailability and unreliability (i.e. components and specific failure modes) are excluded from the model only if it is shown that the omission of the contributor does not have a measurable impact on the results and at least one of the following screening criteria		RATIONALE: Other component failure modes will be dominating contributors to system unavailability. In addition, CCF contribution is likely to be dominated by components and failure modes that are not excluded.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	is met: a) The total failure probability of the excluded component failure modes resulting in the same effect on system operation is at least two orders of magnitude lower than the highest failure probability of the other components in the same system train that results in the same effect on system operation. b) The contribution of one or more excluded failure modes for a component to the total failure rate or probability is less than 1% of the total failure rate or probability for that component, taking into account the same effect on system operation. c) The screened contributors are position faults for components (such as those that occur during or following test and maintenance activities) for which the component receives an automatic signal to place it in its required state and no other position faults exists (e.g. pulled breakers) that would preclude the component from receiving the signal. Components or failure modes using criteria (a), (b), or (c) if they could fail multiple systems or multiple trains of a system ARE NOT SCREENED. Components or failure modes using any of the above criteria must meet the selected criterion for BOTH random failure and failure caused by all of the hazard events being evaluated in the PSA. If in a particular POS a plant specific configuration causes the component to be an important consideration to remaining system or train mitigation reliability, the component is not screened.	COMMENT: The screening concept applies to all hazards, but when it is applied the hazard-specific context will apply. It is permissible to screen out failures for certain hazards, so it is not necessary to include all failure modes for all components. For example, the failure of a component may be eliminated from the internal events model because its random failure mode is very low probability, but the seismic failure mode may be much higher. In such case it is not necessary to provide a random failure probability when the seismic failure is added to the model.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	SY-B19-S1	*The basic event*[10] *screening process is revisited for certain applications.*	*RATIONALE: A check will be needed to make sure that originally screened out events do not have an impact on application results.*
SY-B20	The basic event screening process is revisited in the hazard analysis in order to avoid loss of information due to rearranged importance caused by the hazard.		RATIONALE: The hazard may disable SSCs being important contributors in the internal events PSA, and as a result less important (and potentially screened out) SSCs may become more important in the hazard PSA if not disabled.
SY-B21	No credit is given to repair (recovery) of hardware faults, unless the feasibility of repair is justified.		COMMENT: In some shutdown cases where relatively long times are available before core/fuel damage, more credit for restoration of equipment could be feasible than is true for full power models. It needs to be ensured that the equipment providing the safety function is capable of restoration (i.e. not completely failed as a result of the initiating event).
SY-B22	When simplified models, such as single basic event modelling and grouping of basic events into super components, are used, potential sources of dependencies are considered explicitly.		RATIONALE: Simplified models may mask contributions to the results of support systems or other dependent failure modes. EXAMPLES: Examples of dependencies that are needed to be considered explicitly include operator actions, functional dependencies, shared components, etc. Systems that sometimes have not been modelled in detail include the scram system, the power conversion system, instrument air, and the keep-fill systems.

[10] ‘Basic event’ is an element representing an event in a system fault model that requires no further decomposition (e.g. ‘pump fails to start when demanded’, ‘pump is unavailable due to test or maintenance’, etc.).

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	SY-B22-S1 *Each system is modelled with separate basic events down to the level of detail required for supporting a specific application.*	*RATIONALE: Certain applications may require a detailed modelling to take into account differences between components grouped together. Examples of differences include:* - *Hardware failures that are not recoverable versus actuation signals which are recoverable;* - *Events with different recovery potential;* - *HE events that can have different probabilities dependent on the context of different accident sequences;* - *Events which are mutually exclusive of other events not in the module;* - *Events which occur in other fault trees (especially common cause events);* - *Components having different maintenance and testing strategies;* - *SSCs used by other system.*
SY-B23	An appropriate reliability model, that matches the definitions and data available, is used for each basic event.	EXAMPLES: Reliability models in use in different PSAs include: – Monitored, repairable (standby failure rate, repair time); – Periodically tested (standby failure rate, test interval); – Constant unavailability (probability); – Fixed mission time (operating failure rate, mission time); – Non repairable (standby failure rate).
	SY-B23-S1 *Time dependent failure models are used.*	*RATIONALE: Certain applications, e g test interval optimization, require the use of time dependent models.*
SY-B24	The event naming scheme is developed in a consistent manner.	RATIONALE: Model manipulation and interpretation is facilitated by for example using the same designator for a component type and failure mode.

TABLE 9.2-C ATTRIBUTES FOR SYSTEMS ANALYSIS: TASK SY-C ‘IDENTIFICATION AND MODELLING OF DEPENDENCIES’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-C	All dependencies for internal events, internal hazards and external hazards for all POS are identified. Design related and operational dependencies, both direct and indirect, are explicitly modelled as far as possible. Residual dependencies are accounted for by CCF modelling.		COMMENT: If the scope of the PSA does not include certain hazards or LPSD POS, then these do not have to be considered.
SY-C01	All components or failure modes, which could fail multiple systems (so called shared components), are included in the model, even if the independent impact of the component/failure mode is considered non-significant.		RATIONALE: Failure of shared components may have a significant contribution to risk. EXAMPLE: Common suction pipe feeding two systems.
	SY-C01-S1	*When pipe rupture/leaks are included in the model, the effect of pipe failure on the effectiveness of all connected components (e.g. pumps, heat exchangers) is modelled.*	*RATIONALE: PSA applications dealing with optimization of ISI (i.e. risk informed ISI) require adequate modelling of the impact of pipe ruptures if the latter are included in the model.* *EXAMPLE: When two pumps are connected to the same pipe, a rupture of this pipe would disable both pumps. This need to be correctly accounted for in the model of each pump.*
SY-C02	A subcomponent that is shared by more than one component or affects another component is modelled separately.		
SY-C03	Support functions and systems needed to perform the system mission(s) are modelled explicitly. Justification is provided for cases where dependencies are excluded from the model. ***Caution:*** A careful identification (mapping) and modelling of control logic and power dependencies is needed to account for all dependencies in this area.		EXAMPLE of support functions: - Actuation logic including presence of conditions needed ;for automatic actuation and permissive and lockout signals; - Support systems required for control of components; - Component motive power; - Cooling of components; - Screen cleaning system; - Heating/ventilation system; - Water make-up; - Overpressure protection; - Any other identified support function necessary to meet the success criteria and

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		associated systems.
SY-C04	Mission times for support systems are modelled consistent with the mission time for the front line systems and in accordance with the success criteria.	
SY-C05	The available inventories of fuel, water in tanks etc. are compared with those required to support each success criterion and the model reflects the results of this comparison.	RATIONALE: Different accident scenarios may require different inventories. In some cases inventory is insufficient to complete the mission and supplementary sources may be required. Such sources will need to be included in the system model. EXAMPLE of inventories: - Accumulator air inventory; - Battery life; - Diesel fuel tank capacity; - Water storage tanks. COMMENT: Inventories of air, cooling and other services may be different in different POSs.
SY-C06	The modelling of electric power supply considers different power support cases to account for battery power availability until restoration of auxiliary and external power.	EXAMPLES of different power supply cases are: - All power sources can be accounted for initially; - Battery power available initially (battery) for connecting to auxiliary power; - Long term case without battery availability, but other power source is restored. COMMENT: Batteries can fail to take load when demanded. This failure mode needs to be considered. The probability of such event depends on design and operational features of the battery and battery charging system.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-C07	System conditions that cause a loss of desired system function including conditions that cause the system to isolate or trip, are modelled explicitly by using realistic functional requirements that are supported by engineering analysis. If engineering analyses and data are not available to justify certain failure probability, the equipment/system failure probability is assumed to be 1.0. or the relevant basic events are set to logical TRUE status	EXAMPLES of conditions that isolate or trip a system include: - System-related parameters such as a high temperature within the system; - External parameters used to protect the system from other failures (e.g. the high reactor pressure vessel (RPV) water level isolation signal used to prevent water intrusion into the turbines of the RCIC and HPCI pumps of a BWR); - Adverse environmental conditions. During shutdown, cavitation of a shutdown cooling/residual heat removal pump is possible due to changes in vessel level. COMMENTS: - Equipment protection signals may cause a direct automatic trip for some components, or equipment procedures require a manual trip. Both ways need to be considered if applicable; - Actuation signals sometimes vary by POS or might not be present; - During plant shutdown, unusual or temporary system alignments may create conditions whereby plant equipment is exposed to environments not considered for power operation.
	SY-C07-S1 *Engineering analysis is used to justify certain failure probability due to specific system conditions.*	*RATIONALE: Conservative approach may not be possible in an advanced application, where it can hide important results.*
SY-C08	The systems potential for causing a CCI is considered.	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-C09	SSCs that may be required to operate in conditions beyond their environmental qualifications are identified and dependent failures of multiple SSCs that result from operation in these adverse conditions are included.	EXAMPLES of degraded environments include: - LOCA inside containment (confinement) with failure of containment (confinement) heat removal; - Safety relief valve (in drywell) operability in case of small LOCA, with drywell spray in a BWR; - High energy line breaks, e. g., steam line breaks outside containment; - Debris that could plug screens/filters (both internal and external to the plant); - Heating of the water supply (e.g. BWR suppression pool, PWR containment sump) that could affect pump operability; - Steam binding of pumps; - Containment vent and failure effects.
SY-C10	SSCs that may be simultaneously affected by a hazard event are identified and dependent failures of multiple SSCs that result from exposure to the hazard event are included in the model.	COMMENT: The consideration of such dependency varies depending on the hazard event. Careful consideration must be given to what the controlling dependency mode is and the extent to which the dependency exists. EXAMPLES: – For seismic analysis, dependency is generally applied to similar SSCs that are at the same level in the plant; – For flood analysis, dependency is generally applied to components susceptible to flood that are reached by the flood level at the same time; – For turbine and tornado missiles, dependency is generally applied based on the path of the missile accounting for energy absorption that dissipates the missile energy (i.e. everything in the path of the missile fails until the missile comes to rest).
SY-C11	The locations of components vulnerable to environmental hazards that may impact system operation are identified.	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-C12	Spatial and environmental dependencies resulting from the accident sequence scenarios studied that may impact system operation are identified and accounted for in the system fault tree or the accident sequence evaluation.	EXAMPLE: Use results of plant walk downs as a source of information and resolution of issues in the evaluation of their impacts. COMMENT: Spatial and environmental dependencies could vary significantly from POS to POS (e.g. erection and removal of scaffolding or temporary shielding, removal of flood and ventilation barriers, etc. COMMENT: Spatial dependencies are of special concern for many hazards. Failure of SSCs that are not credited to function in the PSA may cause failure of credited SSCs. EXAMPLE: Structural collapse of an unreinforced block wall in a seismic event can damage nearby equipment. Such a collapse would not have been considered in internal events PSA because a random occurrence would be considered extremely low likelihood.
SY-C13	Operator interface dependencies across systems or trains are considered where applicable.	RATIONALE: Several operator actions relying on the same interface have to be treated as non-independent events in order to avoid too optimistic results.
SY-C14	Intrasystem common cause failures are modelled using a proven modelling approach.	RATIONALE: Common cause failures are dominating contributor to risk in plants relying on redundancies as a means of achieving a high reliability. EXAMPLE: Examples of methods are available in [22, 37].
SY-C15	Intersystem common cause failures are considered for components in systems that are shared between different plants.	EXAMPLE: Multiple unit crossties between the DGs of two units at the same site.
	SY-C15-S1 *Intersystem common cause failures are considered.*	*RATIONALE: Consideration of intersystem common cause failures may be needed to avoid unjustified optimistic results.* *EXAMPLE: The same type of valve across a number of systems.* *COMMENT: For the plants with high redundancy in terms of systems performing the same safety function intersystem CCF may be the most important contributor to the function failure.*
SY-C16	Common cause component groups (CCCGs) are defined based on a logical, systematic justified process that considers similarity. For multiunit PSAs the common cause groups are defined in a manner that distinguishes common cause events that are confined to components	COMMENTS: - Typically this suggests that CCCGs are defined within the same single system at the same plant, but when two or more systems are essentially identical and

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	within a reactor units and those involving combinations of components in different reactor units.	operated in the same manner they can be considered across system boundaries; - Consideration of different functional failure modes may need definition of more than one CCCG for the same set of components. An example is the case of safety/relief valves where the failure to open and failure to reclose after opening are treated by two CCCGs, one for each failure mode; - Service experience data analysed for common cause failures include numerous instances of multiple failures that occur on similar components on different reactor units. If these occur in combination with a multiunit initiating event, significant multiunit accidents may result. EXAMPLES: 1) Typical similarities used for the definition of common cause component groups are: design/hardware, function, installation, maintenance, test interval, procedures, service conditions, location and environment, manufacturer. Candidates for common cause failure groups include both active and passive components such as: motor-operated valves, pumps, safety-relief valves, air-operated valves, solenoid-operated valves, check valves, diesel generators, batteries, inverters and battery charger, circuit breakers, scram valves, RPS logic channels, RPS logic sensors, relays, strainers, electrical buses, chillers, compressors, control rods, air dryers, fuses (wire and electronic), electric heaters, switches, transformers, ventilation flaps, ventilation fans, etc. 2) A common cause failure of 4 emergency diesel-generators at a two reactor unit site due to excessively cold weather is consistent with a common cause grouping that crosses the boundary between the two units. If combined with an initiating event involving a loss of off-site power affecting both units, a significant multiunit accident sequence could result.
	SY-C16-S1 *Diversified components can normally be considered to be independent. However, if the diversified components have identical parts, there may be a need to break down the components into smaller parts, and model identical parts as CCCGs.*	*RATIONALE: Certain application requiring a higher level of detail may also require a higher level of detail in CCCG definitions.*

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-C17	In the PSA for hazards the additional CCCGs are defined that reflect all correlated failure modes.	RATIONALE: Components disabled by the same hazards need to be included in CCCGs induced by the hazard (see also DF-E02).
SY-C18	In the PSA for hazards the basic events representing the SSCs belonging to the set of equipment affected by the hazard are identified, and their probability is adjusted, or the relevant logical switches are set to the appropriate status for considering the effect of the hazard.	EXAMPLES: 1) In seismic PSA the probabilities of the basic events affected by the earthquake are calculated using the relevant fragility curves. 2) The basic events modelling fire affected equipment considered to be disabled by the fire are either set to logical TRUE status, or a suitable logical switch in the fault tree model is set to logical TRUE.

TABLE 9.2-D ATTRIBUTES FOR SYSTEMS ANALYSIS: TASK SY-D ‘DOCUMENTATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-D	Documentation and information storage is performed in a manner that facilitates peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the assumptions made and their bases.	
SY-D01	The processes that were followed to select, to model, and to quantify the system unavailability are documented. Assumptions and bases are stated	
SY-D02	The following aspects of the systems analysis process are documented: - Revision history; - Open issues (questions) and answers on previous issues; - The coding system used for the PSA and PSA model; - System function and operation under normal and accident conditions; - System activation/blocking; - Alternative system alignments; - System boundary; - System schematic illustrating all equipment and components necessary for system operation and components that are modelled; - Dependency matrices on component level (it is useful to produce an integrated dependency matrix to provide an overview of the functional dependencies over all systems); - Information and calculations to support equipment operability considerations and assumptions; - Actual operational history indicating any past problems in the system operation modification history; - System success criteria and relationship to accident sequence	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	models; - Human actions necessary for operation of system; - Reference to system-related test and maintenance procedures; - System dependencies and shared component interface; - Component boundaries; - Component spatial information; - Assumptions or simplifications made in development of the system models; - The systems potential for being a Common Cause Initiator; - A list of all components and failure modes included in the model (the basic events) along with justification for any exclusion of components and failure modes; - A list of all human action failure modes included in the model; - A list of all CCCGs included in the model; - A list of all environmental or spatial dependencies; - A description of the modularization process (if used); - Records of resolution of logic loops developed during fault tree linking (if used); - Results of the system model evaluations; - Results of sensitivity studies (if used); - The sources of the above information, (e.g. completed checklist from walk downs, notes from discussions with plant personnel); - Fault tree description including conditions for the model, top gate, fault tree layout, transfers, house events, attributes, failure modes, CCF modelling, test and maintenance modelling, operator actions and signal modelling.	
SY-D03	The sources of model uncertainty and related assumptions associated with the systems analysis are documented.	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-D04	The input and results of any screening processes shall be stored for future re-analysis, which may be necessary for applications or update of the PSA.	
SY-D05	Storage of the systems analysis information. The information from the systems analysis (e g FMEA and fault trees with gates and basic events) is part of the PSA model. The PSA model is stored and detailed background information is stored in a retrievable and accessible electronic form and format.	

10. PSA ELEMENT ‘HR’: HUMAN RELIABILITY ANALYSIS

10.1. MAIN OBJECTIVES

The objective of the human reliability analysis is to incorporate human factors into the PSA model and to assess the impact of plant personnel actions on risk for each POS. The personnel actions considered are of three types: the first type includes those associated with the performance of surveillance testing, maintenance, and calibration before an accident, often referred to as pre-initiator event actions; the second type is related to similar activities and operator manipulations that could lead to an initiating event, and the third type includes those associated with responses to plant disturbances as outlined in emergency and off-normal operating procedures or their equivalent, often referred to as post-initiating event actions. When constructing the PSA model these translate into the assessment of what in SSG-3 [3] are referred to as Type A, Type B, and Type C human action events.

The important HRA topics are:

- The identification of the specific human activities of all types for each POS, whose impact need to be included in the analysis;
- Consideration of reactor specific, design specific, plant specific, and accident sequence specific factors, including those factors that influence either an activities of interest or human performance, including those leading to errors of commission;
- The estimation of the probabilities of the logic model events (sometimes called human failure events (HFEs) or human errors (HE)) representing the contribution of the operators’ failure to perform the required actions correctly as specific modes of unavailability of the component, system, or function affected;
- The estimation of the probabilities of the human failure events occurring due to erroneous decision making (i.e. errors of commission);
- Consideration of human performance in an integral way so that issues of dependency are captured;
- The representation of the impact of success or failure to perform those activities correctly in the accident sequence models (e.g. event trees) and the system reliability models (e.g. fault trees).

The analyses on the above topics need to be performed using a systematic process and in such a way that the plant specific and, where necessary, accident scenario specific factors are taken into account.

10.2. HUMAN RELIABILITY ANALYSIS TASKS AND THEIR ATTRIBUTES

Table 10.1 lists the main tasks for the PSA element ‘Human Reliability Analysis’. Tables 10.2-A through 10.2-L present the description of general and special attributes for these tasks.

TABLE 10.1 MAIN TASKS FOR HUMAN RELIABILITY ANALYSIS

Task ID	Task Content
Pre-initiating event HRA	
HR-A	Identification of routine activities
HR-B	Screening of activities
HR-C	Definition of pre-initiator human failure events
HR-D	Assessment of probabilities of pre-initiator human failure events
Post-initiating event HRA	
HR-E	Identification of post-initiator operator responses
HR-F	Definition of post-initiator human failure events
HR-G	Assessment of probabilities of post-initiator human failure events
HR-H	Recovery actions
Human induced initiating event HRA	
HR-I	Identification of human failure events that could lead to an initiating event
HR-J	Grouping of human failure events that could lead to an initiating event
HR-K	Assessment of frequencies of human failure events that could lead to an initiating event
Documentation	
HR-L	Documentation

TABLE 10.2-A ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-A ‘IDENTIFICATION OF ROUTINE ACTIVITIES (PRE-INITIATING EVENT HRA)’

Task/ GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-A	A through identification of specific routine activities in each POS, which, if not performed correctly, impact the availability of equipment necessary to perform the system functions modelled in the PSA.	
HR-A01	Through a review of procedures and operational practices, those test and maintenance activities and routine operator manipulations in plant transition POSs that require realignment of equipment or a control system from its normal operational or standby status are identified for equipment and POSs modelled in the PSA.	COMMENTS: The intent is to identify those opportunities for operators to fail to realign equipment to its required status following completion of the activity, such that it would be unavailable should it be called upon to respond to an initiating event. Particular attention need to be paid to activities that can disable multiple trains of a system simultaneously (e.g. the automatic initiation of the standby liquid control system in a BWR is typically disabled for test purposes). It is typically assumed that the contributions to component unavailability from failures resulting from incorrectly performed maintenance are captured in the equipment failure probability. Thus, the focus here is on the failure to realign equipment upon completion of maintenance. Routine operator manipulation activities are those which are routinely performed after each entry to a POS. These include activities to align or block systems from service and to affect POS transitions. If plant specific procedures or finalized design information are not available, the required realignment of the PSA equipment that outside its normal operational or standby status is identified using equivalent identification process (e.g. interview with design engineers).
HR-A02	Through a review of procedures and practices, those calibration activities are identified that, if performed incorrectly, have the capability of defeating the automatic initiation of standby safety equipment or of rendering required functions of systems or components unavailable. In particular, those activities or manual actions that have the potential to affect equipment in multiple trains of a redundant system, or in diverse systems, e.g. as a result of using inappropriate calibration procedures or faulty or improperly calibrated calibration equipment, are identified.	EXAMPLES: • Use of common calibration equipment by the same crew on the same shift, a maintenance or test activity that requires realignment of an entire system, etc. • Incorrect calibration of steam generator level sensors; incorrect setting of torque switches. COMMENT: If plant specific procedures or finalized design information are not available, those calibration activities that if performed incorrectly can have an adverse

Task/ GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	The procedures which allow detecting the faulty alignment or calibration are also reviewed.	impact on the automatic initiation of standby safety equipment are identified using identification process (e.g. interview with design engineers).
HR-A03	Through a review of procedures and practices for shutdown POSs, those activities are identified that, if performed incorrectly, can have an adverse impact on the reactor coolant system level indications to the operators of the need for manual actuation	COMMENT: It is to account for the fact that many responses are manual during shutdown POSs. Past industry experience reveals that the reactor coolant system level indications are the most important.

TABLE 10.2-B ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-B 'SCREENING OF ACTIVITIES (PRE-INITIATING EVENT HRA)'

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-B	Screening of activities that, on the basis of the plant practices, can be argued to result in a likelihood of failure that is insignificant to risk.	COMMENT: This section refers to the screening of activities so that the potential human failures associated with them are not included in the PSA model.
HR-B01	Classes of activities that are performed in a similar manner (e.g. tests of MOVs) are screened only if the plant practices are such that they can be argued to result in the probability of equipment not being restored to standby status is small compared with other modes of unavailability of that equipment, i.e. failures or unavailability due to being out of service for maintenance. The activities are screened from applicability to subsequent POSs when any related HFE would be detected by administrative controls before transitioning from one POS to the next.	RATIONALE: It is possible to reduce the number of contributors to equipment unavailability due to human error to avoid unnecessarily complicating the system models, when those contributors do not impact the results significantly. EXAMPLE: Maintenance and test activities typically screened out from further consideration only if one or several conditions listed below are met: a) Equipment is automatically re-aligned on system demand; b) Following maintenance activities, a post-maintenance functional test is performed that reveals misalignment; c) Equipment position is indicated in the control room, status is routinely checked, and realignment can be affected from the control room, or d) Equipment status is required to be checked frequently (i.e. at least once a shift). EXAMPLE: The human error to leave a valve in wrong position after test may be excluded if there is an indication of the valve position in the main control room and an automatic signal to restore the operating status of the valve is supplied in case of demand for the system actuation. COMMENTS: Probabilities used for screening may be generated by application of simple HRA models, such as THERP [38]. (See also Table 10.2-D, general attribute HR-D02). Screening can only be done on a POS by POS basis, i.e. the screening criteria are to be met for each particular POS, for the activity to be screened.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-B02	Activities that result in multiple trains of a system or diverse systems or multiple systems within the only available (in some shutdown POSs) being made unavailable during the course of the activity are analysed in more detail, since the probabilities are compared to common cause failure probabilities. The applicability of screening when activities span multiple POSs is justified.	
HR-B03	For unique, one-of-a-kind activities, screening is performed only when it can be shown that, on the basis of the activity specific procedures, the defences in place to prevent the failure to return equipment to its required configuration will reduce the failure probability below that of other modes of unavailability of the equipment.	COMMENT: Use of these screening rules is typically justified through application of simple HRA models, such as THERP [38]. (See also Table 10.2-D, general attribute HR-D02). EXAMPLES of defenses include: - Equipment is automatically re-aligned on system demand and the associated control circuitry is not disabled as part of the activity. - A full functional test is always performed on completion of maintenance. - Equipment status is indicated in the control room, its status is monitored routinely, and realignment can be effected from the control room. - Equipment status is required to be checked locally on a frequent basis (e.g. once a shift), and the indications of misalignment are clear.
HR-B04	Screening of specific calibration activities is performed only when it can be shown that, on the basis of practices and procedures for calibration, the likelihood of a degree of miscalibration that will disable an important function is small in comparison with other failures or modes of unavailability, including CCF.	RATIONALE: It is possible to reduce the number of contributors to equipment unavailability to avoid unnecessarily complicating the system models, when those contributors do not impact the results significantly. COMMENT: Probabilities used for screening may be generated by application of simple HRA models, such as THERP [38]. COMMENT: Screening activities need to be POS dependent and there must be assurances that items screened for at power POS are not important for low power / shutdown POS.

TABLE 10.2-C ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-C ‘DEFINITION OF PRE-INITIATOR HUMAN FAILURE EVENTS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-C	Definition of pre-initiating human failure events for each modelled POS to model the impact of the failure in the system or functional failure model is performed within this task.	
HR-C01	For each unscreened activity, pre-initiator human failure events are defined that represents the impact of the human failure at the level appropriate to the modelling of the function, system, or component(s) affected.	RATIONALE: All significant contributors to equipment unavailability need to be included in the system models. COMMENTS: - The defined pre-initiator human failure events apply to the associated POS in which each is performed; – Miscalibration can be especially troublesome if only one train of equipment is available in some POS (e.g. it can lead to a so-called error of commission in stopping running equipment). EXAMPLE: If the consequence of the human failure is to make a train of a system unavailable, then the HFE will be included in the system model as a basic event representing the failure of that train from the human cause. If a miscalibration of torque switches potentially affects a number of valves, then the same HFE would be included as a cause of failure of each of those valves wherever they appear in the system models.
HR-C02	For shutdown POSs the average time and feasibility of detection of the pre-initiator human failure event is defined considering administrative practices.	RATIONALE: Pre-initiator human failure events performed in one POS may influence the plant response to accidents initiated in later POSs. Post-maintenance restoration tests may be delayed during plant transition. The time to detection of the pre-initiator HFE can determine the extent of impact in terms of which subsequent POSs may be affected.
HR-C03	The modes of unavailability due to pre-initiator human failure events that result from failure to restore initial system status after completion of each unscreened activity are included in the model.	EXAMPLE: The modes of unavailability typically considered that results from the following: a) Failure to restore equipment to the desired standby or operational status; b) Failure to restore initiation signal or failure to set point for equipment start-up or realignment;

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		c) Failure to restore automatic realignment or power.
HR-C04	Pre-initiator human failures events identified during the collection of plant specific or applicable generic operating experience, leading to failure modes that leave equipment unavailable for response in accident sequences, are considered and included in the model when applicable.	RATIONAL: Pre-initiator human failure events are relatively rare and may not be observed during operation of the particular plant. However, those human failure events that have been observed at other plants need to be reviewed and all those human failure events that are physically possibility at the plant under consideration need to be included in the PSA model.
HR-C05	The human failure events leading to miscalibration are included as a mode of failure of initiation of standby systems or a mode of failure to continue operation of running systems.	COMMENTS: Miscalibration can be especially troublesome if only one train of equipment is available in some POS (e.g. it can lead to a so-called error of commission in stopping running equipment).

TABLE 10.2-D ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-D ‘ASSESSMENT OF PROBABILITIES OF PRE-INITIATOR HUMAN FAILURE EVENTS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-D	Assessment of the probabilities of the pre-initiator human failure events is performed in a consistent way aimed to assure the justification of final human error probabilities (HEPs).	
HR-D01	The probabilities of the human failure events are estimated using a systematic process, so that the estimation is performed on a consistent basis. This is important to enable the HFEs to be included so that their relative importance is preserved.	COMMENT: Acceptable methods include THERP [38], ASEP [39], etc.
HR-D02	Screening values of the probabilities of the HFEs, based on a simple model, are used. When constructing models for estimating the HEPs, the characteristics of verification processes are considered, including: – Use of a written check-off list; Independence of verification of status; – Performance of a full functional test before the activity is considered complete; – Frequency of verification of status compared to frequency of performance of the activity.	RATIONALE: Typically, unavailability due to failure to reconfigure is not a major contributor when compared with other modes of unavailability. Therefore, in the case that the HFEs are included in the model, e.g. for completeness, a detailed model is unnecessary for many applications, and a simple screening estimation will suffice. COMMENT: Screening values for non-significant human failure basic events need to be based on limiting cases from simple models such as ASEP [39].
HR-D03	A detailed assessment of the HEP is performed for each HFE for which the screening HEP is comparable to the probabilities of other modes of unavailability. A detailed assessment requires a more thorough investigation of the plant practices and conditions (e.g. details of written procedures and plant layout) and results in a higher confidence in the determination of the significance to risk of the pre-initiator event activities. The detailed assessment considers the specific aspects of the procedures and the human machine interface.	RATIONALE: When the unavailability due to pre-initiator human failure events evaluated using a simple model is comparable with the probabilities of other modes of unavailability, a detailed assessment need to be performed to avoid non-realistic representation of pre-initiator human failure events in plant risk profile. COMMENT: The following plant specific relevant information can be included in the evaluation process: – Quality of written procedures (for performing tasks) and administrative controls for independent review (e.g. configuration control process, technical review process, training processes, and management emphasis on adherence to procedures); – Familiarity of the work teams with the written procedures; – Quality of the human machine interface, including both the equipment

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		configuration, and instrumentation and control layout.
HR-D04	The degree of dependence between HFEs is assessed taking into consideration whether there are common elements in their cause within the same POS.	COMMENT: Some analysts will argue that such dependent effects are included in the common cause failure events considered for the affected components. It is important, when such a claim is made, to ensure that this is indeed the case. In any case, the qualitative part of the assessment suggested here provides potentially valuable insights. EXAMPLES of common elements: the performance of the same activity on different trains of the same system by the same maintenance personnel in the same time frame; the use of a common procedure
HR-D05	The uncertainties in the HEP estimates are characterized consistent with the database used.	RATIONALE: Because there is little actuarial data on HEPs, they will be uncertain. An assessment of the uncertainty is important when using the results of a PSA so that the sensitivity of any conclusions drawn from the PSA can be examined. COMMENTS: Acceptable methods for characterization of the uncertainty include Bayesian updating or expert judgment. For the non-significant HFEs, the characterization of the uncertainty could include, for example, specification of the uncertainty range or use of conservative or bounding point estimates for HEPs.
HR-D06	The credibility of the estimates is checked by confirming that there has not been a significant history of restoration failures or miscalibration issues.	RATIONALE: Evidence of a history of problems points to the need for a more detailed examination. Lack of such a history provides support for the modelling assumptions and simplifications.
	HR-D06-S1 *The data collected for the parameter estimation task is reviewed for evidence of occurrences of misalignment or miscalibration problems. The results of the review are used to confirm the credibility of the estimates.*	*RATIONALE: A more complete investigation of the plant history can be obtained by looking through the plant maintenance records.* *COMMENT: This helps to ensure the reasonableness of the HEPs in light of the plant's experience.*

TABLE 10.2-E ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-E ‘IDENTIFICATION OF POST-INITIATOR OPERATOR RESPONSES’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-E	Identification of the set of operator responses following the initiating event is performed in a systematic way using appropriate information sources.	RATIONALE: The operator responses to be included in the accident sequence models for all initiating events need to be identified in a complete manner that none of operator responses that have the potential to influence accident progression is omitted. COMMENT: The identification process involves a systematic review of the relevant plant procedures.
HR-E01	The set of operator responses required to control and safely shutdown the plant following an initiating event is generated by reviewing all relevant operating procedures (e.g. emergency operating procedures, abnormal operating procedures, annunciator response procedures) to determine what actions are required for applicable POSs as a function of the plant status represented in the development of the accident sequences (See also Table 7.2-C, general attribute AS-C05). The following operator responses are identified: - Actions required to initiate, control, isolate, or terminate systems as required to prevent or mitigate core/fuel damage; - Actions required to change the status of components in order to fulfil a function required to prevent or mitigate core/fuel damage; - Actions required to be taken in response to the occurrence of internal or external hazard events (if any).	COMMENT: This task is an integral part of the development of the accident sequence model. EXAMPLES: - Isolation of a faulted steam generator, initiation of the RHR system, depressurization of the reactor coolant system (BWR); - Opening a PORV block valve. COMMENT: While most plants make extensive use of symptom-based procedures to respond to all plant conditions, there are still some plants that use event-based procedures for response to certain hazard events. These may contain actions that override the symptom-based procedures and prescribe alternate ways to control and shutdown the plant.
HR-E02	Actions taken in the control room (or other continuously manned stations) either in response to procedural direction, or as skill of the craft, to recover from a failure of equipment to automatically initiate or change state as required are identified.	RATIONALE: Failures of the initiation signals are typically a small fraction of the component failure probability, so that these recovery actions are typically not significant contributors to CDF/FDF. However, their inclusion leads to a more complete model. COMMENT: Because of cutset specific dependence of available time, these may be best incorporated in the model solution as recovery actions (see Table 10.2-H, Task HR-H). EXAMPLE: Manual starts of a standby pump following failure of auto-start.
	HR-E02-S1 *Significant errors of commission, i.e. actions that lead*	*RATIONALE: Errors of commission can lead to the creation of additional accident*

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	to additional functional unavailabilities, or inappropriately initiate system are identified.	*sequences.* *COMMENT: While it is not yet general practice to include errors of commission in the base PSA, it is advantageous to use information on the general causes of errors of commission (see for example, NUREG-1624 [40]) to reduce the potential for introducing changes that could increase the likelihood of, or create conditions conducive to, errors of commission. The methodology for the identification of errors of commission is not as well formulated as that of errors of omission. An example of an approach is ATHEANA [40].* *EXAMPLE: An error of commission might be securing an injection system inappropriately.*
HR-E03	Actions taken outside the control room in response to procedural direction or control room abandonment are identified for specific accident sequences related to specific hazards (e.g. fire, flooding, seismic, etc.).	RATIONALE: Control Room abandonment may be required due to the control room becoming un-inhabitable, or as a result of loss of functions needed to protect the core.
HE-E04	When identifying the key human response actions system operation procedures and actual plant experience is reviewed in the content of accident scenarios in order to get understanding of how the system(s) functions and the human interfaces with the system is obtained.	
HR-E05	The procedures are reviewed with plant operations and training personnel to confirm that the interpretation of the procedures, and the expected responses are consistent with training and plant operational practices. A detailed talk-through of the procedures and sequences of events is performed.	RATIONALE: The written procedures may not always give a preference of the order in which the various options available to provide for a required safety function are exercised.
HR-E06	Simulator exercises are observed to gain a general understanding of crew dynamics, and the use of the procedures. Talk-through with operators the simulator observations is performed to confirm that the human response actions for accident scenarios are identified and information useful for the assessment of the performance shaping factors is obtained.	RATIONALE: Such exercises and talk-through give information on performance shaping factors, such as the presence of distracting annunciators, the timing associated with the actions, the complexity of the actions, etc. An understanding of the performance shaping factors is important for the evaluation of the HEPs. *COMMENT: For specific accident sequences that are not completely addressed in plant procedures simulator exercises to observe operator response could be additionally performed. The following accident sequences could be examined in more details using simulator exercises:*

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
			- *Sequences with failures of the redundant equipment involved in several modelled functions;* - *Sequences with error forcing content (e.g. due to wrong annunciations or alarms);* - *Sequences for which procedures do not provide clear guidance or set up conditions that can be misunderstood, etc.* - *EXAMPLE: During Three Miles Island accident operators disconnected high pressure injection pumps due to wrong understanding on the level in the reactor and position of pressurizer safety valve.*
HR-E07	In the PSA for hazards; the hazard specific human interactions are identified. For hazards that involve multiunit initiating events and/or accident sequences interactions associated with the need to manage multiple reactor units are considered.		RATIONALE: Depending on the nature of the hazard it is rational to assume human interactions in addition to those identified in the PSA for internal initiating events. Some of these are based on specific operating instructions for the hazard, such as fire response procedures. COMMENT: Hazard specific HRA may result in the identification of some actions which are not applicable or credited in the hazard specific PSA. Some are not applicable (e.g. Fire-induced steam generator tube rupture actions), while others may not be feasible such as recovery of a component located within a flood or fire compartment.
	HR-E07-S1	*Any new undesired operator actions in response to hazards -induced spurious indications or alarms are identified.*	*COMMENT: Undesired operator actions are in response to procedural compliance following a spurious alarm. These actions may result in stopping equipment needed in the PSA, but may be recoverable.*
HR-E08	In the PSA for hazards all of the human interactions identified in the PSA for internal initiating events are revisited and examined if they are relevant to the hazard induced event sequences. Those that are not relevant are removed from the PSA for hazards.		
E09	In the PSA for hazards, hazard-specific human interactions are identified for inclusion in the PSA.		RATIONALE: Many plants have specific procedures for responding to the occurrence of fires, internal or external floods, high winds, etc.

TABLE 10.2-F ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-F 'DEFINITION OF POST-INITIATOR HUMAN FAILURE EVENTS'

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-F	Definition of human failure events for each POS that represent the failure to respond or not properly performed respond as required that are consistent with the structure and level of detail in the accident sequence models.	
HR-F01	Human failure events representing the impact of failure to perform a required action function at the function, system, train, or component level, as appropriate are identified and included in the plant logic model. Failures to perform more than one response are grouped into a single HFE only if the impact on the accident sequence development is the same or can be bounded.	EXAMPLES: An HFE may be included in the plant logic model in a number of ways: - As an event tree branch point; - As a contributor to a functional level fault tree used to evaluate the failure of a function or system; - In a system fault tree as a mode of unavailability of a component, segment, or train.
HR-F02	The definition of each HFE in preparation for estimation of its probability is completed by specifying the scenario specific factors including: - POS and event sequence specific timing of cues, and time window for successful completion; - The scenario specific procedural guidance; - Availability of cues and/or other indications for alerting the operators to the need for action; - Availability of systems, or components identified in the procedures; - The specific detailed tasks (e.g. at the level of trains or individual components, such as pumps or valves) required to achieve the goal of the required for the response; - The event sequence depending evolution of the performance shaping factors; - The interactions between persons involved in the response to the	COMMENT: Many existing HRA models (i.e. methods for calculating human error probabilities) do not address some of these factors explicitly. However, it is necessary to understand the factors, at least qualitatively so that general attribute HR-G06 (Table 10.2-G) can be satisfied. COMMENT: Multiunit accidents are particularly important when hazard events are being evaluated. Multiunit hazard events were defined in HE-C, and each relevant HFE need to be evaluated specifically for those events. COMMENT: Information on the development of the event sequence can help to understand how the change in the PSFs related to the accident sequence progression affects human performance. COMMENT: Interactions between persons involved in the response to the accident are not limited only to interactions between plant operators, but for instance with the authorities that can influence the response (e.g. by delaying the response). EXAMPLE: During the accident at Fukushima Daiichi the containment venting was delayed due to the delay with the permission for the venting from the responsible authority.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	accident; - The impact of various hazard events that can be occurring when the HFE is considered; - The impact of multiunit accidents.		
	HR-F02-S1	*Hazard specific definitions for each HFE are performed and include sequence definitions such as sequence timing, as well as performance shaping factors such as the impact of flooding, smoke or blocked access.*	

TABLE 10.2-G ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-G 'ASSESSMENT OF PROBABILITIES OF POST-INITIATOR HUMAN FAILURE EVENTS'

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-G	Assessment of the probabilities of the post-initiator human failure events and a characterization of the associated uncertainties and dependence between the events in the same accident sequence are performed using a well-defined and self-consistent process that addresses the plant specific and scenario-specific influences on human performance and appropriate methodologies and data.		
HR-G01	Detailed assessment of the HEPs is performed for the significant HFEs Screening values are used for the non-significant HFEs.		COMMENTS: – The identification of the significant HFEs is an iterative process requiring several quantifications of the PSA model; – A significant HFE is one that contributes measurably to the current level of risk, or is relied upon to achieve the current level of risk. An example of criteria that can be used to determine significance is the following: a significant basic event has a Fussell-Vesely importance measure (F-V) greater than a predefined number (i.e. 0.005 or 0.01), or a Risk Achievement Worth (RAW) greater than a predefined number (i.e. 2). Alternative importance measures and criteria may be used.
	HR-G01-S1	*A detailed assessment is performed for each HFE.*	*RATIONALE: Performing a detailed assessment of all HFEs avoids the need for iteration.*
HR-G02	The method used to assess HEPs addresses failure in cognition (detection, situation assessment, and response planning) as well as failures in execution.		RATIONALE: Failures in cognition can the more important contributors to failure, and furthermore, can be a significant source of dependence between HFEs (see HR-G08).
	HR-G02-S1	*The method used to assess HEPs is capable of evaluating the impact of procedure changes.*	*RATIONALE: Evaluation of the impact of procedural changes is essential for applications aimed to optimize EOPs and AMPs.*
HR-G03	The model addresses performance shaping factors on a scenario and plant specific basis for the applicable POSs, including treatment of: - Time at which cues are received, time required to perform the response, and the time available to complete the response; - Quality of the written procedures and administrative controls;		COMMENT: Many HRA models do not deal with each of these factors explicitly. However, they need to be taken into account when comparing the relative values of HEPs (see HR-G06). The complexity may be assessed in part on the basis of a task analysis. Task analyses can be performed at a number of different levels of detail as required by the model used to quantify the HEPs.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	- Availability of instrumentation needed to take actions; - Quality of the operator training or experience; - Human machine interface; - Degree of clarity of cues/indications; - Complexity of detection, diagnosis, decision making, and executing the required response; - Environment (e.g. lighting, heat, radiation) under which the operator is working; - Accessibility of the equipment requiring manipulation; - Distractions caused by parallel tests and maintenance activities and shutdown plant transition tasks; - Crew interactions and communication; - The interactions between persons involved in the response to the accident, etc.	COMMENT: The following are examples of additional performance shaping factors: - The type (classroom or simulator) and frequency of training on the response; - Whether the human actions are associated with a multiunit initiating event or accident sequence; - The effects of the occurrence of hazard events (including degraded PSFs occurring as a result of hazard-induced damage to SSCs or environmental changes). For a specific type of operator response, these factors can vary depending on the scenario being modelled, e.g. a loss of a dc bus may affect the availability of instrumentation. When the response requires actions outside the control room, the following factors are taken into account in addition to the above: - Need for special tools; - Time to reach physically the place if not permanently occupied; - Communication issues between MCR and local personnel; - The effects of the occurrence of hazard events (e.g. blockage of travel path/area access).
HR-G04	The timeline for occurrence of cues and the evaluation of the time available to complete the action is based on applicable realistic generic thermal hydraulic analyses or simulation from similar plants (e.g. plant of similar design and operation) for each applicable POS. The points in time when operators are expected to receive relevant indications are specified.	RATIONALE: Depending on the method used to estimate the HEPs, a precise evaluation of the times may not be necessary. For those that are based primarily on time, the SA HR-G04-S1 applies.
	HR-G04-S1 *The time line is based on plant specific thermal hydraulic analyses and/or simulator exercises.*	
HR-G05	For those HFEs for which a detailed evaluation is performed, the time to complete the action is based on actual time measurements in walkthroughs, plant specific realistic thermal hydraulic analysis, talk-through of the procedures, or simulator observations.	RATIONALE: Depending on the method used to estimate the HEPs, a precise evaluation of the times may not be necessary. However, as a minimum, an estimate of the time is needed to confirm the feasibility of the actions. COMMENT: For actions outside the control room it is useful to include discussion of what operators would do if the normal path was blocked (e.g. alternate paths) or if

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		normal communication systems were damaged (e.g. carry radios).
HR-G06	For those HFEs that are applicable and credited for hazard events, the effect of the hazard event on the performance shaping factors is considered. Special attention is given to the effect of the damage caused by the hazard event on the context of the action. Additional consideration is given to the damage or plant environmental conditions that can prevent or inhibit operators from performing actions.	COMMENT: Hazard events can affect the HEPs in a number of ways. Some are direct (blocked access, disabled equipment, injuries to operators, etc.) where are others are indirect (loss of instrumentation and false alarms, reduction is available manpower, distraction, degradation in environmental conditions, etc.) COMMENT: Many HEPs may be quantified in the base internal events model assuming specific PSFs. When these events are re-analysed for a specific hazard, the PSFs will likely change, resulting in a modified HEP.
HR-G07	After estimation of the HEPs, the relative values are assessed to ensure their reasonableness given the scenario context, plant history, procedures, operational practices, and experience and to check that they are reflective of the impact of the various performance-shaping factors identified in HR-G03 above.	RATIONALE: Assessment of HEPs could be based on very complicated methods, but not on actuarial data; therefore, the absolute values of HEPs are always uncertain and it might be the case that actions that are simpler receive higher HEPs than those that are more difficult to perform. COMMENT: When HRA is performed correctly, the simpler actions receive lower HEPs that more complicated. This assessment helps to identify potential errors in the analysis.
HR-G08	The degree of dependence between HFEs appearing in the same accident sequence or cut set (i.e. including pre-initiator, human-caused initiator, and post-initiator HFEs including recovery actions) is assessed taking into account the influence of success or failure in preceding human actions and system performance on the human response under consideration. - Time required to complete all actions in relation to the time available to perform the actions; - Factors that could lead to dependence (e.g. common instrumentation, common procedures, increased stress, etc.); - Availability of resources (e.g. personnel). A joint human error probability that reflects the dependence and conditional probability of the second, third, etc. event, given failure of the first, second, etc. is evaluated. As a minimum, the following factors affecting the degree of dependence are included: - Time required to complete all actions in relation to the time available to perform the actions;	RATIONALE: This is a crucial attribute. Because accident sequence models are developed in terms of discrete functions or in terms of separate systems, consideration of HFEs for each function or system in isolation can lead to excessive credit for operator action unless the dependency is accounted for. COMMENT: The assumption of independence is supported by arguments such as: - The required actions are separated sufficiently in the development of the accident sequence. - The cues for subsequent actions are independent of those for prior actions. - The workload is not significantly increased by virtue of the failure of the prior actions. - The second action would be required whether or not the first were required. COMMENT: Dependency can vary POS by POS and can occur across POSs for actions whose latent impacts (e.g. due to pre-initiator HFEs) are applicable to subsequent POSs.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	- Factors that could lead to dependence (e.g. common instrumentation, common procedures, use of common cues, increased stress caused by failure of the first response, etc.); - Availability of resources (e.g. personnel). The assumption of independence between HFEs is justified.	
HR-G09	A characterization of the uncertainty in the HEPs is provided, consistent with the quantification method.	RATIONALE: Because there is little actuarial data on HEPs, they will be uncertain. An assessment of the uncertainty is important when using the results of a PSA so that the robustness of any conclusions drawn from the PSA can be examined. COMMENT: For significant HEPs acceptable methods include Bayesian updating or expert judgment. For the non-significant HFEs the uncertainty characterization could include, for example, specifying the uncertainty range, qualitatively discussing the uncertainty range, or identifying the estimate as conservative or bounding.
HR-G10	Hazard induced effects on the operators' performance shaping factors are taken into account. As a minimum, the following hazard induced effects on the operators' performance shaping factors are taken into account: a) Availability of pathways to specific structures, systems and components after a hazard event; b) Unavailability or reduced availability of specific SSCs affected by the hazard; c) Increased stress levels; d) Failures of indication or false indication; e) Failure of communication systems.	RATIONALE: The hazard may affect the conditions to the human interactions, therefore hazard specific human HRA should re-evaluate the related performance shaping factors and re-quantify the related human error probabilities. COMMENT: The listed factors may not be the only ones relevant to the specific hazard. An assessment need to be performed to consider other applicable factors impacting the operators' behaviour
HR-G11	The probabilities of all post-initiator human errors that could occur in response to the initiating event, as modelled in the Level 1 PSA for internal initiating events, are revised and adjusted for the specific hazard conditions and multiunit considerations as-applicable.	
HR-G12	In the PSA for hazard events, the effect on operator diagnosis from hazard-induced erroneous indications are considered, up to one parameter, one channel of multiple parameters, or the effect of one group	RATIONALE: Because of the high reliability and redundancy of instrumentation, most instrument failures are screened from the internal events PSA as an impact on the operators. However, other hazards may have effects that defeat that reliability and

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	of correlated failures.	redundancy. COMMENT: The considerations are different for different hazards. Some examples are: *Fire:* If the fire damages indications directly such that they are disabled, then all disabled instrumentation is accounted for in its “failed when no signal” or “failed when no power” state. When the concern is a spurious signal (as would be caused by a short), then only such occurrence for all channels of a single parameter or for all parameters on a single channel (depending on the cables affected by the fire.) *Seismic:* Similar to fire, if the seismic event causes failure of a correlated set of control cabinets, or the power to them, then all signals would be accounted for in their “failed when no signal” or “failed when no power” state. When the concern is spurious signals due to relay chatter, then it is only necessary to consider the impacts from a single set of correlated relays (i.e. the set of relays would have the same effect on the indications affected by the relays.) From these examples, the extrapolation to other hazards can be made.
HR-G12	In the PSA for hazard events, for scenarios that involve correlated hazard event, including hazard-induced internal fires and floods, the performance shaping factors are adjusted for the impacts of the combined hazard impacts.	

TABLE 10.2-H ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-H ‘RECOVERY ACTIONS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-H	Identification of plausible and feasible recovery actions (at the cutset or scenario level) after the initial solution of the PSA model for each hazard and each POS.	COMMENT: Recovery actions are actions taken in addition to those normally identified in the review of emergency, abnormal, and system operating procedures, which would normally be addressed in PSA. They are included in PSA when failure to take credit for recovery would distort the insights from the risk analysis. COMMENT: Recovery actions do not include repair of the equipment. EXAMPLE: The following recoveries are typically considered: manually opening a valve that had failed to open automatically, manual start of the pumps in case of automatic start failure, etc.
HR-H01	Recovery actions that can restore the functions of systems or components are included on an as-needed basis to provide a more realistic evaluation of significant accident sequences. .	COMMENTS: 1) Use of diverse or alternative means is considered as recovery actions; 2) The recovery actions are included in the model at a level (e.g. scenario, cutset) such that the context (e.g. PSFs) associated with that level, which determines the probability of the recovery action, can be regarded as uniform. For example, such actions are often included at the cutset level, because the context (e.g. time available to perform the action) can vary from cutset to cutset.
HR-H02	Recovery actions are credited only if: – A procedure or procedural guidance is available and operator training has included the action as part of crew's training, AND – Cues (e.g. an annunciator) alerts the operators to the need for action OR the procedure directs the operator to check the status of the component, AND – Attention is given to the relevant performance shaping factors provided in Requirement HR-G03, AND – Feasibility of the action is confirmed and there is sufficient manpower to perform the action,	COMMENT: Recovery actions may be applicable for the base internal events model, but not applicable to specific hazards or shutdown POSs. Additionally, hazard or POS specific procedures (such as fire emergency response procedures or shutdown procedures) may involve new recovery actions applicable to that hazard or POS. COMMENT: When procedure is not available or operator training has not been included in the crew's training it is still possible to credit recovery action when the justification for the omission for one or both is provided. EXAMPLE: Skill of the craft recovery action, i.e. one for which a procedure is not needed as it is one that, because of the operator’s skill and experience, is clearly identifiable.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	– AND – Any environmental effects (e.g. high temperatures, loss of visibility) associated with the scenario do not preclude the recovery actions.	
HR-H03	The potential for dependency between recovery actions and any other HFEs in the accident sequence cutset, including dependency with any human-caused initiator human failure event causing the initiating event, and dependency with initiating events or accident sequences on another unit, is assessed.	RATIONALE: The need for recovery actions is generally recognized by the control room crew responsible for the performance of the proceduralized actions modelled in the event trees and fault trees. Therefore, there may be performance shaping factors that affect both recovery and proceduralized actions.
HR-H04	In case of crediting recovery for hazard events, the recoveries modelled in the internal events PSA are re-evaluated to account for the effects of the external hazard. The recovery models are adjusted accordingly.	RATIONALE: The recovery actions may be more complex, less reliable or even not possible after a hazard event. See also HR-G06
HR-H05	Recovery actions that cannot be performed due to the impact of the hazard of certain severity are set to fail in the PSA model.	EXAMPLE: If there is no access to the fire affected room, the field operator cannot perform manual closing of the valve located in that room, which was considered in the PSA for internal initiating events as a recovery of the failure of automatic closing of the same valve due to loss of electric supply of the valve.

TABLE 10.2-I ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-I ‘IDENTIFICATION OF HUMAN FAILURE EVENTS THAT COULD LEAD TO AN INITIATING EVENT’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-I	A through identification of routine test activities, maintenance activities, and activities needed to execute plant transitions for each modelled POS that could result in initiating events if incorrectly carried out.	
HR-I01	The set of test activities, maintenance activities, and plant shutdown transition activities that require realignment of equipment (i.e. as part of normal operation and standby status), or involve changes in reactor coolant circuit level (e.g. drain downs), and that involve a mechanism that could result in an initiating event if incorrectly carried out is generated by reviewing procedures, practices and discussions with relevant plant personnel.	COMMENT: These include activities to align or remove systems from service and to perform the necessary system manipulations need to affect POS transitions. Normal operational or standby conditions vary by POS. Reviews of LPSD operational events can assist the analysts to identify activities and alignments that have led to HFEs causing an initiating event.
HR-I02	The set of calibration activities that if performed incorrectly can lead to automatic initiation or trip of safety equipment is generated through a review of procedures and practices.	
HR-I03	Generic analyses and operating experience for all modelled POSs for similar plants is reviewed to assess whether the initiating events caused by HFEs included in the model accounts for industry experience, and to track cases where human-caused initiator human failure events impact later human responses.	

TABLE 10.2-J ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-J ‘GROUPING OF HUMAN - FAILURE EVENTS THAT COULD LEAD TO AN INITIATING EVENT’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-J	Grouping the identified HFEs that could lead to an initiating event for each modelled POS so that events in the same group have similar mitigation requirements (i.e. the requirements for most events in the group are less restrictive than the limiting mitigation requirements for the group) to facilitate an efficient but realistic estimation of CDF/FDF resulting from human failure events that represent the failure to respond as required and that are consistent with the structure and level of detail in the accident sequence models.	
HR-J01	For each modelled POS HFEs that could lead to an initiating event are combined into initiating event groups to facilitate definition of accident sequences in the accident sequence analysis element and to facilitate quantification in the Quantification element.	
HR-J02	HFEs that could lead to an initiating event are grouped for a given POS only when the following can be assured: (a) The events are all applicable to the POSs; (b) The events can be considered similar in terms of plant response, success criteria, timing, and the effect on the operability and performance of operators and relevant mitigating systems; (c) The events can be shown to be bounded by the worst case impacts within the “new” group, without being overly conservative.	COMMENT: A grouping valid for one POS may not be appropriate for another. Identifying the “bounding” or “worst case” could also require a careful review of plant operational practices. COMMENT: The intent here is similar to that done when grouping initiating events, since this is just another cause of initiating events. The sum of the HEPs for all of the HFEs in the group will be converted to a frequency (by considering the number of opportunities per year) and will represent the total frequency of the given human-caused initiating event. Therefore, the individual failures in the group must be reasonably representative of the same initiating event.
HR-J03	Events with different plant response (i.e. those with different success rate criteria) impacts or those that could have more severe radionuclide release potential (e.g. LERF) are grouped separately from other initiating event categories.	
	HR-J03-S1 *For multiunit sites with shared systems, HFEs that could lead to a multiunit initiating event are not subsumed into initiating event groups if they impact*	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	mitigation capability differently.	
HR-J04	HFEs that could lead to an initiating event are grouped separately with hardware failures to allow proper accounting of dependencies between HFEs.	

TABLE 10.2-K ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-K 'ASSESSMENT OF FREQUENCIES OF HUMAN FAILURE EVENTS THAT COULD LEAD TO AN INITIATING EVENT'

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-K	The assessment of the annual frequency of initiating events or initiating event groups made up of HFEs that could lead to an initiating event is performed.	
HR-K01	Estimation of frequency of the activity and of the HEPs conditional on the occurrence of the activity is performed for the human-caused initiator HEPs associated with test and maintenance activities and plant transition activities using a systematic process consistent with the requirements of HR-D or expert judgment.	
HR-K02	Detailed assessment in the quantification of HEPs conditional on the occurrence of the associated activity is performed for the significant HFEs associated with test and maintenance activities and plant transition activities. Screening values are used for the non-significant HFEs.	COMMENTS: – The identification of the significant HFEs is an iterative process requiring several quantifications of the PSA model. – A significant HFE is one that contributes measurably to the current level of risk, or relies upon to achieve the current level of risk. An example of criteria that can be used to determine significance is the following: a significant basic event has a Fussell-Vesely importance measure (F-V) greater than a predefined number (i.e. 0.005 or 0.01), or a Risk Achievement Worth (RAW) greater than a predefined number (i.e. 2). Alternative importance measures and criteria may be used.
	HR-K02-S1 *A detailed assessment is performed for each HFE.*	*RATIONALE: Performing a detailed assessment of all HFEs avoids the need for iteration.*
HR-K03	The joint HEP of HFEs that could lead to an initiating event associated with test and maintenance or plant transition activities is assessed if multiple HFEs are needed to cause the initiating event and they are identified as having some degree of dependency (i.e. having some common elements in their causes, such as performed by the same crew in the same time frame).	
HR-K04	Initiating event frequencies for HFEs that could lead to an initiating event for each applicable POS are calculated on a per reactor year basis.	COMMENT: It is important to account for whether the failure event being represented will occur during the POS under consideration.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	The initiating event frequency analysis for the frequency in an average year accounts for each applicable POS how frequently each POS is entered and hence each activity potentially leading to HFEs is challenged.	
HR-K05	Screening criteria for HFEs that could lead to an initiating event are consistent with criteria used in IE-B01.	COMMENT: Part (c) of IE-B01 does not apply to shutdown conditions but does apply to low power conditions.
	HR-K05-S1 *If the shutdown PSA is to be used for other types of analyses (e.g. for configuration risk management applications), then it is possible that different numerical criteria might need to be developed. Development and defence of such criteria would be a unique obligation of such an analysis.*	*COMMENT: For evaluation of a specific outage, screening on an initiating event frequency not adjusted by the fraction of time in a POS may be necessary to avoid inappropriate loss of the risk contribution of POSs with high conditional core/fuel damage frequencies.*
HR-K06	The consistency of the quantification of HEPs for HFEs that could lead to an initiating event is checked. The HFEs, associated HEPs, and their final initiating event frequencies relative to each other are reviewed to check their credibility given the procedures, operating practices, plant history, and experience.	
HR-K07	The uncertainty in the initiating event frequencies for HFEs that could lead to an initiating event is characterized in a manner consistent with the quantification approach.	COMMENTS: - Acceptable methods of characterization of uncertainty include Bayesian updating or expert judgment; - For non-significant HFEs mean values for use in the quantification can be used. The characterization of uncertainty could include, for example, specifying the uncertainty range, qualitatively discussing the uncertainty range, or identifying the estimate as conservative or bounding.

TABLE 10.2-L ATTRIBUTES FOR HUMAN RELIABILITY ANALYSIS: TASK HR-L ‘DOCUMENTATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-I	Documentation and information storage is performed in a manner that facilitates peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the assumptions made and their bases.	
HR-I01	The following aspects of the human reliability analysis process are documented: – HRA methodology; – Approach used to identify HFEs; – Methods used to estimate HEPs; – Approach to the assessment of dependency; – Definition of each HFE; – Description of correct action; – Discussion of errors that would fail the action; – Assumptions; – Basis for the timeline; – Results of operator interviews; – Summary of procedures used for the action; – Discussion of cues; – Basis for each HEP: ○ Screening values ○ Detailed HEP evaluations: ▪ Factors used in the quantification of the HEPs ▪ Hazard specific PSFs and timing ▪ How they were characterized ▪ How they were incorporated in the quantification.	
HR-I02	The sources of model uncertainty and related assumptions associated with the human reliability analysis are documented.	

11. PSA ELEMENT ‘DA’: DATA ANALYSIS

11.1. MAIN OBJECTIVES

The objective of the data analysis is to provide estimates for the parameters, called reliability parameters, of the reliability models specified under systems analysis. The reliability models serve to determine the probabilities of the basic events representing specific equipment failures and unavailabilities.

Reliability parameters typically include:

- Failure rates;
- Probabilities for failure on demand;
- Unavailabilities due to maintenance or test;
- Test and maintenance frequencies and repair, test, and maintenance durations;
- Mission times as specified in systems analysis;
- Common cause failure (CCF) model parameters.

Important aspects and characteristics of reliability parameters are the following:

a) Parameters, whether estimated on the basis of plant specific or generic data, or both, appropriately reflect design and operational features of the plant;

b) Component or system unavailabilities due to repair, test and maintenance are properly accounted for;

c) Uncertainties in the data are understood and accounted for.

Note: The parameters of reliability models as discussed here should not be confused with the parameters of probability distributions used to describe the uncertainty of reliability parameters.

11.2. DATA ANALYSIS TASKS AND THEIR ATTRIBUTES

Table 11.1 lists the main tasks for the PSA element ‘Data Analysis’. Tables 11.2-A through 11.2-H present the description of general attributes and special attributes for these tasks.

TABLE 11.1 MAIN TASKS FOR DATA ANALYSIS

Task ID	Task Content
DA-A	Reliability model parameter identification
DA-B	Component grouping for parameter estimation
DA-C	Collecting and evaluating generic information
DA-D	Plant specific data collection and evaluation
DA-E	Derivation of plant specific parameters, integration of generic and plant specific information
DA-F	Derivation of plant specific parameters for common cause failure events
DA-G	Use of mechanistic models (fragility analysis)
DA-H	Documentation

TABLE 11.2-A ATTRIBUTES FOR DATA ANALYSIS: TASK DA-A ‘RELIABILITY MODEL PARAMETER IDENTIFICATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-A	Each reliability parameter is identified for the reliability models as defined in systems analysis in terms of the logic failure model (fault trees, event trees or special failure model) and basic event characteristics and boundary. The reliability models and their parameters are identified under Task SY-B.	
DA-A01	From systems analysis, the reliability models for which parameters are required are identified. Associated equipment boundaries, failure modes, and mission success criteria are identified consistent with the corresponding basic event definitions in systems analysis for failure rates, failure probabilities, unavailabilities, and common cause failure parameters. Boundaries of unavailability events are defined consistent with corresponding definitions in systems analysis.	EXAMPLE for a component mission success criterion: Minimal flow rate for 2 hours. Basic events and associated reliability models for which parameters are required typically include: a) Independent or common cause failure of a component or system to start or change state on demand; b) Independent or common cause failure of a component or system to continue operating or provide a required function for a defined time period; c) Equipment unavailability to perform its required function due to being out of service for repair or maintenance; d) Equipment unavailability to perform its required function due to being tested; e) Failure to recover a function or system (e.g. failure to recover off-site power); f) Failure to repair a component, system, or function in a defined time period; g) Equipment failure caused by hazard initiating events; h) Spurious operation caused by fire-induced circuit failure.
DA-A02	Basic event IDs are established based on the plants system and equipment ID system as far as feasible. Thus, equipment and system IDs are normally contained in associated basic event IDs. Deviations from this principle are justified and the exact correlation between basic events and plant equipment is established and documented. A database of basic events and associated reliability models is established containing the exact correlation to specific plant equipment.	
DA-A03	The parameters are estimated and the data required are identified.	EXAMPLES are as follows: a) For failures on demand the parameter is the probability of failure or unavailability on demand, and the data required are the number of failures given a number of

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		demands. Basically this representation corresponds to a binomial probability model. b) For standby failures (if standby failures are described in this manner) and operating failures, the parameter is the failure rate, and the data required are the number of failures in the total (standby or operating) time. Basically, this representation corresponds to a Poisson probability model.

TABLE 11.2-B ATTRIBUTES FOR DATA ANALYSIS: TASK DA-B ‘COMPONENT GROUPING FOR PARAMETER ESTIMATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-B	Components are grouped into appropriate population groups for parameter estimation.	
DA-B01	The rationale for grouping components into a homogeneous population for parameter estimation considers the design, environmental, functional and operational conditions of the components in the as-built and as-operated plant. For parameter estimation, components are grouped according to type and according to the detailed characteristics of their usage	EXAMPLE: Functional and operational conditions regarding centrifugal pumps. Different parameters can be defined for low pressure pumps with different functional and operational conditions: - On-line cooling water systems which are required also post trip versus cooling systems normally in standby; - Cooling water systems circulating raw water versus cooling water systems circulating clean water; - Well water pumps. COMMENT: Examples of detailed characteristics include: a) Design/size; b) System characteristics: – standby, operating – operational conditions (e.g. clean vs. untreated water, air) – maintenance practices – frequency of demands; c) Environmental conditions; d) Other appropriate characteristics including manufacturer. Not included in the definition of a group are obvious outliers (e.g. valves that are never tested and unlikely to be operated are not grouped together with those that are tested or otherwise manipulated frequently). The grouping and the grouping rationale are included in the database. COMMENT: 1) A too narrow population in a group may lead to a sample of plant specific data that is not statistically significant. 2) Components affected by the hazard should not be part of the population formed in the PSA for internal initiating events.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	DA-B01-S1	*For specific applications, such as the assessment of test procedures for certain types of pumps, a refinement of the component grouping is advisable. This refinement provides the resolution required for these specific applications.*	*RATIONALE: A too broad population within a group may mask or average-out the specific features of particular components. This in turn could significantly hinder certain applications.*

TABLE 11.2-C ATTRIBUTES FOR DATA ANALYSIS: TASK DA-C ‘COLLECTING AND EVALUATING GENERIC INFORMATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-C	Generic information is collected and evaluated regarding its applicability. Appropriate generic parameters are selected or parameters are composed for the plant from applicable generic sources and provide traceability.	
DA-C01	Generic information on failures and unavailabilities appropriate for the POS is collected in order to account for a broader range of conditions and exposure (exposure time or total number of demands) as available from the limited plant experience. The information may include raw data, e.g. failure events and associated exposure, or may only be in the form of reliability model parameters such as failure rates. The source and the derivation process of the generic parameter estimates are identified and described. The parameter definitions and boundary conditions are evaluated in view of consistency with component identification and grouping. Generic data for unavailability due to test, maintenance, and repair have to be used with caution since different plants can have different test and maintenance philosophies. The generic information is evaluated regarding its applicability for the plant, considering the characteristics, design and operational features of the equipment for which this information is intended to be applied. The collection and evaluation of generic information includes an assessment of the uncertainty in the original data.	EXAMPLE: Sources of uncertainties regarding the use of generic reliability parameter: - Differences in component design and operational features; - Differences in test, repair and maintenance practices; - Quality of the generic data (e.g. completeness); - Statistical uncertainties.
DA-C02	Generic parameters for the plant are composed or selected. Information from different plants is integrated to obtain suitable generic parameters using Bayesian methods, classical approaches and expert judgment. The selection of generic parameters or the composition of generic information into a parameter applicable for the plant includes an appreciation and an assessment of the uncertainties involved in the original data and in using them for the plant.	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	DA-C02-S1	*For new equipment, the use of generic data and manufacturer data for the assessment of reliability parameters is justified.*	*COMMENT: The use of only manufacturer data for new equipment may not reflect the equipment reliability in real operational conditions. The use of justified generic data with supplemental consideration of manufacturer data may help to avoid excessive optimism in estimation of reliability parameters.*
DA-C03	The same generic estimates are used for multiple POSs if the generic estimates are justified to be applicable for all such POSs.		RATIONALE: The data collected and used must be applicable to the POS being evaluated. This may include data from the specific POS and any other POSs in which the equipment performance would be expected to be similar. Use of the same data in multiple POSs requires care and justification. COMMENT: Generally, equipment failure data are no different during shutdown than during operations. However, several factors are important, when considering using normal failure data. The following factors can affect all parameter estimates, not just equipment failure rates: - Long outages with equipment far outside normal operating conditions and test practice can affect successful performance; - Systems analysis models can account for different test and operating practice during the outage; Parameter estimates are affected by special configurations that occur during shutdown POSs.

TABLE 11.2-D   ATTRIBUTES FOR DATA ANALYSIS: TASK DA-D ‘PLANT SPECIFIC DATA COLLECTION AND EVALUATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-D	Plant specific data collection and evaluation is performed in a consistent and systematic way. Plant specific data is collected in accordance with the parameter definitions and the grouping.	
DA-D01	Plant specific data for the basic event/parameter is collected. The following data is collected: (1) Failure data: equipment failures, planned and unplanned maintenance, test events, time between tests and mission time; (2) Success data: exposure to demands and, depending on the type of equipment, the exposure to standby and operation.	COMMENT: Plant changes may affect available reliability parameters by changing operational conditions. For newly added equipment, new parameters are required. As for the ‘base case PSA’ data analysis, the parameter estimates are based on relevant generic industry and plant specific evidence. Where applicable, generic and plant specific evidence are integrated using acceptable methods to obtain plant specific parameter estimates. Each parameter estimate is accompanied by a characterization of the uncertainty. COMMENT: If modifications to plant design or operating practice lead to a condition where past data are no longer representative of current performance limit the use of old data: a) If the modification involves new equipment or a practice where significant generic parameter estimates are available, parameter estimates updated with plant specific data as it becomes available are used; or b) If the modification is unique to the extent that generic parameter estimates are not available and only limited experience is available following the change, then the impact of the change is analysed and the hypothetical effect on the historical data is assessed to determine to what extent the data can be used.
DA-D02	Plant specific data from as broad a time period as possible is collected, consistent with uniformity in design, operational practices, and experience. The rationale for screening or disregarding plant specific data is justified (e.g. plant design modifications, changes in operating practices).	
DA-D03	When evaluating maintenance or other relevant records to extract plant specific component failure event data, a clear basis for the identification of events as failures is required: (a) The distinction is made between those degraded states for which failure, as modelled in the PSA, would have occurred on demand	COMMENT: Failures in post-maintenance testing need to be screened on whether the failure is caused by the maintenance or due a pre-existing cause.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	(e.g. an operator discovers that a pump has no oil in its lubrication reservoir), and those that would not (e.g. slow pick-up to rated speed); (b) *A*ll events that would have resulted in a failure to perform the mission as defined in the PSA are included as failures.	
DA-D04	The success data for standby components in terms of the number of plant specific demands is determined on the basis of the number of surveillance tests, maintenance acts, surveillance tests or maintenance on other components, and operational demands. Additional demands from post-maintenance testing are not counted; that is part of the successful renewal. Only those tests and testing steps are counted which realistically test the function of particular equipment and which are able to detect the associated failures modes as appearing in the PSA.	COMMENT: Demands resulting from post maintenance testing do not need to be included (unless they reveal new failures unrelated to the original cause of maintenance), because such tests are needed to confirm that the component has been returned to “as good as new” status which is typically assumed in the equipment reliability models used in the PSA.
DA-D05	The number of surveillance tests and planned maintenance activities is based on plant requirements.	RATIONALE: Most of the demands for standby components result from routine activities, which are predictable. Actual demands are generally a minor adjustment, which do not have a significant impact on the parameter estimates.
	DA-D05-S1 *The number of surveillance tests and planned maintenance activities is based on actual activities and operation.*	*RATIONALE: For certain applications a realistic representation of these features is required, for example for considering preventive maintenance for operational equipment such as main feedwater pumps.*
DA-D06	The success data is estimated in terms of operational time from surveillance test practices for standby components, and from actual operational data for normally operating components. Component operating times are estimated in terms of actual operating times and practices and operating times in surveillance tests. For normally operating components, regular switchovers are taken into account between redundant components and trains, and associated tests, which are usually carried out at the time of switchovers. Equipment run hour meter and start counter data are used if available, e.g. for sump pumps.	COMMENT: The run times for standby components in periodical surveillance tests may be small compared to the mission time specified in the PSA. In this case, the surveillance tests do not provide information for the time span between the end of the test runs and the end of the mission time. In principle, the behaviour of the particular component is then untested for this time span when demanded after an initiating event. This situation needs special consideration, e.g. the use of additional information (generic, equipment manufacturer) to cover the extended time period.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	DA-D06-S1	*When in the accident sequences any equipment is required under environmental or operating conditions that are more severe than those under which the failure events data are collected the failure rate is adjusted accordingly to account for this. The adjustment is based on available failure data under such conditions or, where such data is not available, on the use of expert judgment.*	*RATIONALE: In PSA models for certain accident sequences the operation of some equipment is required under conditions that are worse than the conditions they are typically operated or tested. Therefore reliability data derived from operation or tests failure data may be optimistic for those sequences.* *COMMENT: In some PSA models pumps that take suction from the sump are assumed to have the same reliability parameters in case when sump water is cooled or is not cooled when justification of the possibility to avoid cavitation is provided. In such cases it would be appropriate to attempt to determine the effect of the adverse conditions on the pump failure rate. If the determination of the effect of the adverse conditions on the pump failure rate is not possible it is more appropriate to assume that pump fails when sump is not cooled.* *COMMENT: In PSA models it is typically assumed that when room temperature is within the design limits of a component (e.g. pump) that its failure rate is represented by the available data. However, the probability of failure of the running components may be higher when the ambient temperature is above the nominal temperature and is closed to the upper boundary of the design limits. It is necessary to be careful in considering whether the failure rate would be affected by this condition, since the failure events used to assess the pump failure rates are typically derived from operation or tests when ambient temperature is much below design limits and thus performance of the pump during the PSA mission time in such conditions is not represented by the available failure data.*
DA-D07	When using data on maintenance and testing durations to estimate unavailabilities at the component, train, or system level, as required by the system model, only the unavailabilities from those maintenance or test activities that would leave the component, train, or system unable to perform its function when demanded are included in the data set.		
DA-D08	When an unavailability of a front line system component is caused by an unavailability of a support system, the unavailability is counted towards that of the support system and not the front line system.		COMMENT: Counting the unavailability for the front line system would lead to an overestimation of its unavailability.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-D09	For equipment outage, the duration of the actual time that the equipment was unavailable is identified and evaluated for each contributing activity. Since maintenance outages are a function of the plant status, only those outages, including those caused by special maintenance activities in some POSs, and are counted which occurred during the particular POSs for which maintenance unavailability data is collected. Special attention is paid to the case of a multiplant site with shared systems, when the Technical Specifications can be different depending on the status of both plants, which in turn requires a corresponding allocation of outage data among basic events.	COMMENT: Out of service unavailability data are very different for shutdown conditions, primarily because - Equipment unavailabilities are correlated by planned maintenance configurations; - Equipment repair is more a function of outage schedule and outage management than actual time required to complete repair. Outage times may be much longer than at-power [i.e. there may be no Limiting Conditions for Operation and outage management considerations may defer restoration to service; thus data for outage time is often to be based on policy and outage practice, rather than past experience (full power data are irrelevant to such cases)].
DA-D10	Coincident outage times for redundant equipment (both intra and intersystem) are identified and evaluated based on actual plant experience.	
DA-D11	Plant specific repair events or related and applicable industry experience are identified and evaluated for each repair including the associated repair time. The repair time is the time span from the identification of the component failure until the component is returned to service.	
DA-D12	Data on recovery from loss of off-site power, loss of service of service water, etc. are rare on a plant specific basis. If available, for each recovery, the associated recovery time is identified and evaluated. The recovery time is the time span from the identification of the system or function failure until the system or function is returned to service.	EXAMPLE: For the loss of off-site power special approaches to make use of the statistical data from the entire electrical network to which the plant is connected have been developed (see for example [41]).

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-D13	Plant specific outage timeline data, accounting for POS start time and duration and special maintenance configurations for each POS, are collected.	COMMENT: The data are a function of the outage plan and uncertainties in the plant staff's ability to meet that plan. Thus data collection may include the use of expert elicitation. Uncertainty information can be developed from time lines of previous outages combined with expert elicitation. All indications are that such data are very plant specific and vary with time, especially in recent years. Data may be collected and assembled differently for average risk calculations and outage-specific assessments. COMMENT: Caution is required, because changes in outage practice are occurring. Refuelling occurs less often, outages are getting much shorter, some forced outages are far less frequent, and planning is improving. The analyst is faced with playing off the value of historical data against its current relevance.

TABLE 11.2-E ATTRIBUTES FOR DATA ANALYSIS: TASK DA-E ‘DERIVATION OF PLANT SPECIFIC PARAMETERS, INTEGRATION OF GENERIC AND PLANT SPECIFIC INFORMATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-E	The parameter estimates are based on relevant generic industry and plant specific evidence. Where applicable, generic and plant specific evidence is integrated using proven methods to obtain plant specific parameter estimates. Each parameter estimate is accompanied by a characterization of the uncertainty.	COMMENT: For many applications, generic parameter estimates may be adequate. In general, if the generic estimates are chosen carefully, and are appropriate for the plant specific component design, component boundary and failure mode definitions, and operational conditions, the plant specific estimates would not be expected to be significantly different. However, the use of plant specific data will result in a higher level of confidence in the results of the PSA.
DA-E01	Plant specific parameter estimates are calculated using Bayesian updates where feasible. Prior distributions are selected as either non-informative, or representative of variability in industry data.	COMMENT: Constant failure rate is usually postulated assuming absence of aging and ‘teething trouble’ effects.
	DA-E01-S1 *A time trend analysis is performed to explore the existing trends in the reliability parameters, in particular for passive and non-replaceable components taking into account the aging effects.*	*COMMENT: The time trend analysis is useful for the applications dealing with exploration of aging phenomena.*
DA-E02	If neither plant specific data nor generic parameter estimates are available for the parameter associated with a specific basic event, estimates for the most similar equipment available are used, adjusting, if necessary, to account for differences. Use can be made of expert judgment or analytical models and the rationale behind the choice of parameter values is documented.	
DA-E03	A mean value of, and a statistical representation of the uncertainty intervals for the parameter estimates is provided.	COMMENT: Acceptable systematic methods include for instance: Bayesian updating or expert judgment. COMMENT: Uncertainty estimates are required for parameters associated with both internal and external hazards, including for example fire non-suppression estimates, severity factors, conditional events following an external hazard, etc.
DA-E04	When the Bayesian approach is used to derive a distribution and mean value of a parameter, a check is made to ascertain that the posterior distribution derived is credible given the prior distribution and the plant specific evidence.	COMMENT: If the estimator for the mean value of a parameter based on plant evidence is outside of a 95% confidence interval around the median value of the prior distribution the applicability of that particular prior data and distribution need to be reconsidered regarding its applicability to the component and failure mode under consideration.

TABLE 11.2-F ATTRIBUTES FOR DATA ANALYSIS: TASK DA-F ‘DERIVATION OF PLANT SPECIFIC PARAMETERS FOR COMMON CAUSE FAILURE EVENTS’

<table>
<tr><th>Task / GA</th><th colspan="2">Characterization of Task/General Attributes
<i>Identifier and Description of Special Attributes (in Italics)</i></th><th>Rationale/Comments/Examples for: General Attributes and
<i>Special Attributes (in Italics)</i></th></tr>
<tr><td>DA-F</td><td colspan="2">Derivation of plant specific parameters for CCF Events. As for the parameter estimates for independent events, these parameters are based on relevant generic industry and plant specific evidence if available. Each parameter estimate is accompanied by a characterization of the uncertainty.</td><td>COMMENTS:
– Because CCF events are rare events, only very few plant specific data are usually available. Therefore CCF parameter estimation relies much more on generic data and on expert judgment;
– Equipment common cause failure data is a difficult area for shutdown conditions. Many of the underlying causes of common cause failure can be affected by physical activities during outages, changes in plant conditions, and outside personnel having access to plant equipment. Full-power common cause data may be applicable to the POS and maintenance activities during each phase of shutdown. However, adjustments are often necessary.</td></tr>
<tr><td>DA-F01</td><td colspan="2">The <i>Alpha Factor Model</i> or an equivalent method is used for CCF models and regarding the estimation of CCF parameters.
The Beta-factor approach or an equivalent method is only used for an initial screening step with screening values for the parameters or for the CCF components groups of 2 components. For the finalized model, a model is used which allows a refined representation of failure combinations for higher order redundancies.</td><td>RATIONALE: Beta Factor approach typically provides over conservative estimation of CCF probabilities and may masks-out intermediate failure combinations for equipment with more than two redundancies.
EXAMPLE: The following detailed modelling methods for CCF can be mentioned in addition to Alpha Factor Model;
(a) Multiple Greek Letter Model;
(b) Basic Parameter Model;
(c) Binomial Failure Rate Model.
COMMENT: Other methods can be also used if these methods provide intermediate failure combinations and are supported by available data.</td></tr>
<tr><td></td><td><i>DA-F01-S1</i></td><td><i>For multiunit PSAs special common cause models may be needed to resolve common cause basic events within and between or among multiple reactor units.</i></td><td><i>EXAMPLE: An example of a two tiered Beta-factor model for this purpose will be in IAEA publication: Technical Approach to Multiunit Probabilistic Safety Assessment (under preparation). The common cause source data are reviewed for information to estimate these different types of common cause failures.</i></td></tr>
<tr><td>DA-F02</td><td colspan="2">When generic common cause data are used the applicability of the generic data for the particular components included in common cause group is verified and the uncertainty associated with common cause failure events is addressed.</td><td>RATIONALE: For many applications, the use of generic CCF data is generally acceptable, although the conclusions from the PSA need to be assessed for their robustness with respect to the applicability of the generic CCF data including uncertainty.</td></tr>
</table>

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
			COMMENT: Since CCF events are rare, uncertainties in estimates of CCF probabilities are relatively large and they are even larger when generic data are used.
	DA-F02-S1	*Realistic common cause data consistent with plant specific design and operational practices, supported by plant specific screening and mapping of industry-wide data are used for dominant common cause events.*	*RATIONALE: CCF events usually have a major impact on results. Use of generic CCF model parameters may mask-out differences which characterize applications.* *COMMENT: An example approach is provided in NUREG/CR-5485 [37]. Alternatively, an approach like the Partial Beta-factor is used which is, however, limited to the Beta-factor CCF model.*

TABLE 11.2-G ATTRIBUTES FOR DATA ANALYSIS: TASK DA-G ‘USE OF MECHANISTIC MODELS (FRAGILITY ANALYSIS)’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-G	When the primary mechanism is induced by a physical phenomenon, as is the case for internal and external hazard events, the failure probabilities are determined by mechanistic analysis, referred to as fragility analysis	
DA-G01	The systems, structures, and components (SSCs) that are susceptible to the hazard events included in the PSA and that can either cause an initiating event or cause damage to components required to respond to an initiating event are identified.	COMMENT: This attribute results in an initial version of the hazard equipment list that will form the basis for the fragility analysis task and the inclusion of hazard-induced failures in the model.
DA-G02	For seismic PSA, the seismic-fragility evaluation is based on a seismic response that the SSCs experience at their failure levels..	
DA-G03	For fire PSA, the fire-induced circuit failure probabilities are included in the model. The probabilities are based on based on available generic data, using plant specific circuit analysis used to derive attributes	
DA-G04	SSCs that are indicated in the systems model as being important to large early release frequency due to a hazard event (i.e. have the potential to lead directly to containment/confinement bypass) and are susceptible to hazard events are identified.	COMMENT: The concern is that these hazard-induced failure of the containment (confinement) boundary have an elevated level of importance in the internal and external hazard PSA versus the internal events PSA. Through these failures hazard events can breach two layers of defence-in-depth. It is advisable that such events not be screened from the model and have fragilities calculated.
DA-G05	SSCs that can result in internal fire or internal flood when subjected to a hazard (i.e. have a hazard-induced failure mode that can result in internal fire or internal flood) are identified. SSCs that are screened for this possibility are screened using a defined and justified basis.	RATIONALE: Under certain conditions, the addition of a fire or flood to the damage caused by a seismic event can increase the extent of equipment damage and thus increase the conditional probability of core/fuel damage or large early release. COMMENT: Not every ignition source or flood source will have a credible failure mode that can result in the fire of flood when subjected to a hazard. Further, they may have a high capacity or be located in areas where there are not any important targets that would be failed. It is important to take this into consideration when deciding which SSCs to consider under this attribute. Failure to conduct a thorough screening can result in a very large and unwieldy model that does not add to the risk insights.
DA-G06	Plant specific information on the SSCs identified in DA-G01 is gathered. A key part of this process is a plant walkdown. This	COMMENT: The walkdown need to be conducted based on documented walkdown procedures developed by the PSA team. These procedures need to be based on existing

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	walkdown is conducted to gather plant specific information about the SSCs. The walkdown is also used to identify potential interactions where failure of an SSC not identified in DA-G01 can cause damage to one of those SSCs. These are added to the model.	guidance and should list the necessary qualifications of the walkdown team members. The search for potential interactions is an important part of the walkdown process. Hazard-induced failures of nearby SSCs (such as walls and ceilings) can impact important components [42 - 44]. EXAMPLE: Detailed seismic walkdowns of the plant need to be focusing on the anchorage, seismic support, and potential systems interactions.
DA-G07	Generic information is used to augment plant specific information where necessary to perform the fragility analysis. The specific generic information used is assessed as to its applicability to the plant.	EXAMPLE: Generic equipment qualification tests (e.g. seismic shake tables, fire damage tests on cable). Experimental data (e.g. heat release rate experiments, explosion overpressure measurements). Experience data (site surveys following hazard events).
DA-G08	Realistic failure modes are defined for the response of each susceptible SSC for each hazard event.	COMMENT: Design documents and the walkdown are important in identifying hazard-induced failure modes. The generic information discussed in DA-G03 will also provide useful information on how SSCs fail when subjected to a particular hazard.
DA-G09	If SSCs susceptible to the hazard are to be screened based on an assessment of high capacity against the hazard events, this is done using a documented and justified basis. The basis is developed such that it assures that the screened SSCs are not significant to CDF/FDF or LERF.	EXAMPLE: A typical approach to screening for seismic PSA is to use the criteria in EPRI NP-6041-SL, Rev. 1 [44]. In order to use these criteria, a bounding analysis needs to be performed using both a bounding fragility associated with the screening level in combination with the plant seismic hazard curve in order to estimate the potential risk contribution of the screened SSCs.
DA-G10	Mechanistic models appropriate to the hazard events being analysed are used to determine the fragility of each included failure mode of each SSC. These are expressed as either fragility curves (when the frequency of the hazard severity is represented by a continuous distribution of a controlling parameter) or by a series of single probability values (when the frequency of the hazard severity is represented by discrete hazard events).	COMMENT: There may be cases where the fragility of a specific failure mode is expressed in terms of a conditional probability given the occurrence of a seismic failure. For example, in the case of a seismically-induced internal fire the likelihood of the fire may be expressed as the probability of fire given a seismically-induced failure of the SSC.
DA-G11	The information used to develop the fragility parameters is plant specific augmented by applicable and appropriate generic information.	COMMENT: See also DA-G04.
DA-G12	Fragilities developed for the SSCs that appear in dominant cutsets are based on site-specific fragility parameters and plant specific information, including the results of detailed walkdowns to	RATIONALE: The use of generic information for SSCs in dominant cutsets can distort the results and give incorrect insights as to the important SSCs associated with the risk from the hazard. This distortion is increased because it also changes the value of the

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	determine as-installed and as-current conditions. Generic information is only used when strongly justified.	success terms.
DA-G13	Fragilities for SSCs that can be affected by multiple hazards are determined individually. Fragility impacts are not combined.	RATIONALE: It would be too complicated to consider that the effect of one hazard might weaken an SSC such that it was more vulnerable to a second correlated hazard, and the gain in risk insight would be minimal.
DA-G14	Regardless of the how the fragility is expressed the uncertainty in the underlying models and assumptions are mathematically expressed as parameters in an appropriate distribution.	

TABLE 11.2-H ATTRIBUTES FOR DATA ANALYSIS: TASK DA-H ‘DOCUMENTATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-H	Documentation and information storage is performed in a manner that facilitates peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the assumptions made and their bases.	
DA-H01	The following aspects of the data analysis process are documented: a) System and component boundaries used to establish component failure probabilities; b) Grouping criteria for components; c) The model used to evaluate each basic event probability; d) Sources for generic parameter estimates; e) The plant specific and POS-specific sources of data; f) The time periods for which plant specific data were gathered; justification of any censoring of the data for specific POS conditions; g) Walkdown reports, including notes and photographs; h) Assumptions made in the interpretation of data and the reasoning (based on engineering judgment, systems modelling, operations, and statistical knowledge) supporting its use in parameter estimation; i) Justification for exclusion of any data; j) The basis for the estimates of common cause failure probabilities, including justification for screening or mapping of generic and plant specific data; k) The rationale for any distributions used as priors for Bayesian updates, where applicable; l) Parameter estimates including the characterization of uncertainty as appropriate; m) The rationale for using generic parameter estimates for multiple	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	POSs; n) The results of the fire-induced circuit failure analyses and the associated conditional failure probability values.	
DA-H02	The derivation of the parameter values is documented. The information/database is documented and stored in a way, which allows the reproduction of the data analysis task for example for reliability parameter updates.	
	DA-H02-S1 *The information from the data analysis including the databases created is part of the PSA model and documentation. This data including the databases and the detailed background information is stored in a retrievable and accessible electronic form and format. Due to the amount of information arising from the data analysis tasks electronic storage of this information is essential for many of the applications.*	*RATIONALE: Certain applications could be practically prevented without the information being available and accessible in this way.*
DA-H03	In the PSA for hazards the documentation covers the following: a) Description of the method of derivation of the probabilities of the failures due to the hazards; b) Description of the input information; c) Fragility and load curves if appropriate; d) Uncertainty estimations for each failure probability derived; e) Results in terms of probabilities and related uncertainties.	
DA-H04	The sources of model uncertainty and related assumptions associated with the data analysis are documented.	

12. PSA ELEMENT ‘DF’: DEPENDENT FAILURES ANALYSIS

12.1. MAIN OBJECTIVES

The objective of the dependent failure analysis is to support other PSA elements with dependent failure information and assure that all possible dependencies are correctly considered. Correctly modelling dependencies is essential to the development of the PSA model. The dependent failure analysis tasks provides the vehicle for confirming that all dependencies, including subtle dependencies, are included in the PSA, either by explicit modelling or by common cause failure modelling. Dependent failures to be considered and analysed are:

- Design related dependencies;
- Operational related dependencies;
- Physical dependencies;
- Initiator related dependencies;
- Multiunit dependencies residual dependencies (common cause failures).

It needs to be noted that the dependency analysis is exercised as part of almost all other PSA elements. The categories of dependencies and PSA elements in which they are addressed are provided in Table 12.1. Dependencies that arise from area events (e.g. internal fires and floods) and external initiating events (e.g. earthquakes, high winds) are not included here since they are outside the scope of this publication.

TABLE 12.1 DEPENDENCE CATEGORIES AND PSA ELEMENTS

Dependence Type	Dependence Category	Analysis Procedure or Method	PSA Elements
Design Related	Functional dependencies	Development of accident sequences Development of success criteria	Accident sequence analysis Success criteria Systems analysis
	Support system dependencies	Development of system models	Systems analysis Accident sequence analysis (large event tree approach)
	Shared component dependencies	Development of system models	Systems analysis
Operations Related	Human action dependencies	Development of accident sequences Human reliability analysis Modelling of support state initiating events Modelling of post-accident restoration of multiple unavailable components Modelling of non-restoration of component within a POS	Initiating events analysis Accident sequence analysis Systems analysis Human reliability analysis Data analysis
Physical	Common environmental effects	Development of accident sequences Development of system models	Accident sequence analysis Systems analysis
	Spatial Interactions	Physical analyses	Systems analysis Accident sequence analysis
	Dynamic effects	Physical analyses	Initiating events analysis (pipe breaks)

Dependence Type	Dependence Category	Analysis Procedure or Method	PSA Elements
Initiator	Common Cause Initiating Events	Analysis of operating experience, insights from other PSA studies, link from functional dependencies Use of fault tree models	Initiating event analysis Systems analysis
Residual Dependencies	Common Cause Failures	Definition of CCCGs Use of accepted CCF model	Systems analysis Data analysis

12.2. DEPENDENT FAILURE ANALYSIS TASKS AND THEIR ATTRIBUTES

Table 12.2 lists the main tasks for the PSA element 'Dependent Failure Analysis'. Tables 12.2-A through 12.2-G present the description of general and special attributes for these tasks.

TABLE 12.2 MAIN TASKS FOR DEPENDENT FAILURE ANALYSIS

Task ID	Task Content
DF-A	Design related dependency analysis
DF-B	Operations related dependency analysis
DF-C	Physical dependency analysis
DF-D	Common cause initiating event analysis
DF-E	Common cause failure analysis
DF-F	Subtle interactions
DF-G	Documentation

TABLE 12.2-A ATTRIBUTES FOR DEPENDENT FAILURE ANALYSIS: TASK DF-A 'DESIGN RELATED DEPENDENCY ANALYSIS'

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DF-A	The design related dependencies are included in the accident sequence and system models.	
DF-A01	Functional dependencies are addressed in the structure of the accident sequences models.	EXAMPLES: Functional dependence: - BWR: if depressurization of the reactor fails, the low pressure injection function is guaranteed to fail; - PWR: if low pressure injection fails, the recirculation function fails.
DF-A02	Support system dependencies are modelled by linking system models (e.g. fault trees) through appropriate transfer gates (fault tree linking approach), or by developing models for each support system state (large event tree/support state/event tree linking approach).	COMMENT: The correct identification of implicit system dependencies (not evident from schematics) is crucial. Thus, dependence on ambient environmental conditions is also a design dependence. EXAMPLE: The dependence on room temperature and thus on the ventilation system and on the room heating system.
DF-A03	Common component dependencies are modelled in the fault trees (fault tree linking approach) or by explicitly including the component as an event tree branch point (large event tree/support state/event tree linking approach).	COMMENT: Special attention need to be given to support system dependencies that result in a change in state of a component, rather than just the loss of ability to actuate a component. The change in state, while intended to place the component in a "safe" state, may not always be the desired state for certain accident sequences.

TABLE 12.2-B ATTRIBUTES FOR DEPENDENT FAILURE ANALYSIS: TASK DF-B ‘OPERATIONS RELATED DEPENDENCY ANALYSIS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DF-B	Operational related dependencies are addressed in the structure of the accident sequence and system models by the inclusion of human failure events.	RATIONALE: This class of dependency addresses the impact of human actions on the success or failure of functions or systems, and includes both pre-initiator actions, and actions in response to changes in plant conditions (precursors to initiating events resulting from loss of support systems, and initiating events). COMMENT: The analysis of operational related dependencies is primarily addressed in the Initiating Event Analysis, Accident Sequence Analysis, Systems Analysis, and Human Reliability Analysis.
DF-B01	Pre-initiator operational related dependencies, i.e. those resulting from test/maintenance/calibration errors (pre-initiator errors) are included in the appropriate system models.	
DF-B02	Pre-initiator operational related dependencies are adjusted for disabled components by the hazard.	RATIONALE: If a component is disabled by the hazard, the pre-initiator operational related dependencies with other components need to be reconsidered and adjusted accordingly.
DF-B02	The dependencies arising from the need for operator intervention in the case of partial support system failures (e.g. loss of a train of component cooling water system) as called for by emergency operating procedures are addressed in the system models used to evaluate the initiating event frequency.	
DF-B03	Dependency of functions or systems on operator intervention following an initiating event is modelled in the structure of the accident sequence and system models.	
DF-B04	The values of the HEPs used for the HFEs are appropriate for the plant specific and scenario specific conditions.	RATIONALE: The performance of the operators, in particular for response actions, is conditioned by a number of factors that are dependent on the scenario characteristics.
DF-B05	The dependency between HEPs appearing in the same cutset is assessed and the values changed as appropriate.	
DF-B06	Dependencies between HFEs that could lead to an initiating event and pre-initiator HFEs / post-initiator HFEs for all modelled POSs are	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	addressed.	
DF-B07	Dependency caused by limited resources for post-accident restoration of multiple unavailable components in parallel or in managing accidents on two or more reactor units concurrently.	COMMENT: The issue is availability of spare parts and repair staff for several repairs simultaneously.
DF-B08	Dependency between POSs that is caused by non-restoration of a failed component within a previous POS.	COMMENT: Safety related equipment failed in a particular POS can be not restored by the end of the POS. There may be no Limiting Conditions for Operation preventing from the entry to the next POS. In this case the additional unavailability due to corrective maintenance need to be taken into account in the next POS.

TABLE 12.2-C ATTRIBUTES FOR DEPENDENT FAILURE ANALYSIS: TASK DF-C: ‘PHYSICAL DEPENDENCY ANALYSIS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DF-C	Dependencies that arise because of degradation of the environment of the plant equipment are addressed. These include dynamic effects of a pipe break and secondary effects of other initiating events and events occurring during an accident scenario that can cause failures of safety related equipment, which is needed for the mitigation of the initiating event or failures of which can make the initiating event worse.	
DF-C01	The analysis scope for the physical dependencies includes the following categories of phenomena: Category 1: Impacts of pipe whip, projectiles, and water/steam jets in case of pipe breaks, vessel ruptures, etc.; the influences can be directed to adjacent equipment or building structures. Category 2: Consequences of increased humidity and temperature. Category 3: Distribution of pipe insulation material and blocking of the recirculation flow (post–LOCA). Category 4: Spatial interactions	RATIONALE: Physical effects can substantially reduce the mitigation possibilities. COMMENT: Spatial interactions include failures that can interfere with the performance of operator actions in the plant, such as the collapse of walls, presence of fires, presence of water, and similar things that could block or hinder operator access to areas and equipment essential to the performance of these actions.
DF-C02	Physical dependencies resulting from internal and external hazard events are considered. This is done during the plant walkdown for the fragility analysis. Particular attention is paid to the potential for hazard-induced fires and floods.	COMMENT: See also the related attribute DA-G02.
DF-C03	Multiunit dependencies associated with the occurrence of an accident on one reactor unit and its impact on the control and accident management on another reactor unit is considered.	COMMENT: If there is a release and contamination of the site from one reactor unit, the adverse effects on the control and accident management on the other reactors on the site need to be considered. Any operator actions that must be performed following site contamination, especially those actions outside the control room, or actions following a control room evacuation will be severely limited in order to prevent unacceptable doses to the operators.

TABLE 12.2-D ATTRIBUTES FOR DEPENDENT FAILURE ANALYSIS: TASK DF-D ‘COMMON CAUSE INITIATING EVENT ANALYSIS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DF-D	An analysis of common cause initiating events is performed.	
DF-D01	Common cause initiating events are identified and included in the PSA model as necessary.	COMMENTS: A common cause initiator (CCI) is an event causing a transient (or requiring manual shutdown) and at the same time degrading one or more safety functions that may be needed after the transient/shut-down. CCIs are restricted to failures occurring inside the plant systems, such as failures in the control and protections systems, electric power supply system, service water system or other support systems. The CCI analysis is usually a part of the Initiating Events Definition and Grouping Task and the Systems Analysis Task, except for the modelling of the plant response to an identified and important CCI, which belongs to the Accident Sequence Analysis.

TABLE 12.2-E ATTRIBUTES FOR DEPENDENT FAILURE ANALYSIS: TASK DF-E ‘COMMON CAUSE FAILURE ANALYSIS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DF-E	A component common cause failure analysis (CCF) is performed.	
DF-E01	Common cause failures are included in the system models as appropriate.	RATIONALE: While many sources of dependency can be modelled explicitly in the PSA model, there are failure mechanisms at the component level that can result in multiple start failures when components are demanded or multiple component failures within the mission time required of those components. These are the so-called ‘common cause failures’.
DF-E02	Common cause groups are developed to incorporate hazard-induced dependencies and correlations. Bounding or generic correlation values are used, with the basis provided.	COMMENTS: – See also SY-C10 and SY-17; – Because of a significant lack of actual data to develop plant specific correlation values, the best that can be achieved in this area is to use generic values; – Seismically induced failures of similar equipment in the same building at the same level and in the same orientation are typically modelled as completely correlated. All other equipment is typically modelled as completely independent. Both approaches are simplified, but it may be that this is the most reasonable approach to use and is commonly accepted by the PSA community. CCF models for seismic correlations can be used, but their use must be justified.

TABLE 12.2-F ATTRIBUTES FOR DEPENDENT FAILURE ANALYSIS: TASK DF-F ‘SUBTLE INTERACTIONS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DF-F	An analysis of subtle interaction dependencies is performed.		
DF-F01	Operational experience of the plant being analysed and similar plants is reviewed to identify events that involve unusual dependent effects. PSA model addresses these effects.		
	DF-F01-S1	*Historical events that involve unusual dependent effects are reviewed to determine whether such occurrences can occur at the plant being analyzed.*	*RATIONALE: A structured identification and consideration of subtle interactions may be needed for completeness purposes.* *COMMENT: So called subtle dependencies[11] are not ordinary functional dependencies but are specific to actual demand conditions, when the plant systems are actuated and operated under transient or emergency conditions.* *Typically, subtle dependencies are not detected in normal operation or by surveillance tests. The interaction between systems or subsystems can be transmitted by the process medium, via support system routes or indirectly via operating environment, e.g. temperature, humidity, pressure waves or vibration.* *Subtle dependencies are either functional or physical, but they are difficult to foresee. Identified subtle dependencies can be treated by explicit modelling, or considered in the CCF models.* *EXAMPLE: A list of subtle interactions can be found in NUREG-1150 [45].*

[11] Subtle dependencies are also called ‘system interactions’ or ‘subtle interactions’.

TABLE 12.2-G ATTRIBUTES FOR DEPENDENT FAILURE ANALYSIS: TASK DF-G ‘DOCUMENTATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DF-G	Documentation and information storage is performed in a manner that facilitates peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the assumptions made and their bases.	
DF-G01	Functional dependencies are documented in the form of component information tables and system dependency matrices in a clear and traceable manner.	COMMENT: It is useful to produce an integrated dependency matrix to provide an overview of the functional dependencies over all systems.
	DF-G01-S1 *The information contained in the component information tables, protection signal tables, dependency matrices etc. is stored in a relational database.*	*COMMENT: Documentation of complex and interrelated data in the form of a relation database is important for applications based on Living PSA (Risk Monitor).*
DF-G02	The specific assumptions and limitations concerning functional dependencies are documented.	EXAMPLES: The following items are examples of generic assumptions and limitations: - In some plant rooms, the failure of room cooling/heating can constitute a CCI. Similarly, specific failure situations in other support systems can lead to CCIs, which are analyzed separately; - Failure of component protection is not considered as failure if it is likely that the component will survive the demand and needed mission time (will fulfil the safety function even though degraded).
DF-G03	The CCI analysis is documented: - Description of the CCI identification process as defined in the Initiating Events Definition and Grouping Task; - List of the CCIs considered as initiating events with a reference where the associated accident sequence analysis and event tree modelling are described; - CCIs that were screened out. Complex cases are discussed in the Initiating Event Analysis or in the corresponding systems analysis report, in order to explain the details of the causal modelling, special initiator characteristics and derivation of	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	the initiator frequency.	
DF-G04	The physical dependency analysis is documented: - Extensions to LOCA and transient categories; - Refinements to accident sequence models of LOCAs and transients; - Evaluation of containment (confinement) sump operability; - Hazard-induced physical dependencies.	
DF-G05	The CCF analysis is documented: - Identification and definition of CCCGs; - All CCCGs and components included; - Treatment of intrasystem and intersystem CCFs; - Models used; - Special CCF events; - CCF data; - A description of how CCF is implemented in the overall PSA model.	
DF-G06	In the hazard PSA, the changes in the CCF analysis are documented: – Identification and re-definition of the affected CCCGs; – Affected CCCGs and new list of components included; – New CCF data.	
DF-G07	The sources of model uncertainty and related assumptions associated with the dependency analysis are documented.	

13. PSA ELEMENT ‘MQ’: MODEL INTEGRATION AND LEVEL 1 PSA QUANTIFICATION

13.1. MAIN OBJECTIVES

The main objective of the model integration and quantification process is to develop an integrated plant specific PSA model that will be used to estimate the Level 1 PSA risk metrics and to develop an understanding of the contributors to core/fuel damage model (see also Section 12). For a single reactor PSA, CDF/FDF is the primary Level 1 risk metric. For a multireactor PSA, the metrics include SCDF/SFDF and MCDF/MFDF. However, there are other risk metrics that may be of interest, so this section applies to integration and quantification regardless of the risk metrics of interest.

The following principles need to be met:

- The PSA model reflects the current design, operational practices (procedures, configuration strategy), and the operational experience;
- The parameter uncertainties are considered in the model;
- The quantification is performed correctly, taking into account the dependencies discussed in Section 10;
- The results are reviewed to ensure that the solution reflects the plant characteristics;
- Illogical or incorrect minimal cutsets are removed;
- Recovery actions are applied to minimal cutsets that are assessed to be too conservative, as needed.

13.2. MODEL INTEGRATION AND LEVEL 1 PSA QUANTIFICATION TASKS AND THEIR ATTRIBUTES

Table 13.1 lists the main tasks for the PSA element ‘Model Integration and Risk Metric Quantification’. Tables 13.2-A through 13.2-D provide the description of general and special attributes for these tasks.

TABLE 13.2 MAIN TASKS FOR MODEL INTEGRATION AND LEVEL 1 PSA QUANTIFICATION

Task ID	Task Content
MQ-A	Integrated model
MQ-B	Requirements on the quantification
MQ-C	Review and modification of the results
MQ-D	Documentation

TABLE 13.2-A ATTRIBUTES FOR MODEL INTEGRATION AND RISK METRIC QUANTIFICATION: TASK MQ-A ‘INTEGRATED MODEL’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MQ-A	Construction of an integrated plant specific PSA model from the elements addressed in Sections 4 through 12 is performed.	
MQ-A01	All system models, accident sequence models, and data are integrated to provide the logic structure of the PSA model, and are presented in a traceable manner. Initiating events for which accident sequence are not developed, but that are assumed to lead directly to core/fuel damage are also included in the integrated model (e.g. undeveloped ISLOCA, reactor vessel rupture).	RATIONALE: There are two commonly used approaches to PSA logic model construction: the so-called fault tree linking approach; and the linked event tree approach. The former relies on computer codes that use Boolean logic to address dependencies arising from common components or common support systems. The latter depends on the consistent application of logic rules that identify the appropriate conditions for the solution of system models so that the events on the event tree can be treated as independent. COMMENTS: For the fault tree linking approach, at each branch point, the corresponding fault tree is solved for the function or system success criteria and boundary conditions that reflect the scenario specific plant conditions. Support system dependencies are addressed by the consistent event-naming scheme used for fault tree construction and establishing logic links between the system models (frontline-to-support systems, support-to-support systems). For the event tree linking approach, the probabilities of the branch points (sometimes called split fractions) are conditional on the path through the event tree.
	MQ-A01-S1 *For specific applications, such as a risk monitor application, the models for all the POSs and hazards analysed are combined in an integrated model.*	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MQ-A02	For the fault tree linking approach, logic loops are cut in a manner that minimizes loss of information and does not produce optimistic results by, for example, removing some of the dependencies (by neglecting parts of the support system logic failure model).	RATIONALE: When fault trees are linked to create an integrated logic model, logic loops can appear due to mutual dependencies between support systems, e.g. see below. EXAMPLE: The classical example is described in NUREG/CR-2728 [46] dealing with an emergency diesel generator depending on service water for cooling which in turn requires electric power from the diesel. Many contemporary PSAs have refined and extended models for electrical power supplies and control I&C which may create more complex logic loops. These logic loops have to be resolved, basically by cutting the loop at an appropriate place or level because, otherwise, the model cannot be resolved and quantified. The cutting of logic loops is carried out in a manner, which minimizes the loss of information and does not produce non-conservative results. It is carried out according to a defined concept and procedure and the details of resolving logic loops are fully documented.
MQ-A03	The initiating event frequencies and the probabilities associated with basic events of the model are consistent with the definitions of the events in the context of the logic model.	COMMENT: The parameters are defined in such a way that they represent the plant specific design and operational experience as well as scenario specific boundary conditions (especially important for human error probabilities) as discussed in Sections 4 - 12.
MQ-A04	For each scenario quantified as a contributor to the Level 1 PSA risk metric, quantify the PSA plant response model reflecting the scenario-specific quantification factors (i.e. circuit failure likelihoods, HEP values for HFEs quantified per the HRA requirements, and the hazard-induced equipment and cable failures)	
MQ-A05	For multiunit sites that have either shared systems or for which multiunit hazard events are being evaluated as part of the PSA, a single integrated multiunit PSA model is developed. This model accounts for the effect of multiple units being impacted at one time for a single reactor unit PSA and for a multiunit PSA the contribution to site risk metrics from accidents involving multiple units, whose total frequency is the applicable multiunit risk metrics, is also included.	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MQ-A06	For correlated hazards, including hazard-induced internal fires and floods, the model is integrated so that the effects of the correlated hazards can be propagated through the model during the quantification.	

TABLE 13.2-B ATTRIBUTES FOR MODEL INTEGRATION AND QUANTIFICATION: TASK MQ-B ‘REQUIREMENTS ON THE QUANTIFICATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MQ-B	Solution of the model to derive the logical combinations of events leading to the risk metrics of interest (for example, core/fuel damage and the associated minimal cutsets) and the quantification of the Level 1 PSA risk metric (for example, CDF for single reactor PSA, and SCDF and MCDF for multiunits PSA), is performed with an appropriate code.		COMMENT: This publication refers to minimal cutsets as an important result of PSA. This term applies to the fault tree technique for PSA models assuming coherent logic models. For non-coherent logic models, the corresponding mathematical term is ‘prime implicants’. EXAMPLE: The prior generation of cutsets is not required for the quantification. Prime implicants can be derived on the basis of the generation of Binary Decision Diagrams (BDDs). BDDs are a specific representation of Structural Boolean Logic Functions of complex systems allowing the exact quantification of fault trees including non-coherent logic models (models using negative logic, i.e. NOT-Gates).
MQ-B01	The computer code used for solution and quantification of the PSA model is verified and validated, and is used only within its specified range of applicability. Specific limitations of the code are recognized.		EXAMPLE for specific limitations that may occur in a linked fault tree model: If the event tree quantification uses a success probability of 1, significant quantification errors can occur, if the failure probability of a linked fault tree is high.
MQ-B02	The PSA model is solved and quantified to allow identification of the significant sequences contributing to core/fuel damage frequency.		
MQ-B03	For the quantification of hazard risk, the hazard frequency, fragility, and systems analyses are integrated.		COMMENT: The conditional probability of the initiating event(s) associated with each hazard event is a part of this quantification. It is not specifically mentioned because this is accomplished within the fragility analysis and system analysis.
	MQ-B03-S1	*For the quantification of multiunit sites that have shared systems or multiunit hazard events, the quantification is accomplished using an integrated multiunit model. This model accounts for the effect of multiple units being impacted at one time for a single reactor unit PSA and for a multiunit PSA the contribution to site risk metrics (for example, SCDF from accidents involving core/fuel damage on multiple units, whose total frequency is MCDF), is also*	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		included.	
MQ-B05	For the fault tree linking approach, the final truncation value is justified by a sensitivity analysis demonstrating that the core/fuel damage frequency does not significantly change, if the truncation value is reduced.		COMMENT: Expert opinion suggests that the truncation value need to be at least 3 orders of magnitude lower than the dominant value (e.g. the CDF) that is considered. However, only a sensitivity study can assure that an appropriate truncation value was applied.
	MQ-B05-S1	*For the derivation of some importance lists (especially RAW) the truncation value is re-evaluated and justified.*	*RATIONALE: If this is not done, several low-probability events might be excluded from the importance list whenever RAW is significant for the application.*
	MQ-B05-S2	*If the application is related to a specific initiating event, of a specific group of sequences, the attribute is applied for those contributions to the risk metrics rather than the total risk metrics.*	*COMMENT: Sensitivity tests need to be conducted for the set of results of interest.*
MQ-B06	Level 1 PSA risk metrics are evaluated as mean value and the uncertainty distributions characteristics are provided, for the total Level 1 metrics, each POS and for the significant individual accident sequences. Parameter uncertainties associated with HEPs, component reliability parameters, initiating event frequencies, etc. are propagated (via fault and event trees) through the model. State of knowledge correlations between uncertainty distributions are addressed and considered for the uncertainty quantification. When using a Monte Carlo, or other simulation approach, the number of simulations used has been demonstrated to produce stable results.		COMMENT: A point estimate obtained by substituting a mean value for each parameter in the minimal cutset equation, without a propagation of uncertainty gives an approximation to the mean value. The closeness of the approximation to the true mean value depends on the failure events included in the cutsets, the extent of correlation between uncertainty distributions and the shape of uncertainty distributions involved.
MQ-B06	For the fault tree linking approach, when hazard events are evaluated and failure probabilities become large, the analytical approach to determining the cutset upper bound is varied to determine the point at which the results converge.		COMMENT: Default quantification algorithms do not treat high failure probabilities very well. The lower success probabilities are not accounted for, and the summing of cutset frequencies will often lead to CCDP/CFDP values greater than 1.0. Tools exist to perform the quantification in a mathematically exact way, but applying them to the entire quantification will result in extremely slow quantification or even system crash.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		The tools provide parameter options to limit the extent of use of the mathematically exact algorithm, and by varying these parameters the optimum settings can be achieved.
MQ-B07	When using logic flags (also designated as house events), the logic flag events are either set to be logical true or false (instead of setting the basic event probability to 1.0 or 0.0), prior to the quantification of the sequences.	EXAMPLE: Logic flags may be used to model guaranteed success or failure, or to switch on or off the models corresponding to different configurations.
MQ-B08	In the PSA for hazards the logical settings of the logic flags and/or the basic events or any fault tree elements representing the effect of the hazard are stored providing an easy access and form the basis for review, for the update or upgrade of the PSA and utilization of the PSA results.	COMMENT: In many cases the effect of the hazard is represented by setting logic flags, or even the related basic events to the necessary logical value. The setting of the logic flags and basic event logical settings are usually stored in so called “boundary conditions” specific to the hazard.

TABLE 13.2-C ATTRIBUTES FOR MODEL INTEGRATION AND RISK METRIC QUANTIFICATION: TASK MQ-C 'REVIEW AND MODIFICATION OF THE RESULTS'

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MQ-C	The task includes a review of results and corrections to the integrated model made as necessary.		RATIONALE: Depending on the way the integrated model has been developed, some post-processing of the results may be needed. A review of the results acts as a confirmation that the model has been integrated correctly.
MQ-C01	A sample of significant minimal cut sets or sequences of each event tree type is reviewed in order to determine, if the logic of the minimal cut sets or sequences is correct. As a spot check, a sample of less significant cut sets or sequences is reviewed.		
MQ-C02	Minimal cut sets (or sequences) containing events that are mutually exclusive but appear because of the approach to modelling (e.g. if NOT gates are not used to eliminate disallowed maintenance, or multiple initiators) are identified and corrected.		
	MQ-C02-S1	*The system models are incorporated such that each configuration of a system (e.g. no maintenance, maintenance on train A, maintenance on train B, etc.) is modelled separately with an appropriate time fraction.*	*RATIONALE: A more detailed modelling approach requires less post-processing, e.g. in a Risk Monitor application.*
MQ-C03	Minimum cut sets (or sequences) containing multiple operator actions are identified, the degree of dependency and the dependency is include in the quantification for each hazard and POS.		RATIONALE: Because the dependency between HFEs is accident scenario dependent, it is often addressed by post-processing to adjust the combined probability of the set of dependent HFEs.
MQ-C04	Minimal cutsets that include hazard events are reviewed to assure that the appropriate success terms have been accounted for. Sequence frequency totals are reviewed to assure that high failure probabilities have been correctly treated.		COMMENT: The default quantification approach for most quantification tools assume that success probabilities are close to 1 and that the rare event approximation can be used for combining cutsets. This is often not true for hazard events, and this can result in sequence CCDPs/CFDPs in excess of 1 due to approximations and overestimation of sequence frequencies.
	MQ-C04-S1	*For quantifications that use an integrated multiunit model, minimal cutsets are reviewed to assure that the model correctly accounted for shared systems, simultaneous accident conditions, and multiunit*	

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	damage.	
MQ-C05	Recovery actions are included in the quantification process in applicable sequences and minimal cut sets. Recovery actions credited in the evaluation are either proceduralized or can be shown to be feasible and credible assuming that trained and qualified personnel are performing the recovery action(s).	

TABLE 13.2-D ATTRIBUTES FOR MODEL INTEGRATION AND RISK METRIC QUANTIFICATION: TASK MQ-D ‘DOCUMENTATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MQ-D	Documentation and information storage is performed in a manner that facilitates peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the assumptions made and their bases.	
MQ-D01	The following aspects of the model integration and Level 1 PSA risk metric quantification process are documented: - The integration process of all fault and event trees; - PSA model version; - A general description of the quantification process; - The process and the results for establishing the truncation values; - Software version and quantification setup (truncation values, etc.); - The process and the results of the quantification review; - The mean value and the uncertainty distribution of the total risk metric (for example CDF/FDF), each POS, each class of initiating events, and of significant risk metric (for example, core/fuel damage) sequences; - The accident sequences and their contributing cut sets.	
	MQ-D01-S1 *When only a fraction of the Level 1 PSA risk metric is required to be analysed for an application, the documentation supports this analysis.*	
MQ-D01	The sources of model uncertainty and related assumptions associated with the model integration and risk metric quantification are documented.	

14. PSA ELEMENT ‘RI’: RESULTS ANALYSIS AND INTERPRETATION

14.1. MAIN OBJECTIVES

The objective of the results analysis and interpretation activity is to derive an understanding of those aspects of plant design and operation that have an impact on the risk. In addition, an important part of this task is to identify the key sources of uncertainty in the model and assess their impact on the results.

Uncertainties can be thought of as being of three main types:

- *Parameter uncertainty*: these are uncertainties in the values of the initiating event frequencies, component failure probabilities, human error probabilities, etc. These uncertainties can be propagated through the analysis to generate an assessment of the uncertainty on the overall quantitative results using standard methods. Parameter uncertainties are addressed in Section 11.
- *Model uncertainty:* There are questions with how to model certain failures (e.g. RCP seal LOCAs), or how to represent the impact of plant conditions on system success criteria, for example, for which there is no universally accepted approach. Typically, in PSAs, these model uncertainties are dealt with by making assumptions and adopting a specific model. In relatively rare cases, alternate models may be incorporated into the PSA, weighting each model by a probability representing the degree of belief in that model as being the most appropriate.
- *Completeness uncertainty:* This is the most difficult to deal with as it represents those contributors to risk that are not included in the model. If the PSA model only includes internal initiating events at power, the contributors to risk not modelled include external hazards, and alternate modes of operation. At a more subtle level, typically PSAs do not include contributions from errors of commission.

The significance to risk of individual contributors (initiating events, accident sequences, functional failures, system failures, component failures, human failures, etc.) are explored to derive an understanding of the risk profile of the plant, i.e. what is the impact of various aspects of plant design and operation on risk. The impact of uncertainties and assumptions on the PSA results are addressed in order to determine the robustness of the conclusions concerning the risk profile. The analytical tools used for the analysis of results are importance analyses and sensitivity analyses.

14.2. RESULTS ANALYSIS AND INTERPRETATION TASKS AND THEIR ATTRIBUTES

Table 14.1 lists the main tasks for the PSA element ‘Results Analysis and Interpretation’. Tables 14.2-A through 14.2-C present the description of general and special attributes for these tasks.

TABLE 14.1 RESULTS ANALYSIS AND INTERPRETATION TASKS

Task ID	Task Content
RI-A	Identification of significant contributors
RI-B	Assessment of assumptions
RI-C	Documentation

TABLE 14.2-A ATTRIBUTES FOR RESULTS ANALYSIS AND INTERPRETATION: TASK RI-A ‘IDENTIFICATION OF SIGNIFICANT CONTRIBUTORS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
RI-A	The task includes identification of significant contributors to the risk profile of the plant.	
RI-A01	Significant contributors to the risk metrics are identified. The contributors are, in increasing level of resolution: - Hazard events; - Plant operational states; - Initiating events; - Accident sequences; - Key safety function failures; - System failures; - Basic events; - Fire compartments or scenarios (in fire PSA); - Flood compartments (in flooding PSA). The basic events include: - Equipment failures or unavailabilities; - Common cause failures; - Human failure events; - Hazard specific events such as fire-induced circuit failure probabilities.	
RI-A02	Significant contributors to accident sequences, key safety functions, and systems are identified.	RATIONALE: Reviews of the solutions to system models, functional models and accident sequences are an essential part of the validation of the structure of the plant logic model, and furthermore, provide additional insights on the risk profile of the plant. For hazard events, significant contributors may include significant fire compartments or scenarios, significant flooding events, or other hazard related scenario information consistent with the level of resolution of the hazard PSA.
RI-A03	When assessing the significance of basic events using importance measures that involve setting failure probabilities to unity, such as the risk achievement worth (RAW), the assessment is performed by resolving the	RATIONALE: A cutset list generated with too high truncation value will exclude some components and therefore their RAW values are identically unity. An alternative to resolving the model is to use a cutset equation solved at a lower

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	PSA model rather than re-quantifying a pre-solved cutset list.	truncation value.

TABLE 14.2-B   ATTRIBUTES FOR RESULTS ANALYSIS AND INTERPRETATION: TASK RI-B ‘ASSESSMENT OF ASSUMPTIONS’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
RI-B	Assessment of the significance of assumptions and model uncertainties is performed.	
RI-B01	Key sources of model uncertainty are identified (see the comment).	COMMENT: A model uncertainty is one associated with the modelling of an issue or phenomenon, for which there is no consensus approach. Such model uncertainties are typically addressed by adopting one of a number of models, or making an assumption about the impact of a phenomenon on the operability of a system or function. A *key* source of uncertainty is one where the adoption of a different model or a different assumption can alter the significance of a contributor. Since different applications make use of different results, the key sources of uncertainty will differ between applications. RATIONALE: When the results of the PSA are to be used for decision making, the decision maker needs to be aware of the impact of the uncertainties on the PSA results used in the decision (see RI-B02). EXAMPLES of potential sources of model uncertainty include: - Success criteria; - RCP seal LOCA model; - Assumptions about the necessity for room cooling; - Choice of quantification model for human error probabilities; - Fire models and damage estimates; - Modelling of hazard impacts on HEPs; - Fragility models; - Hazard frequency models; - Model used for correlating failure; - Use of assumed cable routing in the fire PSA; - Fire-induced circuit failure probabilities and modelling
RI-B02	The effect of a significant assumption on the results is assessed by performing sensitivity studies, using different plausible assumptions.	RATIONALE: Understanding of the impact of modelling uncertainty on the results of the PSA is crucial to a decision maker. An exception can be when a particular model has been approved as the standard model.

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
		COMMENT: Some sensitivity studies can be performed by changes to parameter values, or turning off parts of the model to represent groups of failure. Others may involve adding new portions to the model. These are done in a manner consistent with the relevant attributes.
RI-B03	For model uncertainties or assumptions affecting the same parts of the PSA model, sensitivity studies are performed simultaneously to determine whether there are synergistic effects.	
RI-B04	The choice of the specific assumptions or models adopted for the base case model is justified.	RATIONALE: Understanding the reasons for choosing a specific assumption or model is important for the decision maker.

TABLE 14.2-C ATTRIBUTES FOR RESULTS ANALYSIS AND INTERPRETATION: TASK RI-C ‘DOCUMENTATION’

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
RI-C	Documentation and information storage is performed in a manner that facilitates peer review, as well as future upgrades and applications of the PSA by describing the processes that were used and providing details of the assumptions made and their bases.	
RI-C01	The results of the analysis of the significance of contributors are presented in a variety of ways to characterize the risk profile of the plant, i.e. what are the aspects of design and operational practices that have an impact on risk, how they impact risk, and why.	
RI-C02	The results of the sensitivity analyses are documented so that the impact of each significant assumption is characterized appropriately, and the choice of the assumption or model for the base case justified.	
RI-C03	The impacts of the sources of model uncertainty and assumptions identified in the previous tasks on the results analysis and interpretation are documented.	

15. MAINTENANCE AND UPGRADE OF THE PSA

15.1. MAIN OBJECTIVES

It is essential to have a process for updating the PSA to account for changes that impact the PSA model. The objective of maintenance and upgrade (MU) of the PSA is to update a PSA model to ensure it represents the as-designed, as-built, as-operated plant[12]. The MU process also accounts for the current state of the art in PSA techniques (e.g. thermal hydraulic analysis, fragility analysis, hazards frequency assessment, etc.) to the extent needed to support PSA applications.

The PSA model needs to be maintained as realistic as possible. However, as any other model, there are many approximations and assumptions that might impact its realism and the ability to use the PSA for applications. The specification of the boundary conditions and an identification of the approximations, assumptions and limitations of the PSA model determine the applications for which the PSA can be used. This specification is an integral part of the PSA process that can be changes with time and need to be comprehensively documented and maintained.

As a plant operates over time, its PSA risk estimate may change due to the following reasons:

- Improved methods or techniques;
- Updated operational data for the plant’s structures, systems, and components;
- Changes in plant design or operation.

The PSA model should account for all of these potential changes and should provide up to date risk estimates and risk insights. Therefore a process for maintaining and upgrading the PSA need to be developed to ensure:

- The PSA supporting information directly relates to existing plant information[13] or to the analysts' assumptions of how the plant is operated;
- The PSA is updated as changes are made to plant design and operation, feedback is obtained from internal and external operational experience, understanding of thermal hydraulic performance or accident progression is improved, or advances are made in modelling techniques.

[12] “As-built, as-operated” is the term that reflects the degree to which the PSA matches the current plant design, plant procedures, and plant performance data. At the pre-operational stages (design, construction, etc.) the plant is neither built nor operated and the term “as-built, as-operated” is meant to reflect the “as-designed plant” assuming site and operational conditions for the given design.

[13] The NPP design and operational information used to develop the PSA models may not be included in permanent plant documents outside of the PSA documents. Typical examples of the information not directly supported by plant documents is the information obtained: a) during plant walk-downs; b) from interviews and questionnaires to plant staff, from observation of simulator training sessions; c) from the analysis of maintenance records, operational logs, events reports, etc. All this information needs to be adequately and comprehensively documented in the framework of the PSA in order to link these plant design and operational features to the appropriate aspects of the PSA models and database.

Keeping the PSA up to date is essential for PSA applications. The scope and frequency of the update need to be the same for all the PSA elements and hazards, since PSA applications may utilize different PSA models (e.g. full power and shutdown models when comparing risk options) or different hazards (e.g. when importance measures from several hazards are used to determine significance). However, immediate update of the full scope PSA might not be feasible, or an update might not be rapidly performed. This could be acceptable for certain decisions when the updated PSA for one hazard (i.e. full power internal events) is all that is needed to justify the decision. However, it must be demonstrated that the expected changes in other parts of the PSA will not impact the decision made.

The maintenance and upgrade process need to be established at the initial stage of the PSA project to ensure that maintenance and upgrade of the PSA can be performed in a complete and comprehensive manner. If this was not performed when the PSA is initially developed, it is essential the process be put in place as soon as practical.

Maintenance and upgrade of the PSA is a part of PSA process rather than specific PSA element. However, it has several tasks with specific attributes similarly to other PSA elements.

15.2. MAINTENANCE AND UPGRADE OF THE PSA TASK AND ITS ATTRIBUTES

Table 15.1 lists the main tasks for the Maintenance and Upgrade of the PSA. Tables 15.2-A through 15.2-D present the description of general and special attributes for these tasks.

TABLE 15.1 MAIN TASKS FOR THE MAINTENANCE AND UPGRADE OF THE PSA

Task ID	Task Content
MU-A	Monitoring of PSA inputs and collecting new information
MU-B	Implementation of maintenance and upgrade of the PSA
MU-C	Control of the computer codes and models versions used for PSA model integration and quantification
MU-D	Documentation of maintenance and upgrade

TABLE 15.2-A ATTRIBUTES FOR MONITORING OF PSA INPUTS AND COLLECTING NEW INFORMATION

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MU-A	A process to monitor changes that could affect the PSA is established. This process is typically applied through the development and implementation of the PSA Configuration Control Program (CCP).		RATIONALE: In order to enable maintenance and upgrade process, the changes that can impact the PSA results and insights are monitored, including: – Changes in plant design and/or operation; – Updated operational data on the reliability of the plant’s structures, systems, and component; – New methods and techniques; – Improved methods or techniques in PSA and related areas.
MU-A01	The PSA CCP includes monitoring of changes in the design, operation and maintenance of the plant that could affect the PSA.		COMMENT: The changes include those that impact the scope of the PSA models, including one or more PSA elements (e.g. HRA, system analysis, failure data, accident sequence models). COMMENT: The plant configuration changes being monitored will depend on the scope of the PSA. For example, a PSA that includes internal fire hazards analysis will result in the CCP monitoring changes in the plant fire protection programme, procedures and related areas such as cable routing. Similarly, a PSA that includes shutdown will result in the CCP monitoring changes to the Outage Risk Management Program and related areas such as planned outage schedules.
	MU-A01-S1	*The PSA CCP for the plants at the design or construction phases is developed to ensure that each successive update of the PSA during the design-construction cycle corresponds to the design documents and assumptions existing at the moment of the update.*	*RATIONALE: At the design phase, PSAs are performed to evaluate the proposed design which can be frequently changed when different design options are assessed. At the construction phase, PSAs are updated to account for actual plant configuration. For both cases it is essential to account for the as-designed configuration in the PSA model.*

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MU-A02	The PSA CCP includes the monitoring of changes to the PSA technology and industry experience that could impact the results of the PSA model.	COMMENT: Changes in PSA technology include increased understanding of the plant behaviour and processes through either research and development or additional industry experience. EXAMPLE: Recent Fire-Induced Circuit Testing result in new modelling of spurious operation probability and duration values. This was documented in NUREG/CR-7150, V2 [47]. The changes will likely impact a Fire PSA result, and need to be incorporated during the next PSA update, if the changes are significant. EXAMPLE: During the design phase, NPPs heavily rely on features the PSA practice is rapidly changing (e.g. software reliability, passive systems reliability, digital C&I reliability). The ongoing research in these areas needs to be monitored and implemented in the PSA.
MU-A03	The PSA CCP evaluates the impact of single changes that would impact risk informed decisions and prioritizes them to ensure that the most significant changes are incorporated as soon as practical.	EXAMPLE: The CCP may rank PSA-impacting changes as High, Medium and Low based on the initial estimate of PSA impact. High could, for example, be based on greater than 25% change in risk or a factor of 2 increase in a single accident class or accident sequence. Additional qualitative factors involving completed RI-applications should also be considered. Medium may be, for example, a factor of 10 lower impact or higher. COMMENT: The decisions of if and when to update the PSA may change, when the change results in significant increases in risk.
MU-A04	The PSA CCP evaluates the cumulative impact of PSA changes that could impact the PSA results and risk informed applications.	COMMENT: The decisions of if and when to update the PSA may change, when combined changes result in significant increases in risk.

TABLE 15.2-B ATTRIBUTES FOR IMPLEMENTATION OF MAINTENANCE AND UPGRADE OF THE PSA

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MU-B	The implementation of the maintenance and upgrade in the PSA is performed sufficient to support PSA applications and ensure the PSA represents the as-designed, as-built, as-operated plant, and incorporate PSA technology developments and industry wide experience. The changes in the PSA models are controlled.	RATIONALE: The PSA used in various applications need to be as realistic as practical and should reflect the current design and operational practice using State of knowledge in the PSA technology.
MU-B01	The changes in the design, operation and maintenance of the plant that could affect the PSA are evaluated to determine whether a PSA update is required.	
MU-B02	The changes in the PSA technology or lessons learned from industry wide experience that could affect the PSA are evaluated to determine whether a PSA update is required.	COMMENT: Update of the PSA may include a new methodology or changes in scope or capability that impact the significant event sequences. This could include items such as new human error analysis methods, new data update methods, new approaches to quantification, or new treatment of CCF. COMMENT: Monitoring of PSA technology is particularly important for the design phase of the plant.
MU-B03	The update of the PSA is performed as soon as practical when changes are identified that has the potential to significantly impact PSA results and risk informed decisions.	EXAMPLE: Changes to the plant that impact the PSA may be included in a PSA update process, involving a PSA change form (more typically in a database form). The PSA update is typically performed on a regular basis (e.g. every 2-3 years), but may be updated more frequently if a PSA change is determined to have a large impact that may change the decisions made for one or more PSA applications. Off-schedule changes are implemented as soon as practical, and may include other PSA changes already identified or may include only the significant PSA changes, depending on the schedule need for the update.
MU-B04	Changes to a PSA model due to PSA updates meet the attributes for specific PSA elements.	RATIONALE: All changes in the PSA model and documentation need to be in compliance with the attributes defined in Sections 4-14 of this document.
	MU-B04-S1 *Updates of a PSA that involve new methodologies receive a review for the areas of the PSA that have been updated.*	*RATIONALE: Update of the PSA may lead to significant changes in the PSA model that should receive an independent review. This is particularly important when changes involve implementation of new methodologies.*

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MU-B05	When the PSA results and insights are used in RI applications between updates of the PSA, the cumulative impact of pending changes are shown to not impact the application results and insights.	RATIONALE: It is recognized that PSA update is not always feasible immediately following a design or plant change or upon identification of a subject for model improvement. Therefore, the PSA may not represent the plant until the change or model improvements are incorporated into the PSA. However, this is acceptable for use in applications that are not impacted by the changes.
MU-B06	The impact on risk informed applications previously performed are reviewed when the PSA update is complete. Update to the risk informed applications is performed if the insights or decisions change as a result of the update.	RATIONALE: One of the inputs to determining if and when to update a PSA is the impact on previously performed risk informed applications. In many cases, the applications will be unaffected by the PSA update, especially if the application involves a “change in CDF” calculation where the change in risk is very small. However, when it is evident that the application results are potentially impacted by the PSA update, the update needs to be performed as soon as practical and the Risk informed application need to be updated to reflect the latest PSA results.
MU-B07	The PSA model versions are retained. The differences between PSA versions are understood and documented.	RATIONALE: The risk informed decisions made in the past may need to be reproduced using the PSA at the time of the risk informed application. The PSA model used for each Risk informed application revision need to be maintained to allow for reproducing the results or review of the impact of plant changes.

TABLE 15.2-C ATTRIBUTES FOR CONTROL OF THE COMPUTER CODES AND MODELS USED FOR PSA MODEL INTEGRATION AND QUANTIFICATION

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MU-C	The PSA model quantification results are verified when new version of PSA software is released and used.	
MU-C01	When transferring to the new version of the PSA software, or new software is used, the consistency and reproducibility of the results are verified. The differences in the results are explained and shown to be correct. The PSA CPP includes a process for control of computer codes used to support PSA quantification. PSA results are compared when new versions of PSA software are implemented.	RATIONALE: The PSA models developed under an earlier version of PSA software believed to be fully compatible with a new software version. However, it often happens that changes in the versions of PSA software may lead to different results of the PSA.

TABLE 15.2-D ATTRIBUTES FOR DOCUMENTATION OF MAINTENANCE AND UPGRADE

Task / GA	Characterization of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MU-D	Documentation and information storage of the PSA Update is performed in a manner that facilitates review, as well as future upgrades and applications of the PSA.	
MU-D01	The documentation of a PSA Update demonstrates that the PSA is consistent with the as-designed, as-built, as-operated plant as well as with the State of knowledge in PSA technology and industry wide experience. The differences in the versions of the PSA models prior and after update are understood and documented.	COMMENT: The documentation typically includes the following: a. Description of changes in a PSA model due to each PSA update including the basis for each change; b. Analyses of the results obtained using PSA model prior to and after an update c. Documentation for the reasons for differences between before and after PSA results d. Record of the process and results used to address the cumulative impact of pending changes; e. Analyses of the results obtained using PSA model with earlier and current PSA software versions and reasons for differences (if any).

16. DETERMINATION OF SPECIAL ATTRIBUTES FOR PSA APPLICATIONS

As mentioned earlier in the publication, it is assumed that general attributes described in the publication characterize a contemporary state of the art PSA performed with the aim of assessing the overall NPP safety. The special attributes provide additional requirements within particular PSA elements to meet specific needs of PSA applications.

In order to indicate what specific features of PSA are needed for particular PSA applications, Tables 16.1 through 16.6 were developed that provide information in a structured form on which special attributes are appropriate for the applications included in the PSA application categories defined in Section 2 and briefly described in Appendix II. The special attributes in these tables are distinguished as 'Essential' and 'Supplemental'.

An e*ssential SA* emphasizes a feature of a PSA element that is considered to be important to generate the results needed to reliably support the PSA application. Failure to meet an essential SA may preclude meaningful use of the study for an intended application.

Supplemental SAs are those that are not necessarily important for a specific application but could further enhance the usefulness of the PSA by providing a greater level of detail, or improving confidence in the results. In general, it is expected that failure to meet a supplemental SA does not have a significant impact on the overall results of the PSA application, but may limit the fidelity of the study for certain applications.

In the frame of this publication, it is difficult to foresee all possible PSA application cases and their specific features. Therefore, the division into Essential and Supplemental special Attributes is to some extent subjective but it is included here to provide a general orientation on the importance of the special attributes in relation to PSA applications. It need to be also noted that there are cases when the same special attribute could be considered as essential for some of the applications and supplemental for the others.

Table 16.7 provides a mapping of the Special attributes of the PSA elements to the list of PSA applications presented in Section 2 thus providing an overview of what sets of the Special Attributes are appropriate for each application. Special attributes for the PSA elements listed in SSG-3 [3] are shown in separate columns, for other PSA elements introduced in this publication they are combined under the column "Other".

The following steps provide a practical approach to using the information presented in this publication to determine the Special attributes appropriate for the application of interest:

STEP (1) Identify the PSA application category(s) and specific application(s) from the list presented in Section 2. If needed, consult Appendix II to get supporting information characterizing PSA applications.

STEP (2) Consult Table 16.7 for the set of identifiers of Essential and Supplemental special attributes relevant for the application.[14] If several applications are planned, the corresponding attributes have to be selected and considered jointly.

STEP (3) Consult relevant information presented in Tables 16.1-16.6 in order to get understanding of what features of the PSA could be achieved if the special attributes are met.

STEP (4) Consult Section 3.1 to get information on which sections of the publication address the selected special attributes.[15]

STEP (5) Consult corresponding Sections 4-14 of the publication to get information on the content of the special attributes and the features of PSA elements needed to meet them.

[14] In Table 16.7, the identifiers of essential special attributes are provided in bold font. The identifiers of supplemental special attributes are provided in regular font.

[15] The first two letters of the identifier of a special attribute indicate the corresponding PSA element.

TABLE 16.1 SAFETY ASSESSMENT

SA Identifier	Relevance to Specific Applications in the Category
Essential SAs	
	No Essential SAs identified.
Supplemental SAs	
AS-C03-S1	Plant specific realistic thermal hydraulic analyses are necessary to assure a realistic representation of the specific plant features influencing the accident progression (Application 1.2).
AS-C13-S1	Detailed modelling of ATWS sequences provides a better understanding of the impact of reactor protection system failures in the plant risk profile (Application 1.2).
AS-C17-S1	An expanded graphical representation of the accident progression is helpful for documenting the accident sequence models, as well as for understanding, updating, and use of the PSA for Applications 1.2.
DA-D06-S1	Understanding of the impact of potentially reduced reliability of the systems operating under conditions that are more severe than those under which the failure events data are collected is important for the assessment of plant safety (Applications 1.1,1.2,1.3)
DA-H02-S1	A periodic safety review requires an update of the reliability parameters, which in turn is facilitated by plant equipment failure data that are electronically retrievable and an evaluation that is retrievable and reproducible (Application 1.2).
DF-F01-S1	A structured identification and consideration of subtle interactions based on historical information from other plants is helpful for the completeness of the PSA model used for realistic estimation of changes in plant risk (Application 1.2).
DF-G01-S1	A relational database containing information on different dependencies and their interconnections is helpful for providing the completeness of the PSA model used for realistic estimation of changes in plant risk (Application 1.2).
HE-D01-S1 HE-E01-S1	In design stage of a plant the information needed to support the internal fire or flooding PSA is not complete or simply not yet available. Any missing information needed to develop the hazard definitions are documented in the assumptions, which can later be used in the uncertainty and sensitivity analysis (Application 1.3).
HR-F02-S1	Hazard specific definitions for each HFE will ensure the HRA is performed accurately. These definitions include sequence definitions such as sequence timing, as well as performance shaping factors such as the impact of flooding, smoke or blocked access (Applications 1.3)
HR-G04-S1	The time windows for operator actions that are based on plant specific thermal hydraulic analyses and/or simulator exercises provide a more realistic input in the HRA and thus promote getting plant specific insights dealing with operator performance (Application 1.2).
IE-H02-S1	The availability of information on IEs in the form of an electronic database is useful for periodic PSA updating (Application 1.2).
SC-B01-S1	The use of proven computer codes and realistic models help to avoid conservative and simplifying success criteria which may mask out the differences or effects of changes (Application 1.2).
SY-C01-S1	PSA applications requiring detailed modelling of the impact of pipe ruptures will benefit from modelling the impact on connected systems and components. (Application 1.3)

TABLE 16.2 DESIGN EVALUATION

SA Identifier	Relevance to Specific Applications in the Category
Essential SAs	
DA-C02-S1	For newly designed plants, when plant specific data are not available, the choice of generic data becomes important for justifiable risk results (Application 2.1).
DA-D06-S1	Understanding of the impact of potentially reduced reliability of the systems operating under conditions that are more severe than those under which the failure events data are collected is important for the assessment of different design options and for identification of the research activities to support the design (Applications 2.1,2.2,2.5)
SY-C07-S1	Realistic estimation of the failure probabilities in specific system conditions provides important information for insights regarding the plant behaviour for newly designed NPPs (Applications 2.1 and 2.2).
SY-C15-S1 SY-C16-S1	Consideration of intrasystem common cause failures and more detailed modelling of CCF are important for realistic estimation of the plant risk for newly designed NPPs (Applications 2.1 and 2.2.
Supplemental SAs	
AS-B03-S1 AS-C03-S1 AS-C04-S1 AS-C16-S1	Use of best estimate codes, plant specific t/h analyses, and best estimates of important modelling parameters may help to gain additional insights for evaluation of design features and possible alternatives (Applications 2.1,2.4).
AS-C14-S1	Detailed modelling of ATWS sequences provides support for the evaluation of the effectiveness of reactor protection system design from the risk perspective (Application 2.1).
AS-C17-S1	An expanded graphical representation of accident progression is helpful for documentation of accident sequence models, as well as for understanding, updating, and use of the PSA (Application 2.1).
DA-D06-S1	In certain accident sequences the equipment may operate under more severe conditions that during tests or may be exposed to the conditions beyond the design limits. New failure rates may need to be estimated for those sequences, rather than assuming failure or no change from the predicted reliability at normal/typical conditions. (Application 2.3)
DF-F01-S1	A structured identification and consideration of subtle interactions is helpful for modelling dependencies for newly designed NPPs (Applications 2.1 and 2.2)
DF-G01-S1	A relational database containing information on different dependencies is helpful for providing the completeness of the PSA model used for the assessment of an existing plant design and an updated/revised plant design (Application 2.2).
HE-D01-S1 HE-E01-S1	In design stage of a plant the information needed to support the internal fire or flooding PSA is not complete or simply not yet available. Any missing information needed to develop the hazard definitions are documented in the assumptions, which can later be used in the uncertainty and sensitivity analysis (Applications 2.1, 2.2, and 2.3).
HE-D04-S2 HR-E07-S1	Modelling of spurious operation that may lead to a failure of operator actions or result in an undesired operator action that impacts a credited function is important for a complete review of potential operator responses. (Application 2.6)
HR-F02-S1	Hazard specific definitions for each HFE will ensure the HRA is performed accurately. These definitions include sequence definitions such as sequence timing, as well as performance shaping factors such as the impact of flooding, smoke or blocked access (Applications 2.3 and 2.6)

SA Identifier	Relevance to Specific Applications in the Category
HR-G01-S1 HR-G02-S1 HR-K02-S1	Performing a detailed assessment of all HFEs avoids the need for iteration for specific applications (Application 2.6)
IE-C02-S1 IE-C02-S2	More detailed grouping of the events at the design phase helps to identify and eliminate deficiencies in the systems design (Application 2.1).
MQ-B05-S1 MQ-B05-S2 MQ-D01-S1	Use of reduced truncation values for quantification of the whole PSA model or in relation to the particular IEs of major interest may be useful for the assessment of safety of an existing plant design (Application 2.2).
MU-A01-S1	At the design phase, PSAs are performed to evaluate the proposed design which can be frequently changed when different design options are assessed. At the construction phase, PSAs are updated to account for actual plant configuration. For both cases it is essential to account for the as-designed configuration in the PSA model (Applications 2.1, 2.2)
MU-B04-S1	Risk Applications submitted for regulatory approval would normally require an independent review of any PRA updates where the risk informed application is impacted. (Applications 2.1 and 2.2),
OS-C01-S1	Shutdown PSA perform during design may need to include a review of operational experience of similar plants with the same refuelling programme, generic PSA studies, design requirements, planned refuelling procedure, or other sources of information (Application 2.1)
SC-B01-S1	The use of proven computer codes and realistic models help to avoid conservative and simplifying success criteria (Application 2.2).
SY-B19-S1	Revisiting the components screening process promotes a more realistic estimation of the risk for newly designed NPPs at different stages of the design (Applications 2.1, 2.2 and 2.4)
SY-B22-S1	A detailed modelling of the components promotes a better appreciation of the risk impact of constituting parts of components for newly designed NPPs (Applications 2.1, 2.2 and 2.4)
SY-C01-S1	PSA applications requiring detailed modelling of the impact of pipe ruptures will benefit from modelling the impact on connected systems and components. (Application 2.3)

TABLE 16.3 NPP OPERATION

SA Identifier	Relevance to Specific Applications in the Category
Essential SAs	
AS-B03-S1 AS-C03-S1 AS-C04-S1 AS-C16-S1	Use of best estimate codes, plant specific t/h analyses, and best estimates of important modelling parameters is essential for adequate modelling of accident scenarios being addressed in the emergency operating procedures for Applications 3.2.1, 3.3.1, and 3.4.2.
AS-C05-S1 AS-C06-S1 AS-C08-S1	Incomplete modelling of accident progression dealing with requirements of plant emergency procedures may cause incomplete or inadequate coverage of accident scenarios for Applications 3.2.1, 3.3.1, and 3.4.2.
DA-B01-S1	Too broad grouping of components will prevent the identification of specific features of members of the group, which is of importance to maintenance planning and configuration control activities (Applications 3.1.1 and all of Application Group 3.4).
DA-D05-S1	Realistic representation in the model of surveillance tests and planned maintenance activities is essential for maintenance programme optimization and configuration planning (Applications 3.1.1 and 3.4.1).
DA-E01-S1	The time trend analysis is essential for activities dealing with optimization of plant aging management programme (Application 3.1.3).
HR-G02-S1	The capability of the HRA method used to evaluate the impact of procedure changes is essential for Applications 3.2.1 and 3.2.2.
HR-G04-S1	The time line for the human interactions for dominant ASs defined based on realistic plant specific thermal hydraulic analyses and/or simulator exercises is essential for the development and improvement of emergency operating procedures and improvement of operator training programmes (Applications 3.2.1 and 3.3.1).
IE-B01-S1	It is important to reconsider the events screened out based on low frequency that are impacted by the equipment subjected to the TS exemption (Application 3.4.3).
MQ-C02-S1	A more detailed modelling of specific system configurations (e.g. maintenance on specific trains) is important for maintenance programme optimization (Application 3.1.1) and all Risk Monitor type applications (Application Group 3.4).
SY-B14-S1	The possibility to effectively handle maintenance basic events allows assessment of the impact of maintenance programme optimization (Application 3.1.1), impact of improvements in maintenance personnel training programme (Application 3.3.2), and is essential for the real time configuration assessment and control, configuration planning, exemptions to TS, justification for continued operation, and dynamic risk informed TS (Application Group 3.4).
SY-B14-S2	Modelling of test and maintenance unavailabilities at train level is needed for the real time configuration assessment and control, configuration planning, exemptions to TS, justification for continued operation, dynamic risk informed TS, and maintenance programme optimization (Application 3.1.1 and Application Group 3.4).
SY-B14-S3	Symmetric models are needed for Risk Monitor type applications in order to avoid overestimation or underestimation of specific POS (Application Group 3.4).
SY-B19-S1 SY-B22-S1	Maintenance programme and ageing management may include more components than those already modelled in the system models and the models would need to be extended to the level of detail needed for the assessment of the impact of maintenance programme optimization (Applications 3.1.1 and 3.1.3).

SA Identifier	Relevance to Specific Applications in the Category
SY-B23-S1	Time dependent modelling is needed for application dealing with changes to test activities (Application 3.4.1).
Supplemental SAs	
AS-B03-S1 AS-C03-S1 AS-C04-S1 AS-C16-S1	Use of best estimate codes, plant specific t/h analyses, and best estimate of important modelling parameters is useful for realistic modelling of accident scenarios being used for the improvement of management training programmes based on plant specific PSA insights (Application 3.3.3).
AS-C05-S1 AS-C06-S1 AS-C08-S1	A more complete modelling of accident progression dealing with requirements of plant emergency procedures is useful for the improvement of management training programmes (Application 3.3.3).
AS-C17-S1	An expanded graphical representation of accident progression is helpful for documentation of accident sequence models, as well as for understanding, updating, and use of the PSA for Applications 3.3.1, 3.3.2, 3.3.3, and 3.4.2.
DA-D05-S1	Realistic representation in the model of surveillance tests and planned maintenance activities is useful for getting insights for improvement of operator and management training programmes (Applications 3.3.1, 3.3.3, 3.4.2, 3.4.3, and 3.4.4).
DA-D06-S1	In certain accident sequences the equipment may operate under more severe conditions that during tests or may be exposed to the conditions beyond the design limits. New failure rates may need to be estimated for those sequences, rather than assuming failure or no change from the predicted reliability at normal/typical conditions. (Application 3.2.2)
DA-F02-S1	Since CCFs often have a major impact on system unavailability, particularly in highly-redundant systems, a more realistic and specific modelling of CCF events would improve the plant configuration control applications (Application Group 3.4).
DF-F01-S1 DF-G01-S1	A structured identification and consideration of subtle interactions and availability of a relational database containing information on different dependencies is helpful for maintenance programme optimization (Application 3.1.1), support for plant ageing management programme (Application 3.1.3), development and improvement of the emergency operating procedures and NPP accident management (Applications 3.2.1 and 3.2.2). Availability of a database containing information on different dependencies provides possibility to efficiently maintain a living PSA model for Risk Monitor type applications (Application Group 3.4).
HE-D04-S1	Equipment affecting containment function, such as containment isolation or cooling is modelled in the Fire PSA in order to determine severe accident release estimates following a fire (Application 3.2.2).
HR-D06-S1	An identification of past problems can help to identify improvements in maintenance practices (Applications 3.1.1 and 3.3.2).
HR-E02-S1	Identification of the conditions and plant status conducive to errors of commission could reduce the potential for such errors (Application 3.3.1).
HR-G02-S1 HR-G04-S1 HR-K02-S1 HR-K05-S1	Improvement of the management training programme and outage management would benefit from a more realistic HRA that use the time windows for operator actions which are based on plant specific thermal hydraulic analyses and/or simulator exercises and use of more precise screening criteria for HFE that could lead to an initiating event (Applications 3.1.4, 3.3.3, and 3.3.5).

SA Identifier	Relevance to Specific Applications in the Category
IE-B01-S1	1) Previously screened IEs caused by equipment failures may appear in the list with a higher frequency due to changes in the maintenance programme (Application 3.1.1). 2) It is useful to re-consider low frequent events that have a potential to cause un-mitigated releases (Applications 3.2.2 and 3.2.3).
IE-H02-S1	An electronic IE database is helpful in assessing the impact of components aging, which may be the cause for the changes in the number of IEs (Application 3.1.3).
MQ-A01-S1 MQ-C02-S1	A more detailed modelling of specific system configurations (e.g. maintenance on specific trains) is helpful for the improvement of operator and management training programmes (Applications 3.3.1 and 3.3.3).
MU-B04-S1	Risk Applications submitted for regulatory approval would normally require an independent review of any PRA updates where the Risk informed application is impacted. (Application 3.4.4)
OS-A01-S1	Consideration of forced outages resulting from safe short term accident sequences at-power is important for the support for NPP accident management (Application 3.2.2).
OS-A03-S1 OS-C01-S2	One time or specific known activities as well as specific duration of POSs that are determined based on an actual planning are accounted for in the assessment of outage risk (Application 3.1.5)
SC-A03-S1	Modelling the decay heat level based on the planning outage and POS durations will ensure the shutdown PSA is accurate (Application 3.1.5).
SC-B01-S1	The use of proven computer codes and realistic models helps to avoid conservative and simplifying success criteria; this is useful dynamic risk informed TS application (Application 3.4.4).
SY-B14-S1 SY-B14-S2	The possibility to effectively handle test and maintenance basic events may be useful for the improvement of operator training programmes (Application 3.3.1).
SY-B19-S1 SY-B22-S1	Improvement of operator training programmes may ask for inclusion of more components than those already modelled in the system models (Application 3.3.1).

TABLE 16.4 PERMANENT CHANGES TO THE OPERATING PLANT

SA Identifier	Relevance to Specific Applications in the Category
Essential SAs	
AS-B03-S1 AS-C03-S1 AS-C04-S1 AS-C16-S1	Use of best estimate codes, plant specific t/h analyses, and best estimates of important modelling parameters is essential for adequate modelling of the accident scenarios being addressed in the emergency operating procedures (Application 4.1.1).
DA-C02-S1	Use of generic sources of data for reliability parameters for new equipment need to be justified (Application 4.1.1).
DA-E01-S1	A time trend analysis of the existing trends in the reliability parameters is important for Application 4.1.2.
IE-H02-S1	An electronic IE database is essential for Applications 4.1.2, 4.3.1, and 4.3.2.
MQ-C02-S1	A more detailed modelling of specific system configurations is important for applications dealing with changes in TS (Application Group 4.2, and 4.3.1).
SC-B01-S1	The use of proven computer codes and realistic models helps to avoid conservative and simplifying success criteria; this is essential for the assessment of the effects of changes (Application 4.1.1).
SY-B14-S1	The possibility to effectively handle maintenance basic events allows assessing the impact of changes to the allowed outage time and required TS actions (Application 4.2.1).
SY-B14-S2	A detailed maintenance model allows an assessment of the impact of changes to the allowed outage time and required TS actions (Application 4.2.1).
SY-B14-S3	Symmetric models are essential for realistic evaluation of changes to AOT, required TS actions, surveillance test intervals, as well as for the equipment risk significance evaluation and evaluation of changes to QA requirements (Applications 4.2.1, 4.2.2, 4.2.3, 4.3.1, and 4.3.2).
SY-B23-S1	Time dependent failure models allow for the assessment of impact of NPP upgrades (Application 4.1.1), changes to the allowed outage time and required TS actions, changes to surveillance test intervals (Applications 4.2.1, 4.2.2, 4.2.3), and risk informed in-service testing (Application 4.2.4).
SY-C01-S1	PSA applications dealing with optimization of ISI or RI-internal flooding require adequate modelling of the impact of pipe ruptures if the latter are included in the model (Application 4.2.5 and 4.4.2).
Supplemental SAs	
AS-C05-S1 AS-C06-S1	Incomplete modelling of accident progression dealing with requirements of plant emergency procedures may cause incomplete or inadequate coverage of accident scenarios for Application 4.1.1.
AS-C17-S1	An expanded graphical representation of accident progression is helpful for documentation of accident sequence models, as well as for understanding, updating, and use of the PSA for Application 4.1.1.
DA-B01-S1	A finer level of resolution in identifying groups of components is helpful because too broad grouping can mask the specific features of group members (Application Group 4.2).
DA-D05-S1	A realistic representation of surveillance and maintenance activities is useful for assessing the impact of specific changes (Applications 4.1.1, 4.4.1 and 4.4.2, and Application Group 4.2).

SA Identifier	Relevance to Specific Applications in the Category
DA-D06-S1	In certain accident sequences the equipment may operate under more severe conditions that during tests or may be exposed to the conditions beyond the design limits. New failure rates may need to be estimated for those sequences, rather than assuming failure or no change from the predicted reliability at normal/typical conditions. (Applications 4.4.1, 4.4.2, and 4.4.3)
DA-F02-S1	Because technical specifications such as allowed outage times relate to individual trains of systems, a detailed modelling of CCFs reflecting the number of redundancies/diversities and a realistic and specific modelling of CCF events is helpful for assessing the impact of common cause failures (Application Group 4.2).
DF-G01-S1	Analysis of the risk impact of NPP upgrades and justification for lifetime extension may benefit from detailed identification and modelling of possible dependencies and availability of database containing information on different dependencies (Applications 4.1.1 and 4.1.2).
HE-D04-S1	Equipment affecting containment function, such as containment isolation or cooling is modelled in the Fire PSA (Application 4.1.1).
HE-D04-S2 HR-E07-S1	Modelling of spurious operation that may lead to a failure of operator actions or result in an undesired operator action that impacts a credited function is important for a complete review of potential operator responses. (Application 4.4.1).
HE-K09-S1	Fire protection features credited in risk significant fire scenarios are estimated using plant specific availability data in order to better estimate the fire risk for risk-informed fire protection (Application 4.4.1).
HR-F02-S1	Hazard specific definitions for each HFE will ensure the HRA is performed accurately. These definitions include sequence definitions such as sequence timing, as well as performance shaping factors such as the impact of flooding, smoke or blocked access (Applications 4.4.1) and 4.4.2).
HR-G01-S1	Performing a detailed assessment of all HEPs may be useful in prioritising the NPP upgrades, backfitting activities and plant modifications (Application 4.1.1).
HR-G04-S1	Categorization of SSCs would benefit from a more realistic HRA that use the time windows for operator actions which are based on plant specific thermal hydraulic analyses and/or simulator exercises (Application 4.3.1).
IE-B01-S1	NPP upgrades, life-time extension and changes in in-service testing may increase the frequency of the previously screened low frequent events (Applications 4.1.1 and 4.1.2).
IE-C02-S1 IE-C02-S2	Merging of the IE in a single group may mask the impact of plant modifications or changes in testing/inspections activities (Applications 4.1.1, 4.2.4, and 4.2.5).
IE-F12-S1	The detailed impact analysis for fire initiating events includes deterministic fire propagation calculations using qualified computer codes in order to reduce the unnecessary conservatism of the associated assumptions (Application 4.4.1).
MQ-B05-S2 MQ-D01-S1	Use of reduced truncation limits in relation to the particular IEs of major interest may be useful for the assessment of benefits from specific NPP upgrades (Application 4.1.1).
MU-B04-S1	Risk Applications submitted for regulatory approval would normally require an independent review of any PRA updates where the risk informed application Risk informed application is impacted. (Applications 4.1.1, 4.2.3, 4.2.4, 4.2.5, 4.3.1, and 4.3.2.
SY-B06-S1	Modelling of pipe failures in the PSA provides the possibility to more precisely assess the importance to risk of particular pipelines/pipe segments that would give a more robust input to the applications dealing with optimization of ISI (Application 4.2.5 and 4.4.2).

SA Identifier	Relevance to Specific Applications in the Category
SY-B14-S1 SY-B14-S2	A realistic representation of test and maintenance unavailabilities in system models is useful for risk informed in-service testing (Application 4.2.4).
SY-B19-S1	Other components than those originally modelled may need to be included in the PSA (Applications 4.1.1, 4.2.1, 4.2.2, 4.2.3, 4.2.5, 4.3.1, 4.3.2).
SY-B22-S1 SY-C16-S1	A deeper level of model resolution down to the level of details needed to assess the impact of specific changes associated with the application may be needed (Applications 4.1.1, 4.2.1, 4.2.3, 4.2.4, 4.2.5, 4.3.1, and 4.3.2).
SY-B23-S1	Time dependent failure models are useful for the equipment risk significance evaluation and evaluation of the risk impact of changes to QA requirements (Applications 4.3.1 and 4.3.2).

TABLE 16.5 OVERSIGHT ACTIVITIES

SA Identifier	Relevance to Specific Applications in the Category
Essential SAs	
IE-C02-S1	The lists of IEs and IE groups need to be detailed enough to allow the evaluation of inspection findings and operational events (Application 5.2.2).
SC-B01-S1	The use of proven computer codes and realistic models helps to avoid conservative and simplifying success criteria; this is essential for the assessment of a particular inspection finding or event (Application Group 5.2).
Supplemental SAs	
All AS-SAs	Detailed realistic representation of plant behaviour addressing different mitigation strategies would be helpful for adequate reflection of a wider range of inspection findings and operational events in the PSA model (Applications 5.2.1 and 5.2.2).
DA-B01-S1 DA-F02-S1 DA-H02-S1	These SAs would result in a more detailed PSA and better understanding of particular performance issues (Applications 5.1.2, 5.1.3, Application Group 5.2).
DF-F01-S1 DF-G01-S1	Detailed identification and modelling of possible dependencies and availability of database containing information on different dependencies is helpful for all Applications in Category 5.
IE-H02-S1	An electronic IE database is useful for Application Group 5.1.
MQ-B05-S1 MQ-B05-S2 MQ-D01-S1	Application of reduced truncation values may be useful for planning the inspection activities (Application 5.1.1), for the analysis of performance indicators (Applications 5.1.2 and 5.1.3), and for possibility to assess inspection findings and operational events (Applications 5.2.1 and 5.2.2).
MQ-C02-S1	A more detailed modelling of specific system configurations may be useful for planning the inspection activities and assessment of risk based performance indicators (Application Group 5.1).
SY-B19-S1 SY-B22-S1 SY-C16-S1	More components may need to be included into the model for Application Group 5.2.

TABLE 16.6 EVALUATION OF SAFETY ISSUES

SA Identifier	Relevance to Specific Applications in the Category
All SAs	For Application 6.1.1, 6.1.2, 6.1.5, 6.2.1 and 6.2.2, any of the special attributes may be required on a case-by-case basis depending on the issue to be analysed. For these applications, the PSA model need to be upgraded in a manner that would allow evaluating the impact associated with the considered measure or issue by the PSA model.
MQ-B03-S1 OS-A01-S2 OS-B01-S1 OS-C01-S4 HE-B06-S1 AS-B01-S1 DA-F01-S1	The modelling of multiunit attributes in the PSA model is required to help determine the overall site risk for multiunit accidents, including modelling of POSs, multiunit CCF, the screening of multiunit hazards and modelling of accident sequences (application 6.1.4).
SY-C07-S1	Realistic estimation of the failure probabilities in specific system conditions provides a better understanding of the deviations between an existing plant design and revised design-related rules (Application 6.1.3).
SY-C15-S1 SY-C16-S1	Consideration of intrasystem common cause failures and more detailed modelling of CCF provide a better understanding of the deviations between an existing plant design and revised design-related rules (Application 6.1.3).
Supplemental SAs	
DA-D06-S1	In certain accident sequences the equipment may operate under more severe conditions that during tests or may be exposed to the conditions beyond the design limits. New failure rates may need to be estimated for those sequences, rather than assuming failure or no change from the predicted reliability at normal/typical conditions (Application 6.1.3).
DF-F01-S1	A structured identification and consideration of subtle interactions is helpful for modelling dependencies and assessing the safety importance of deviations between an existing plant design and updated/revised design-related rules (Application 6.1.3).
DF-G01-S1	A relational database containing information on different dependencies is helpful for providing the completeness of the PSA model used for the assessment of safety importance of deviations between an existing plant design and updated/revised design-related rules (Application 6.1.3).
HR-F02-S1	Hazard specific definitions for each HFE will ensure the HRA is performed accurately. These definitions include sequence definitions such as sequence timing, as well as performance shaping factors such as the impact of flooding, smoke or blocked access (Applications 6.1.3).
MQ-B05-S1 MQ-B05-S2 MQ-D01-S1	Use of reduced truncation values for quantification of the whole PSA model or in relation to the particular IEs of major interest may be useful for the assessment of safety importance of deviations between an existing plant design and updated/revised design-related rules (Application 6.1.3).
SC-B01-S1	The use of proven computer codes and realistic models help to avoid conservative and simplifying success criteria which may mask out differences or effects of changes (Application 6.1.3).
SY-B19-S1	Revisiting the components screening process promotes a better understanding of the deviations between an existing plant design and revised design-related rules (Application 6.1.3).
SY-B22-S1	A detailed modelling of the components provides a better understanding of the deviations between an existing plant design and revised design-related rules (Application 6.1.3).

SA Identifier	Relevance to Specific Applications in the Category
SY-C01-S1	PSA applications requiring detailed modelling of the impact of pipe ruptures will benefit from modelling the impact on connected systems and components (Application 6.1.3).

TABLE 16.7 MAPPING THE SPECIAL ATTRIBUTES OF PSA ELEMENTS TO PSA APPLICATIONS[16]

PSA Application	PSA Application Group/	PSA Elements								
Category	PSA Application	IE	AS	SC	SY	HR	DA	DF	MQ	Other
1. SAFETY ASSESSMENT	1.1 Assessment of the overall plant safety	-	-	-	-	-	DA-D06-S1		-	-
	1.2 Periodic safety review	IE-H02-S1	AS-C03-S1 AS-C13-S1 AS-C17-S1	SC-B01-S1	-	HR-G04-S1	DA-D06-S1 DA-H02-S1	DF-F01-S1 DF-G01-S1	-	-
	1.3 Analysis of the degree of defence in depth and safety margin against beyond design basis site hazards, including correlated site hazards	IE-B01-S1	-	-	SY-C01-S1	-	DA-D06-S1	-	-	HE-D01-S1 HE-E01-S1 HR-F02-S1
2. DESIGN EVALUATION	2.1 Application of PSA to support decisions made during the NPP design (plant under design)	IE-C02-S1 IE-C02-S2	AS-B03-S1 AS-C03-S1 AS-C04-S1 AS-C14-S1 AS-C16-S1 AS-C17-S1	-	**SY-C07-S1** **SY-C15-S1** **SY-C16-S1** SY-B19-S1 SY-B22-S1	-	**DA-C02-S1** **DA-D06-S1**	DF-F01-S1	-	HE-D01-S1 HE-E01-S1 MU-A01-S1 MU-B04-S1 OS-C01-S1
	2.2 Licensing of design	-	-	SC-B01-S1	**SY-C07-S1** **SY-C15-S1** **SY-C16-S1** SY-B19-S1 SY-B22-S1	-	**DA-D06-S1**	DF-F01-S1 DF-G01-S1	MQ-B05-S1 MQ-B05-S2 MQ-D01-S1	HE-D01-S1 HE-E01-S1 MU-A01-S1 MU-B04-S1

[16] The general attributes described in Sections 4-15 of the publication are considered applicable to all PSA applications and are not referred in the table. Only the special attributes to be met in addition to the general attributes are depicted. The identifiers of the attributes that are considered essential for the applications (i.e. essential special attributes introduced in Section 16), are provided in **bold font**. Those attributes, which could be helpful for the applications, but are not deemed very important in accordance with the current state of the art (i.e. supplemental special attributes introduced in Section 16), are provided in regular font.

PSA Application	PSA Application Group/	PSA Elements								
Category	PSA Application	IE	AS	SC	SY	HR	DA	DF	MQ	Other
	2.3 Optimization of protection against hazard events (e.g. fires, floods) and common cause failures, including consideration of correlated site hazards and hazard-induced fires and floods	-	-	-	SY-C01-S1		DA-D06-S1	-	-	HE-D01-S1 HE-E01-S1 HR-F02-S1
	2.4 Establishment of equipment reliability targets for manufactories	-	AS-B03-A1	-	SY-B19-S1	-	-	-	-	-
	2.5 Identification of R&D which are necessary to support the design	-	-	-	-	-	**DA-D06-S1**	-	-	-
	2.6 Development operator procedures and training programmes and support for Human Factors Engineering	-	-	-	-	HR-G01-S1 HR-G02-S1 HR-K02-S1 HR-E07-S1 HR-F02-S1	-	-	-	HE-D04-S2
3. NPP OPERATION	**3.1 NPP maintenance**									
	3.1.1 Maintenance programme optimization	-	-	-	**SY-B14-S1** **SY-B14-S2** **SY-B19-S1** **SY-B22-S1**	HR-D06-S1	**DA-B01-S1** **DA-D05-S1**	DF-F01-S1 DF-G01-S1	**MQ-C02-S1**	-
	3.1.2 Risk informed house keeping	-	-	-	-	-		-	-	-

PSA Application	PSA Application Group/	PSA Elements								
Category	PSA Application	IE	AS	SC	SY	HR	DA	DF	MQ	Other
	3.1.3 Risk informed support for plant ageing management programme	IE-H02-S1	-	-	**SY-B19-S1** **SY-B22-S1**	-	**DA-E01-S1**	DF-F01-S1 DF-G01-S1	-	-
	3.1.4 Risk informed on-line maintenance	-	-	-	-	-	-	-	MQ-A01-S1 MQ-C02-S1	-
	3.1.5 Plant outage management	-	-	SC-A03-S1	-	HR-G02-S1 HR-G04-S1 HR-K02-S1 HR-K05-S1	-	-	-	OS-A03-S1 OS-C01-S2
	3.2 Accident mitigation and emergency planning									
	3.2.1 Development and improvement of the emergency operating procedures	-	**AS-B03-S1** **AS-C03-S1** **AS-C04-S1** **AS-C16-S1** **AS-C05-S1** **AS-C06-S1** **AS-C08-S1**	-	-	**HR-G02-S1** **HR-G04-S1**	-	DF-F01-S1 DF-G01-S1	-	-
	3.2.2 Support for NPP accident management (severe accident prevention, severe accident mitigation)	IE-B01-S1	-	-	-	**HR-G02-S1**	DA-D06-S1	DF-F01-S1 DF-G01-S1	-	OS-A01-S1 HE-D04-S1
	3.2.3 Support for NPP emergency planning	IE-B01-S1	AS-C05-S1	-	-	-	-	-	-	-
	3.3 Personnel training									

PSA Application	PSA Application Group/	PSA Elements								
Category	PSA Application	IE	AS	SC	SY	HR	DA	DF	MQ	Other
	3.3.1 Improvement of operator training programme	-	**AS-B03-S1** **AS-C03-S1** **AS-C04-S1** **AS-C16-S1** **AS-C05-S1** **AS-C06-S1** **AS-C08-S1** AS-C17-S1	-	SY-B14-S1 SY-B14-S2 SY-B19-S1 SY-B22-S1	**HR-G04-S1** HR-E02-S1	DA-D05-S1	-	MQ-A01-S1 MQ-C02-S1	-
	3.3.2 Improvement of maintenance personnel training programme	-	AS-C17-S1	-	**SY-B14-S1**	HR-D06-S1	-	-	-	-
	3.3.3 Improvement of plant management training programme	-	AS-C03-S1 AS-C04-S1 AS-C16-S1 AS-C05-S1 AS-C06-S1 AS-C08-S1 AS-C17-S1	-	-	HR-G02-S1 HR-G04-S1 HR-K02-S1 HR-K05-S1	DA-D05-S1	-	MQ-A01-S1 MQ-C02-S1	
	3.4 Risk based configuration control/ Risk Monitors									
	3.4.1 Configuration planning (e.g. support for plant maintenance and test activities)	-	-	-	**SY-B14-S1** **SY-B14-S2** **SY-B14-S3** **SY-B23-S1**	-	**DA-B01-S1** **DA-D05-S1** DA-F02-S1	DF-F01-S1 DF-G01-S1	**MQ-C02-S1**	-
	3.4.2 Real time configuration assessment and control (response to emerging conditions)	-	**AS-B03-S1** **AS-C03-S1** **AS-C04-S1** **AS-C16-S1** **AS-C05-S1** **AS-C06-S1** **AS-C08-S1** AS-C17-S1	-	**SY-B14-S1** **SY-B14-S2** **SY-B14-S3**	-	**DA-B01-S1** DA-D05-S1 DA-F02-S1	DF-F01-S1 DF-G01-S1	**MQ-C02-S1**	-

PSA Application Category	PSA Application Group/ PSA Application	PSA Elements								
		IE	AS	SC	SY	HR	DA	DF	MQ	Other
	3.4.3 Exemptions to TS and justification for continued operation	**IE-B01-S1**	-	-	**SY-B14-S1** **SY-B14-S2** **SY-B14-S3**	-	**DA-B01-S1** DA-D05-S1 DA-F02-S1	DF-F01-S1 DF-G01-S1	**MQ-C02-S1**	-
	3.4.4 Dynamic risk informed TS	-	AS-C05-S1 AS-C06-S1 AS-C16-S1	SC-B01-S1	**SY-B14-S1** **SY-B14-S2** **SY-B14-S3**	-	**DA-B01-S1** DA-D05-S1 DA-F02-S1	DF-F01-S1 DF-G01-S1	**MQ-C02-S1**	MU-B04-S1-
4. PERMANENT CHANGES TO THE OPERATING PLANT	**4.1 Plant changes**									
	4.1.1 NPP upgrades, backfitting activities and plant modifications	**IE-H02-S1** IE-B01-S1 IE-C02-S1 IE-C02-S2	**AS-B03-S1** **AS-C03-S1** **AS-C04-S1** **AS-C16-S1** AS-C05-S1 AS-C06-S1 AS-C08-S1 AS-C17-S1	**SC-B01-S1**	**SY-B23-S1** SY-B19-S1 SY-B22-S1 SY-C16-S1	HR-G01-S1	**DA-C02-S1** DA-D05-S1	DF-F01-S1 DF-G01-S1	MQ-B05-S2 MQ-D01-S1	HE-D04-S1 MU-B04-S1-
	4.1.2 Life time extension	**IE-H02-S1** IE-B01-S1	-	-	-		**DA-E01-S1**	DF-F01-S1 DF-G01-S1	-	-
	4.2 Technical specification changes									
	4.2.1 Determination and evaluation of changes to allowed outage time and changes to required TS actions	-	-	-	**SY-B14-S1** **SY-B14-S2** **SY-B14-S3** **SY-B23-S1** SY-B19-S1 SY-B22-S1 SY-C16-S1		DA-B01-S1 DA-D05-S1 DA-F02-S1	-	**MQ-C02-S1**	-

PSA Application	PSA Application Group/	PSA Elements								
Category	PSA Application	IE	AS	SC	SY	HR	DA	DF	MQ	Other
	4.2.2 Risk informed optimization of TS	-	-	-	**SY-B14-S3** **SY-B23-S1** SY-B19-S1		DA-B01-S1 DA-D05-S1 DA-F02-S1	-	**MQ-C02-S1**	-
	4.2.3 Determination and evaluation of changes to surveillance test intervals	-	-	-	**SY-B14-S3** **SY-B23-S1** SY-B19-S1 SY-B22-S1 SY-C16-S1		DA-B01-S1 DA-D05-S1 DA-F02-S1	-	**MQ-C02-S1**	MU-B04-S1
	4.2.4 Risk informed surveillance programme	IE-C02-S1 IE-C02-S2	-	-	**SY-B23-S1** SY-B14-S1 SY-B14-S2 SY-B22-S1 SY-C16-S1		DA-B01-S1 DA-D05-S1 DA-F02-S1	-	**MQ-C02-S1**	MU-B04-S1
	4.2.5 Risk informed in-service inspections (ISI)	IE-C02-S1 IE-C02-S2	-	-	**SY-C01-S1** SY-B19-S1 SY-B22-S1 SY-C16-S1 SY-B06-S1		DA-B01-S1 DA-D05-S1 DA-F02-S1	-	**MQ-C02-S1**	MU-B04-S1
	4.3 Establishment of graded QA programme for SSC									
	4.3.1 Categorization of SSC for equipment risk significance evaluation	**IE-H02-S1**	-	-	**SY-B14-S3** SY-B19-S1 SY-B22-S1 SY-C16-S1 SY-B23-S1	HR-G04-S1	-	-	**MQ-C02-S1**	MU-B04-S1
	4.3.2 Evaluation of risk impact of changes to QA requirements	**IE-H02-S1**	-	-	**SY-B14-S3** SY-B19-S1 SY-B22-S1 SY-C16-S1 SY-B23-S1	-	-	-	-	MU-B04-S1
	4.4 Risk informed special site protection measures									

PSA Application	PSA Application Group/	PSA Elements								
Category	PSA Application	IE	AS	SC	SY	HR	DA	DF	MQ	Other
	4.4.1 Risk informed fire protection	-	-	-	-	HR-E07-S1 HR-F02-S1	DA-D05-S1 DA-D06-S1	-	-	IE-F12-S1 HE-D04-S1 HE-D04-S2 HE-K09-S1
	4.4.2 Risk informed internal flood protection	-	-	-	**SY-C01-S1** SY-B06-S1	HR-F02-S1	DA-D05-S1 DA-D06-S1	-	-	-
	4.4.3 Risk informed defence in depth for individual and correlated site hazards	-	-	-	-	-	DA-D05-S1 DA-D06-S1	-	-	-
5. OVERSIGHT ACTIVITIES	**5.1 Performance monitoring**									
	5.1.1 Planning and prioritization of inspection activities (regulatory and industry)	IE-H02-S1	-	-	-	-	-	DF-F01-S1 DF-G01-S1	MQ-B05-S1 MQ-B05-S2 MQ-C02-S1 MQ-D01-S1	-
	5.1.2 Long term risk based performance indicators	IE-H02-S1	-	-	-	-	DA-B01-S1 DA-F02-S1 DA-H02-S1	DF-F01-S1 DF-G01-S1	MQ-B05-S1 MQ-B05-S2 MQ-C02-S1 MQ-D01-S1	-
	5.1.3 Short term risk based performance indicators	IE-H02-S1	-	-	-	-	DA-B01-S1 DA-F02-S1 DA-H02-S1	DF-F01-S1 DF-G01-S1	MQ-B05-S1 MQ-B05-S2 MQ-C02-S1 MQ-D01-S1	-
	5.2 Performance assessment									
	5.2.1 Assessment of inspection findings	**IE-B01-S1**	All SAs for AS	**SC-B01-S1**	SY-B19-S1 SY-B22-S1 SY-C16-S1	-	DA-B01-S1 DA-F02-S1 DA-H02-S1	DF-F01-S1 DF-G01-S1	MQ-B05-S1 MQ-B05-S2 MQ-D01-S1	-

PSA Application Category	PSA Application Group/ PSA Application	PSA Elements								
		IE	AS	SC	SY	HR	DA	DF	MQ	Other
	5.2.2 Evaluation and rating of operational events	**IE-B01-S1** **IE-C02-S1**	All SAs for AS	**SC-B01-S1**	SY-B19-S1 SY-B22-S1 SY-C16-S1	-	DA-B01-S1 DA-F02-S1 DA-H02-S1	DF-F01-S1 DF-G01-S1	MQ-B05-S1 MQ-B05-S2 MQ-D01-S1	-
6. EVALUATION OF SAFETY ISSUES	**6.1 Risk evaluation**									
	6.1.1 Risk evaluation of corrective measures	Any of the special attributes may be required on a case-by-case basis. The PSA model need to be upgraded in the manner that would allow an evaluation of the impact associated with the considered measure by the PSA model.								
	6.1.2 Risk evaluation to identify and rank safety issues	Any of the special attributes may be required on a case-by-case basis. The PSA model need to be upgraded in the manner that would allow an evaluation of the impact associated with the considered issue by the PSA model.								
	6.1.3 Assessment of the safety importance of deviations between an existing plant design and updated/revised deterministic design rules or new information about the site hazards.	-	-	SC-B01-S1	**SY-C07-S1** **SY-C15-S1** **SY-C16-S1** SY-B19-S1 SY-B22-S1 SY-C01-S1	-	DA-D06-S1	DF-F01-S1 DF-G01-S1	MQ-B05-S1 MQ-B05-S2 MQ-D01-S1	-
	6.1.4 Assessment of the significant of overall site risk for multiunit accidents	-	-	-	-	HR-F02-S1	**DA-F01-S1**	-	**MQ-B03-S1**	**OS-A01-S2** **OS-B01-S1** **OS-C01-S4** **HE-B06-S1** **AS-B01-S1**
	6.1.5 Assessment of the significant of overall site risk from all radioactive sources.	**Any of the special attributes may be required on a case-by-case basis. The PSA model need to be upgraded in the manner that would allow an evaluation of the impact associated with the considered issue by the PSA model.**								
	6.2 Regulatory decisions									

PSA Application Category	PSA Application Group/ PSA Application	PSA Elements								
		IE	AS	SC	SY	HR	DA	DF	MQ	Other
	6.2.1 Long term regulatory decisions	**Any of the special attributes may be required on a case-by-case basis. The PSA model need to be upgraded in the manner that would allow an evaluation of the impact associated with the considered measure by the PSA model.**								
	6.2.2 Interim regulatory decisions	**Any of the special attributes may be required on a case-by-case basis. The PSA model need to be upgraded in the manner that would allow an evaluation of the impact associated with the considered issue by the PSA model.**								

17. CONCLUSIONS

The matter of PSA technical quality is very important from the viewpoint of risk informed decision making on various aspects of NPP operation and licensing. This publication provides an approach for achieving the technical consistency of PSA in order to reliably support various PSA applications. The approach involves the consideration of a set of technical features, called attributes, of the major PSA elements relevant for various applications.

A comprehensive list of PSA applications has been compiled. The applications were grouped into the six categories. Some of the categories include several groups. For each PSA application, a brief description of the purpose of the application and the way the PSA can be used to support it were provided along with the information on what PSA results and metrics can be used in the decision making process.

The publication covers a full scope Level 1 PSA. Eleven PSA elements characterizing the major PSA tasks were defined. For each PSA element, a set of general attributes needed for all PSA applications and special attributes needed for specific PSA applications were elaborated. In addition attributes for maintenance and upgrade of the PSA are provided in the publication. In relation to each PSA application, the special attributes were further distinguished as essential and supplemental. An essential special attribute emphasizes a feature of the PSA element that is considered important to generate the results needed to reliably support the PSA application. A supplemental special attribute may not be strongly required for a specific application, but could further enhance the usefulness of the PSA by providing a greater level of detail, or improving confidence in the results. The publication provides a mapping of the special attributes to the considered PSA applications with a brief explanation on why a special attribute is needed in each particular case.

The publication can be used by PSA practitioners for appropriate planning of PSA projects taking into account possible uses of the PSA in the future. The publication can also be used by reviewers as an aid in assessing the quality of PSAs and judging the adequacy of a PSA for specific applications. Particularly, the publication can be used by regulatory authorities to support regulatory reviews of licensees’ PSA and PSA application cases along with other IAEA publications, e.g. [48 - 49].

APPENDIX I: RISK METRIC DEFINITIONS

Risk metric

The risk metric defines what constitutes a “risk” in the definition of a probabilistic safety goal.

Importance measures

- *Risk Achievement Worth (RAW)*

  This is the ratio or interval of the figure of merit, evaluated with the SSC’s basic event probability set to one, to the base case figure of merit. This importance measure reflects the increase in a selected figure of merit when an SSC is assumed to be unable to perform its function due to testing, maintenance, or failure.

- *Fussell-Vesely (F-V)*

  For a specific basic event, the F-V importance is the fractional contribution to the total of a selected figure of merit for all accident sequences containing the basic event to be evaluated.

Core/fuel damage frequency, annual average (CDF_{AVE}, FDF_{AVE})

This is the frequency of core/fuel damage quantified in a single reactor PSA that is averaged over the time dependent variations that may be exhibited during the course of a year due to plant configuration changes, removing equipment from service to perform tests or maintenance, and the occurrence of plant initiating events which may in fact vary over the course of a reactor lifetime. Periodic updates of this risk metric over the course of the plant lifetime provide a slow version of a time dependent Risk Monitor that reflects broad trends in plant and SSC performance that are reflected in the plant data as well as any permanent changes that are made in the design, maintenance and operation. CDF_{AVE} is normally expressed on a per reactor-calendar-year basis.

Multiunit core/fuel damage frequency, annual average ($MCDF_{AVE}$, $MFDF_{AVE}$)

This is the frequency of an accident involving core/fuel damage on two or more reactor units quantified in a multiunit PSA that is averaged over the time dependent variations that may be exhibited from combinations of reactor unit configurations. $SCDF_{AVE}$ is normally expressed on a per site calendar year basis.

Site core/fuel damage frequency, annual average ($SCDF_{AVE}$, $SCDF_{AVE}$)

This is the frequency of core/fuel damage on one or more reactor units quantified in a multiunit PSA that is averaged over the time dependent variations that may be exhibited from combinations of reactor unit configurations. $SCDF_{AVE}$ is normally expressed on a per site calendar year basis.

Change in core/fuel damage frequency, annual average (ΔCDF$_{AVE}$, ΔFDF$_{AVE}$)

This is the change in the annual average CDF/FDF due some change that is being evaluated that may impact this risk metric. The change may be due to an observed degradation, design change, procedure change, change in test, maintenance or inspection practice, change in performance of an SSC, or changes to any input or assumption associated with the PSA model.

Core/fuel damage frequency, time dependent (CDF(t), FDF(t))

This is the frequency of core/fuel damage as a function of time. It is often referred to as the 'instantaneous core/fuel damage frequency.' Only some of the parameters that the *CDF/FDF* is dependent on can be monitored in a time dependent fashion, such as the time periods when equipment is removed from service.

Core damage probability (CDP)

This is the total probability of a core/fuel damage event over a specified time interval.

Conditional core/fuel damage probability (CCDP, CFDP)

This is the conditional core/fuel damage probability given the occurrence of an initiating event. It is calculated by selecting the appropriate PSA initiating event, setting the initiating event frequency to 1, and solving the PSA model for core/fuel damage for the condition that the initiating event has occurred.

Incremental conditional core/fuel damage probability (ICCDP/ICFDP)

This is the increase in the *CDP/FDP*, over that expected from the Base *CDF/FDF* during a configuration change (denoted by the index *j*) within the time *Tj* with an increased CDF_j , FDF_j relative to CDF_{BASE}, FDF_{BASE}. It is referred to as a conditional probability because it is conditioned on being in a specific plant configuration.

Fuel damage frequency (FDF)

This is the frequency of fuel damage as a function of time. Fuel damage is related to any other fuel on a reactor site, e.g. in the spent fuel pool, but not in the reactor core.

Fuel damage probability (FDP)

This is the total probability of a fuel damage event over a specified time interval.

Large early release frequency, annual average (LERF$_{AVE}$)

This is the frequency of a large early release that is averaged over the time dependent variations that may be exhibited during the course of a year, which may in fact vary over the course of a reactor lifetime.

Change in large early release frequency, annual average (ΔLERF$_{AVE}$)

This is the change in the annual average LERF due some change that is being evaluated that may impact this risk metric.

The change may be due to an observed degradation, design change, procedure change, change in test, maintenance or inspection practice, change in performance of an SSC, or changes to any input or assumption associated with the PSA model. LERF_{AVE} is normally expressed on a per reactor-calendar-year basis.

Site large early release frequency, annual average ($\textbf{LERF}_{\textbf{AVE}}$)

This is the frequency of a large early release due to an accident involving releases from one or more reactor units that is averaged over the time dependent variations that may be exhibited during the course of a year, which may in fact vary over the course of a reactor lifetime.

Large early release frequency, time dependent (LERF(t))

This is the frequency of a large early release as a function of time. It is often referred to as the 'instantaneous large early release frequency.' Only some of the parameters that the *LERF* is dependent on can be monitored in a time dependent fashion, such as the time periods when equipment is removed from service.

Large early release probability (LERP)

This is the total probability of a large early release over a specified time interval.

Conditional large early release probability (CLERP)

This is the conditional large early release probability given the occurrence of an initiating event. It is calculated by selecting the appropriate PSA initiating event, setting the initiating event frequency to 1, and solving the PSA model for large early release under the condition that the initiating event has occurred.

Incremental conditional large early release probability (ICLERP)

This is the increase in the *LERP*, over that expected from the Base *LERF* during a configuration change (denoted by the index *j*) within the time *Tj* with an increased $LERF_j$ relative to $LERF_{BASE}$. It is referred to as a conditional probability because it is conditioned on being in a specific plant configuration.

Release category frequency, annual average ($\textbf{RCF}_{\textbf{AVE}}$)

This is the frequency of all the accident sequences binned to a given release category that is quantified in a single reactor Level 2 PSA.

Site release category frequency, annual average ($\textbf{SRCF}_{\textbf{AVE}}$)

This is the frequency of all the accident sequences binned to a given Release Category that is quantified in a multiunit Level 2 PSA. The full set of release categories are sufficient to account for the possible end states of a multiunit Level 2 PSA that range from minimal releases from all units, to significant releases from all reactor units on the site.

Complementary cumulative distribution function, annual average ($\textbf{CCDF}_{\textbf{AVE}}$)

This is the annual frequency of exceedance of consequences quantified in a single reactor Level 3 PSA for different consequence metrics such as early fatalities, latent cancer fatalities, property damage costs, etc. CCDFs are aggregated to account for all the release categories and associated single unit accident sequences modelled in a single unit Level 3 PSA.

Site complementary cumulative distribution function, annual average (SCCDF$_{\mathrm{AVE}}$)

This is the annual frequency of exceedance of consequences quantified in a multireactor unit Level 3 PSA for different consequence metrics such as early fatalities, latent cancer fatalities, property damage costs, etc. CCDFs are aggregated to account for all the release categories and associated single unit and multiunit accident sequences modelled in a multiunit Level 3 PSA.

Quantitative health objectives (QHO)

QHOs are derived from qualitative safety goals and provide a numerical measure of acceptable levels of risk of acute and latent health effects due to accidents. These are normally expressed in terms of a small fraction, e.g. .01% of the expected annual risks of death to individuals in designated areas around the plant due to other causes. Accidental risks of death due to radiation sickness are normally compared against non-nuclear accident risks to an average individual within short distances of the plant (e.g. 1 mile), whereas risks due to latent health effects from a reactor accident are normally measured against the risk of latent cancer fatalities due to non-nuclear causes to the population over larger distances from the plant (e.g. 10 miles). Individual risks from NPP accidents are computed by summing the products of the accident frequencies and total estimate of consequences in the appropriate population segment and then normalizing this population risk metric by the population in that segment.

APPENDIX II: PSA APPLICATIONS

TABLE A-II DESCRIPTION OF PSA APPLICATIONS

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
1. SAFETY ASSESSMENT		
1.1 Assessment of the overall plant safety The assessment of the overall plant safety represents the main purpose of PSA performance and includes identification and ranking of important design and operational features, of dominant accident sequences, systems, components, human interactions and dependencies important for safety. A comparison of the results against safety goals or quantitative health objectives may be involved.	CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk	A complete safety evaluation would in principle require a full scope PSA (Level 1 through 3) covering all operating and shutdown modes and both internal and external plant hazards. A partial but meaningful evaluation can be performed using a limited scope PSA with qualitative evaluation of the missing scope supported by bounding assessments. Risk contributors and importance information are used to develop risk insights.
1.2 Periodic safety review Similar to Item 1.1, PSA provides useful insights to support a periodic safety review. A safety assessment process consists in identifying safety issues, determining their safety significance and making decisions on the need for corrective measures. A major benefit of including PSA in periodic reviews is the creation of an up to date overview of the whole plant. PSA may help in identification of real cost-effective improvements to safety. The application may involve modelling of aging effects in PSA. Typically there are two types of	ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk	In addition to the discussion above in Item 1.1, the important issues in this application are the use of plant specific data, modelling of as-built-as-operated plant conditions, and addressing the possible impact of aging phenomena and component lifetime considerations on the overall risk metrics. Sensitivity calculations may be required to assess the potential effect of ageing on passive components, which are not normally maintained or replaced. For the cost benefit evaluation of severe accident management alternatives the PSA needs to be updated to reflect design and procedure changes associated with each alternative (Level 2 and -3 PSA. The changes in risk metrics are used to evaluate the level of risk reduction associated with each alternative (see also Item 3.2.2). For example, while licensing an NPP for continuation of its operation beyond the design lifetime, a full scope PSA is performed to ensure that it meets the country's

[17] Definitions of risk metrics are provided in Appendix I.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
SSCs: (1) SSCs which are periodically renewed or replaced (can be modelled 'as new'), and (2) SSCs which are subject to an aging process. Currently, modelling of SSC aging in terms of PSA is in an exploratory stage. Thus, PSA treatment of aging effects is not standardly carried out and is considered beyond the current state of the art. In some counties, PSA is required for lifetime extension and to support a cost benefit evaluation of possible backfits to reduce the risk of severe accidents. Aging effects, however, are typically addressed qualitatively.		QHOs or safety goals. In addition, the problems associated with aging may be investigated and accounted for. In some countries, it is required to compare the state and design of an operating plant against actual deterministic regulations. The safety importance of deviations can be judged by the help of a plant specific PSA. The need of backfit measures is derived from the outcome of this assessment. See also Item 6.3.
1.3 Analysis of the degree of defence in depth and safety margin against beyond design basis site hazards, including correlated site hazards The beyond design external hazards has the potential to cause multiple SSCs damage and break several barriers of defence-in-depth. The deterministic assessment of external hazards is typically limited to only selected hazards applicable to the site with the intensity occurring with relatively high frequency (e.g. once in 10 000 years). The defence against hazards of higher intensity is believed to be achieved by embedding safety margins in the design and construction of SSCs. The application is focused on the assessment of the safety margins and Defence in depth (DID) embedded in the design and construction of SSCs	ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CDF/FDF$_{AVE}$, CCDP, LERF$_{AVE}$, QHOs, Risk importance measures of all SSCs and HEs, primary contributors to risk, Qualitative analysis of MCSs with the purpose of identification of critical combinations of faults caused by the hazards.	The external hazards PSA has the objective to assess either qualitatively or quantitatively all external hazards that might challenge the safety of the plant. This assessment is not limited to specific intensities of the hazards but accounts for all credible combinations of the hazards. However, some additional analysis is required to use the results for analysing the DID for each hazard (e.g. estimation of the CCDPs for the specific range of intensities of selected hazards or for specific set of correlated hazards). There are several methods used to evaluate the robustness of NPPs against external hazards that utilize information obtained from PSA. In particular Fault Sequence Analysis (FSA) method currently being developing by the IAEA could be used [50]. In this method the MCSs obtained from Level 1 internal events PSA model are reviewed to verify whether one or several MCSs exist in which all components represented by basic events fail given the hazard or set of hazards of certain intensity. Another approach for advanced plants is the review of the Safety Functional Capability for each hazard to ensure all hazard events (above a specified frequency) can be mitigated using two available safety functions (N+2 designs). Initially, this involves the review of CCDP/CFDP (or CLERP) results to ensure there are two systems credited for each

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
and evaluation of residual risk associated with the hazards not considered in the design, including correlated hazards and hazards of higher intensity and low frequency. This application is focused on a single unit. Multiple Unit assessments are discussed under 6.1.4.		analysed hazard initiating event. However, for spatial events, additional analysis would be performed to ensure that at least one train is available given a credited barrier (for fire or flooding) or other feature fails.
2. DESIGN EVALUATION		
2.1 Application of PSA to support decisions made during the NPP design (plant under design) The aim of this application is to optimize the design of a new plant in terms of risk metrics and cost. The application focuses on identification of design weaknesses and effective areas for improvement in view of plant risk. The improvements considered can include the provision of additional or diverse protective systems and features for mitigating the consequences of a severe accident. This could involve incorporating some additional protective systems and features into a new design. Assessment may include investigation of variants and exploratory design options, sufficiency in systems' redundancy and diversity, effectiveness in emergency and accident management measures, as well as development of reliability and availability targets for SSCs to meet safety goals, if set.	CDF/FDF$_{\text{AVE}}$, LERF$_{\text{AVE}}$, CDP, LERP, QHOs, ΔCDF/FDF$_{\text{AVE}}$, ΔLERF$_{\text{AVE}}$, Risk importance measures of affected SSCs and HEs (e.g. F-V, RAW), PSA insights	Use of PSA model is similar to Item 1.1 except for that additional assumptions are needed in lieu of lack of design and operational details; uncertainties in risk estimates are correspondingly larger than for as-built plant. PSA results can be used to allocate reliability targets for SSCs thereby forming part of the design specification. For design change evaluations, the level of detail of the PSA model in the areas affected by the design changes may be greater than that for the rest of the plant. For example, the PSA can be used as a supporting tool to select or modify the design basis accidents, to decide the classification of safety related SSCs, to define general design criteria, to develop SSC reliability and availability targets, to support the and severe accident list for severe accident management. In addition, PSA can provide an input to cost-benefit analysis. There are several features of the PSA that require more detailed modelling to be able to support the application: • more detailed grouping of the initiating events that can help to identify and eliminate deficiencies in the systems design • explicit consideration of initiating events caused by operator errors that can help to get additional insights regarding deficiencies in the control room design, plant procedures, and operator training. • consideration of intersystem common cause failures and a more detailed modelling of common cause failures for realistic estimation of the plant risk for effectiveness of reactor protection system design from the risk perspective.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
		• detailed modelling of ATWS sequences to provide support for the evaluation of the effectiveness of reactor protection system design from the risk perspective. Particular effort need to be made to identify unique initiating events, failure modes, event sequences and dependencies that may be introduced by new design features. Detailed dependency matrices need to be developed to identify and document all physical and functional dependencies among support systems and front-line systems. All normally operating systems need to be examined to identify possible initiating events that may be caused by loss of the entire system, of a single system train, or of combinations of trains. Event sequence diagrams may be used to develop the accident sequences and identify challenges to relief and safety systems in the period immediately following the initiating fault.
2.2 Licensing of design The application is similar to Item 2.1. The assessment of the overall plant safety is necessary for applying for operational licence and usually requires a full scope Level 1 and Level 2 PSAs. A comparison of the results against safety goals or quantitative health objectives is performed within this application. A safety evaluation for applying a pre-construction licence may involve a limited scope of the PSA. Part of this application is includes providing input to public relation activity in the pre-licensing process aimed to obtain public acceptance for the NPP construction and operation.	ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk	There are no major differences in the use of PSA to support the application comparing to Item 2.1. However, licensing of the design would likely involve an all modes, full scope PSA where the risk results are compared with the QHOs or safety goals for new plants. Additionally, an independent review (e.g. peer review) against the PSA requirements of this TECDOC or similar is likely required.
2.3 Optimization of protection against hazard events (e.g. fires, floods) and common cause failures, including consideration of correlated site hazards and hazard-induced fires and	ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, risk importance measures of all SSCs and	The use of PSA at the design phase for optimization of protection against hazard events as supported by PSA has the following goals: • To establish requirements for the fragilities of the SSCs, including containment

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
floods An early design optimization in relation to hazards events is a necessary requirement to achieve safe and economically prudent nuclear power plant. Carrying out the PSA internal and external hazards PSA from the very beginning of the design development can give the benefit of modifying plant design easily to mitigate impact of the hazard on the NPP. A thorough analysis can provide a cost-effective approach to hazard protection optimization at the design stage. Such a benefit is impossible when performing an assessment for operating plants.	HEs, primary contributors to risk	(based on the results of seismic PSA and aircraft crash) • To define requirements for equipment separation, cable tracing, and plant layout (based on the results of fire/flood PSA) – Separation of systems trains/cables – Location of flood or fire rated barriers and doors – Location of high impact sources, such as large pipes or large fire sources • Location and Elevation of the rooms housing the important equipment (based on flood PSA) • To define requirements for internal hazards protective features (based on Fire/flood PSA) – Drainage system – Fire detection/mitigation – Flood detection – Flood isolation – Isolation of the compartments, etc. • To identify and reduce maintenance activities that can lead to fire/floods events In summary, design features and provision, including human interactions and associated procedures, that are assumed and credited in the PSA and contribute to achievement of acceptably low risk are implemented in the constructed plant. It is important to note that at the design stage there are numerous uncertainties related to the aspects important for internal and external hazards PSA development (e.g. detailed cable tracing, fire and flood barriers, anchorage of the SSCs, location and orientation of the components, etc.). Also lack of operating and emergency procedures introduces additional uncertainties. These uncertainties need to be always taken into account.
2.4 Establishment of equipment reliability targets for manufactories	Risk importance measures and estimated failure rates of all SSCs in the base PSA, and a contribution of each SSC to the plant availability	Reliability Targets for SSCs are established considering one or more of the following: 1) Risk: Contribution to the plant risk, such as core/fuel damage, release, or potential dose to workers or the public. 2) Availability: Contribution to the plant availability or power generation (e.g. impact resulting in reduced power the plant, but the plant remaining available)

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
	and power generation.	3) Cost: In addition to the above costs, the replacement cost may be considered, especially for SSCs requiring significant investment. 4) Other Factors: These may include components not directly impacting the above items, but are important for other reasons such as personnel safety, environmental protection, plant security, or other factors. The two items above where the PSA can be used to support the establishment of reliability targets include items 1 and 2. The risk input is generally focused on ensuring the reliability of SSCs maintains the PSA results at or below the estimated CDF/FDF or release frequencies. Typically this means that the PSA reliability estimates, which are based on historical data for similar components, are the starting point for the manufacturing reliability goals. However, the SSC importance in the PSA is also considered in some cases, where the reliability goal may be established lower from high or medium important SSCs, and may be relaxed (in limited cases) for low importance SSCs. To support this analysis, the PSA may need to be improved to ensure that the SSC modelling in the PSA is comprehensive, including the removal of simplifications and grouping, where possible. PSA models can also be used to analyse the overall plant availability through development of a generation risk assessment (GRA). The GRA includes modelling of all major causes of a plant shutdown combined with the expected down time for the plant as a result of the failure. The PSA model is used for some of the expected failure rate estimates (PSA models typically do not include most of the balance of plant modelling impacting availability), and some of the mean time to repair estimates. The SSC reliability goals are then established to ensure an overall plant availability is below the availability goal (e.g. 90% availability).
2.5 Identification of R&D which are necessary to support the design	ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CDF/FDF$_{AVE}$, LERF$_{AVE}$,	The common examples for advanced plants include the use of passive reliability SSCs, digital I&C, and use of software for controls and actuation. For passive components,

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
Research and Development for plants in the design phase, may include new components, systems or uses of components not included in previous plants in operation (or with limited use). R&D discussed here relates to SSC related R&D, rather than R&D on PSA techniques.	QHOs, risk importance measures of all SSCs, Assumptions and Uncertainties affecting the PSA.	such as passive containment cooling, or for components such as explosive valves, the industry experience is limited. In other cases, new uses of components may be planned, such as changing the MSIV from one valve type to another. Research and Development (R&D) for the above would be important, especially for components that are significant contributors to the plant risk. Given the high uncertainty for some of these SSCs, the overall contribution may require additional uncertainty or sensitivity analysis to account for variation in both reliability and efficiency. For example, for passive containment cooling, the reliability is not expected to be as big a concern as either the efficiency or the impact due to non-condensable gases generated during an accident condition. R&D efforts can be focused on those areas that potentially impact the risk results, accounting for the uncertainty.
2.6 Development operator procedures and training programmes and support for human factors engineering PSA is used to enhance the training, procedures, and HFE (human machine interface) for operator responses associated with high or medium importance HEPs.	CDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CDF/FDF$_{AVE}$, LERF$_{AVE}$, risk importance measures of all HEPs, Assumptions and Uncertainties affecting the PSA.	The PSA importance measures include a list of HEPs that can be used as an input to programmes involving operator training, procedures development or review of HFEs. In all cases, the PSA importance measures are used to ensure the training, procedures, and HFE review are comprehensive for operator responses associated with high or medium importance HEPs. PSA enhancements may be important to support the above, especially in the PSA modelling of operator responses. In some cases, conservatism need to be removed such as the performance of detailed HRA for both risk significant and non-risk significant HEPs (not needed for all HEPs, but at least for those with higher importance measures). More importantly, would be the modelling of operator responses which may not be included in the base PSA model due to assumptions and simplifications.
3. NPP OPERATION		
3.1 NPP maintenance		
3.1.1 Maintenance programme optimization The application includes assessment, optimization and establishment of maintenance plans and	Risk importance measures of affected SSCs (e.g. F-V, RAW), ΔCDF/FDF$_{AVE}$,	Risk importance measures from the base PSA are used to help prioritize candidate maintenance changes: changes in CDF/FDF and LERF are used to justify acceptable risk impacts and to determine risk significance. Explicit model of maintenance

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
procedures in view of plant risk. Maintenance activities are assessed to assure that risk significant systems and equipment are being adequately maintained to support required reliability, and that maintenance activities do not reduce plant safety and increase risk by, for example, extensive maintenance resulting in increased equipment unavailability. Focus is on equipment with greatest impacts on plant risk. Opportunities for reduced or eliminated maintenance tasks are defined and evaluated for SSCs that have low risk significance and for maintenance that does not support critical functions of the SSCs.	$\Delta LERF_{AVE}$	unavailabilities and capability to predict or bound the impact of programme changes on failure rates and maintenance unavailabilities are needed to support the application. The level of detail of the PSA model in the areas affected by the programme changes may be greater than that for the rest of the plant. For example, the application of PSA can serve (a) to identify equipment requiring upgraded preventive maintenance (as an increase in its reliability results in a substantial gain in safety), (b) to identify equipment requiring sustained, slightly reduced preventive maintenance (as a decrease in its reliability does not affect the level of safety), (c) to identify equipment requiring only corrective maintenance (as its unavailability does not result in a major increase in risk), (d) to eliminate maintenance on certain failure modes that are not relevant to the risk significant safety function, (e) to assess the impact of shifting maintenance activities from the plant outage to the operation mode (would require a shutdown PSA).
3.1.2 Risk informed house keeping This application is intended to assure low risk contributions from external hazards (e.g. seismic) and internal hazards (e.g. fire, floods) by directing housekeeping activities to risk important areas.	Risk importance measures of affected SSCs (e.g. F-V, RAW), $\Delta CDF/FDF_{AVE}$, $\Delta LERF_{AVE}$	The results of an external and internal hazard PSA are used to assess the relative risk contributions of rooms and areas and identify improvement measures. For example, the results of an internal fire PSA may be taken into account for adjusting transient combustible control and storage for significant fire areas.
3.1.3 Risk informed support for plant ageing management programme The aim of this application is to optimize the scope of the plant specific ageing programme for safety related equipment. It includes identification of safety significant components and may involve modelling of aging effects in PSA and identification of the risk significant SSCs potentially degrading due to aging phenomena.	Risk importance measures of all SSCs (e.g. F-V, RAW), $\Delta CDF/FDF_{AVE}$, $\Delta LERF_{AVE}$	The key issue in this application is the possible impact of aging phenomena and component lifetime considerations on the overall risk metrics. Depending on the components being evaluated Levels 1 through 2 full scope PSA may be needed.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
3.1.4 Risk informed on-line maintenance This application uses the Full Power PSA to calculate the risk during each planned or actual plant configuration. Risk Management actions are taken for configurations with higher estimated risk, including compensatory measures, schedule changes, and higher visibility of key maintenance activities.	CDF/FDF_{AVE}, $LERF_{AVE}$, risk, $\Delta CDF/FDF_{AVE}$, $\Delta LERF_{AVE}$	The use of the PSA for on-line maintenance is a common practice through the use of Risk Monitors [51]. The PSA model is included in the risk monitor, based on the hazards and scope of the PSA. The PSA model is then modified by the Risk Monitor software based on the plant configuration, maintenance occurring at the plant, and other factors affecting risk such as weather conditions, water temperature used for cooling water (may affect the number of pumps needed for cooling), etc. Enhancements to the PSA in supporting risk monitors or other on-line maintenance support are numerous: The PSA is modified to include all system alignments that may change at power. The base PSA may include an assumed alignment, or a probability of each possible alignment. CCF modelling may need to be modified, based on the change in alignments. Additional detailed modelling may need to be performed for accident sequences or hazards that are initially non-risk significant, but greatly affect the results when the configuration changes. For example, numerous plants have tried to use their base Fire PSA in an on-line risk monitor. However, when specific components are taken out of service, the resulting risk estimates are dominated by fire scenarios that are included in the base model conservatively. Care need to be taken to include a hazard specific PSA model where a large percentage of scenarios are analysed conservatively. Once the model enhancements are performed, the PSA can be used to predict the risk for any configuration, including maintenance condition, that the plant is placed. This allows the plant staff the risk information that allows them to perform actions to reduce overall risk.
3.1.5 Plant outage management Outage Management can involve use of the PSA in planning or during monitoring of actual outage configurations. Outage management may be more	CDF/FDFAVE, $LERF_{AVE}$, risk, $\Delta CDF/FDF_{AVE}$, $\Delta LERF_{AVE}$	Application of the shutdown PSA to management plant outages is a similar process to on-line maintenance. The PSA model enhancements are similar, including consideration for alignments, CCF and model detail. Similar issues may result from conservative modelling of hazard specific accident sequences, such as Fire PSA

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
complex due to higher number of maintenance activities over a shorter period of time, and the changing plant conditions including changes in POSs. Similar to online maintenance, configurations with higher estimated risk may result in risk management actions being implemented.		specific scenarios. Additionally, the base shutdown PSA may need to be expanded to include analysis of POSs that were initially screened or not modelled in detail. Once the model enhancements are performed, the PSA can be used to predict the risk for any shutdown configuration for each POS, including maintenance conditions or alignments, that the plant is placed. This allows the plant staff the risk information that allows them to perform actions to reduce overall outage risk.
3.2 Accident mitigation and emergency planning		
3.2.1 Development and improvement of the emergency operating procedures The systematic assessment of plant vulnerabilities and the insights derived from the PSA process are used to establish or improve the EOPs by providing assurance that a broad scope of vulnerabilities is addressed in a realistic, appropriately detailed and consistent manner. The integral view of the accident progressions provides information on the benefits and drawbacks of various operations in abnormal plant states. Typically, accident sequence analysis in PSA is carried out using existing EOPs and assessment of associated human interactions. This in turn provides detailed information for reconsidering EOPs and eventual improvements in the light of PSA insights. PSA can also provide the basis for specifying the decision points for when the transition into the SAMG phase should occur.	Risk importance measures of affected actions (e.g. F-V, RAW) and associated ASs, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	Importance measures from base PSA used to help prioritize candidate procedural changes, change in CDF/FDF and LERF used to justify acceptable risk impacts and to determine risk significance. The level of detail of the PSA model in the areas affected by the procedure changes including the accident sequences invoking the affected EOPs may be greater than that for the rest of the plant; a more simplified conservative treatment of other parts of the model and accident sequences acceptable. The PSA must explicitly represent operator actions that refer to specific EOPs, and the HRA method used in the PSA must be capable of predicting the impact of the procedure changes to support this application. Examples include development and modifications of event based and symptom based procedures, developing procedures for dominant accident sequences, etc.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
3.2.2 Support for NPP accident management (severe accident prevention, severe accident mitigation) Severe accident prevention is based partly on PSA. Existing, alternative or additional systems, equipment and measures are evaluated and implemented in the accident management procedures with the purpose of restoring the function of safety related systems and for preventing degradation of events into severe accidents. Severe accident mitigation includes PSA based identification and categorization of accident sequences together with descriptions of plant responses and vulnerabilities. PSA helps to understand accident progression, identification of success paths and associated strategies, prioritising safety features to reduce risks. The integral view of plant response utilized in PSA methodology is helpful in discerning the potential for negative effects of certain measures.	Risk importance measures of affected actions (e.g. F-V, RAW) and associated ASs, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	Importance measures from 'base case PSA' are used to help prioritize candidate accident management procedure changes; changes in CDF/FDF and LERF are used to justify acceptable risk impacts and to determine risk significance. The level of detail of the PSA model in the areas affected by the changes including the accident sequences invoking the affected EOPs, AMPs, and affected SSCs may be greater than that for the rest of the plant; a more simplified conservative treatment of other parts of the model and accident sequences is acceptable. In the case of operator actions to implement accident management, the PSA must explicitly represent operator actions that refer to specific EOPs and AMPs, and the HRA method used in the PSA must be capable of predicting the impact of the procedure changes to support this application. A Level 1 PSA treatment of operator actions can support accident management procedure enhancement for those actions aimed at preventing severe core/fuel damage, while a limited to full scope Level 2 PSA is required to address severe accident mitigation strategies. The severe accident consequence codes must be able to simulate the implementation of the actions and measure the impact of changes to be evaluated. In the case of new hardware or design features (e.g. interlocks, new signals, etc.) to implement accident management refer to Item 2.1. Examples: 1) Severe accident prevention: A typical example is the use of fire water for cooling safety related equipment if essential service water is lost. 2) Severe accident mitigation: A typical example for PWR reactors consists in re-filling of steam generators with water during a steam generator tube rupture initiated severe accident in order to enhance retention of radioactive materials.
3.2.3 Support for NPP emergency planning Based on PSA, important elements of emergency planning are explored and appropriate strategies are developed. The issues to be explored are: the characteristics of the plant, the plant site and the	QHOs, Early and latent risk and dose for different emergency planning responses	This application requires a full scope Level 3 PSA covering all modes and all internal and external plant hazards and the capability to predict the risk impacts of any changes to the emergency plan that are to be evaluated including alternative evacuation, sheltering, and food impoundment strategies.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
different possible countermeasures (such as sheltering, evacuation, iodine prophylaxis, long term relocation, land decontamination, food bans). This requires a Level 3 PSA. Specific applications include possible adjustments to the emergency planning zones (EPZ), refinement of emergency action levels, and focusing the resources for evacuation and sheltering.		An example is to support the determination of EPZ distance, emergency action levels, and planning and training for evacuation and sheltering activities.
3.3. Personnel training		
3.3.1 Improvement of operator training programme PSA is used to improve operator training programme by providing information on the accident processes, the relative likelihood of the dominant accident sequences, and the associated operator actions required to prevent or mitigate core/fuel damage. Similarly, the relative consequences of various operator errors and the PSA-predicted chance of failure can be used to select those actions that would benefit from emphasized training. Introduction of SAMGs necessitates having operators understand severe accident scenarios.	Description of dominant ASs for CDF/FDF$_{AVE}$ and LERF$_{AVE}$ in which HEs play a significant role, risk importance measures (e.g. F-V and RAW) of HEs and associated SSCs, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	Description of dominant accident sequences and operator actions to implement EOPs, recovery actions, and SAMGs (requires Level 2 PSA) with high risk importance are sufficient to enhance training. If advanced training is to be evaluated as a change to the risk profile, the HRA treatment must be capable of measuring the affected changes, and change in risk metrics use to evaluate the significance and acceptability of the proposed change. An example is to select dominant accident sequences from the PSA and include some of these in the operator simulator training.
3.3.2 Improvement of maintenance personnel training programme Training of maintenance staff is enhanced based on insights and information from the PSA. Focus is on potential risk significant impacts of	Risk importance measures (e.g. F-V, RAW) of affected SSCs, pre-accident HEs, and basic events dealing with maintenance and CCFs,	The risk importance measures are used to rank component maintenance unavailabilities and pre-accident human errors and associated component failures that could be influenced by maintenance programme changes; change in risk metrics used to evaluate the significance and acceptability of the proposed change to training. An example is to train the maintenance personnel on the SSCs in the scope of the

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
maintenance activities, such as common cause failure and maintenance-induced failure of multiple system trains. This results in an increased focus on risk significant SSCs and on risk significant functions and failure modes that must be addressed in the maintenance programme as well as opportunities to optimize maintenance tasks that are not significant to risk management.	$\Delta CDF/FDF_{AVE}$, $\Delta LERF_{AVE}$	maintenance programme that are most and least risk significant and which SSC failure modes should get the most priority. Another example is to use PSA insights to help manage the maintenance backlog.
3.3.3 Improvement of plant management training programme The application includes adequate communication of the techniques, applications and implications of PSA to plant management to develop an integral understanding in terms of management responsibilities. Furthermore, plant management is ultimately responsible for decisions taken within the framework of SAMGs. This requires a good understanding of important severe accident scenarios, their frequencies and consequences, as well as the relationship between plant design and operational features that impact the PSA results.	CDF/FDF_{AVE}, $LERF_{AVE}$, QHOs, risk importance measures of all modelled events, description of dominant AS, risk insights	The PSA results and a detailed qualitative summary of the results and associated risk insights and risk importance of all modelled SSCs and events are needed in this application to add risk informed insights to the safety culture. In addition, the plant management's active participation in all risk informed application would build an awareness of how to manage the risks. How well the PSA model reflects the as-built and as-operated plant necessary for the management to have confidence in the PSA results, is one of the most important attributes for this application. This must be accompanied by a basic course in PSA concepts and methods so that the results can be interpreted properly. A striking example is to improve the safety culture and to engage the plant managers in consideration and managing the risk of accidents.
3.4. Risk based configuration control/ Risk Monitors		
3.4.1 Configuration planning (e.g. support for plant maintenance and test activities) Note: Different combinations of equipment configuration, tests and maintenance activities will result in different levels of risk. The main benefit of risk informed configuration control is	CDF/FDF(t), LERF(t), ICCDP, ICLERP, risk importance measures of SSCs as a function of time	The PSA model used for the 'base case PSA' must be modified to have the possibility to eliminate time averaged maintenance unavailabilities and average models for alternative configurations, and replace them with binary ('On', 'Off') type models that make the CDF/FDF and LERF results dependent on specific POS and equipment out-of-service conditions to be evaluated. Modelling simplification to treat symmetric trains with shared basic events must be expanded to model each train explicitly. Truncation

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
the reduction of risk peaks and the control of the cumulative, or average, risk. It helps to ensure that, as far as possible, the plant does not enter critical, high-risk situations, the periods of increased risk are minimized, and that other risk significant configurations are avoided. There are two main tasks in the risk based configuration control: Task (1) - risk planning and Task (2) - risk assessment and follow-up (see Item 3.4.2 on the latter). This application is dealing with Task (1). Risk planning is a forward-looking application of PSA and it consists of supporting the preparation, planning and scheduling of plant activities and component configurations. This application can be performed with an on-line or off-line PSA model.		issues must be resolved so the PSA results are valued with any combination of equipment to be evaluated assumed to be out of service. A means of specifying plant state changes, as a function of time into the Risk Monitor must be provided. The risk importance measures in this application are used to develop 'return to service' priorities and 'remain in service' priorities for each SSC. Interface with scheduling software is helpful. The PSA model needs to be capable of predicting the temporal changes in initiating event frequencies, component unavailabilities due maintenance and other configuration changes on CDF/FDF and LERF. In case the application is aimed to assess the risk associated with transitions between different power modes, the PSA model should incorporate the IEs and system configurations for different plant Operational States within the scope of power PSA (e.g. operation with one turbine, operation with no turbine above 2% of nominal power, connection to reserve external grid). An example is the use of a Risk Monitor tool to evaluate the time dependent risk profile for a future time period, in which a series of plant configuration changes is being planned.
3.4.2 Real time configuration assessment and control (response to emerging conditions) This application is dealing with Task (2) discussed above in Item 3.4.1. Risk assessment and follow-up involves the online use of the PSA by plant personnel in order to keep the risk due to actual configurations, plant activities and unanticipated events at an acceptable level.	CDF/FDF(t), LERF(t), ICCDP, ICLERP, risk importance measures of SSCs as a function of time	Use of PSA model is essentially the same as described in Item 3.4.1 except for the time frame over which the risk to be evaluated is different (i.e. conditioned by the duration of emerging conditions). An example is the use of a Risk Monitor tool to perform post mortem evaluation of the time dependent risk profile for a previous time period in which a series of plant configuration changes has occurred. This application may also require reviewing the performance of the monitoring tools to ensure they are able to measure the risk impacts of all activities that were experienced.
3.4.3 Exemptions to TS and justification for continued operation	ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, ICCDP, ICLERP	The scope of this application is normally confined to a subset of SSCs that are currently included in the base case PSA model; otherwise the PSA is updated to incorporate all

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
As a comprehensive tool describing the risk associated with a particular plant configuration, the PSA can provide useful support to TS exemption justifications and/or to proposals for mitigation or compensatory measures, or to justify the relevance of these measures.		affected SSCs explicitly. The PSA model must explicitly model the areas affected by the TS change. The change in risk metrics is used to evaluate the risk significance and acceptability of the proposed change. This application is dealing with temporary changes and hence the decision criteria may be less restrictive than for the case of permanent changes because of one-time nature of the exemption. An example is the failure of an emergency feedwater pump shaft that requires a week to repair and a justification to relax the 72 hour AOT on a one-time basis while taking compensating measures to minimize the risk impacts.
3.4.4 Dynamic risk informed TS Typically, classical TSs consist of a rigid framework of prescriptions for individual equipment and systems involving fixed grace times, for example. The purpose of this rigid framework is to keep plant features within the licensing basis for a reasonably large fraction of time. Dynamic risk informed TS relax some of this rigidity based on the integral view of a PSA. AOTs are calculated for each plant state taking into account the complete picture of plant configuration and equipment out-of-service combinations. In some cases the calculated AOT may be shorter than the standard fixed technical specification version and in some cases a longer AOT is justified, but in all cases a careful evaluation is made at all times of the complete picture of POS including safety and non-safety related SSCs.	CDF/FDF(t), LERF(t), ICCDP, ICLERP	This application is similar to Item 3.4.3 except that new AOTs are not fixed in the technical specification document but dynamically calculated based on the status of all SSCs in the plant and a time dependent Risk Monitor. An example of this is a Risk Monitor that calculates a new AOT for each adverse configuration change made by the plant.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
4. PERMANENT CHANGES TO THE OPERATING PLANT		
4.1 Plant changes		
4.1.1 NPP upgrades, backfitting activities and plant modifications Identification of weaknesses and effective areas for improvement in plant design and operational features in view of plant risk. Assessment may include investigation of variants and of exploratory options. PSA arguments are used to support the selection, design, implementation, justification, and licensing of plant upgrades.	Risk importance measures (e.g. F-V, RAW) of affected SSCs and human actions, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	Importance measures from 'base case PSA' are used to help prioritize candidate design changes; change in CDF/FDF and LERF is used to justify acceptable risk impacts and to determine risk significance. The level of detail of the PSA model in the areas affected by the design changes may be greater than that for the rest of the plant; a more simplified conservative treatment of other parts of the model acceptable. Data for new additional equipment may not be available; therefore, treatment of such equipment in PSA model needs to be justified. A typical example for such application is the introduction of the primary feed and bleed feature in a PWR NPP, which would include hardware upgrades such as installation of relief valves which are qualified for feed and bleed and the elaboration and implementation of associated procedures.
4.1.2 Life time extension The application is often referred as a sub-case of the periodic safety review with the consideration of aging effects beyond the design lifetime. Involves modelling of aging effects in PSA. (See also Item 1.2.)	CDF/FDF$_{AVE}$, LERF$_{AVE}$, CDP, LERP, QHOs, risk importance measures of all SSCs and IEs, primary contributors to risk	A full scope PSA is needed to address the application in complete and consistent manner. The key issue in this application is the possible impact of aging phenomena and component lifetime considerations beyond the design lifetime on the overall risk metrics. Modelling the aging phenomena is in the exploratory stage; in principle the PSA need to be capable of estimating or bounding the possible effects of aging on passive components that are not normally maintained or replaced. Time trend analyses in relation to IE frequencies, equipment failure rates, cable material properties, etc. support the application. The analysis results provide additional information for regulators while licensing the lifetime extension. An example is the evaluation of the increase in risk due to aging of plant equipment past the design lifetime. Typical equipment of major interest are: reactor vessel, steam generator, piping, etc.
4.2 Technical specification changes		

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
4.2.1 Determination and evaluation of changes to allowed outage time and changes to required TS actions Required actions in TS have been typically derived on a classical engineering basis. This involves, for example, modified surveillance activities to compensate for reduced availability of equipment. Such items can be re-evaluated based on the PSA and changed eventually according to risk significance. Focus is on the risk impact due to the AOT period. This requires assessment of three types of risks: (a) instantaneous (conditional) risk while the component is in maintenance; (b) cumulative (integrated) risk over the AOT period; (c) average risk over a long period (e.g. yearly), taking into account the frequency of maintenance performed on a component. Optimum AOT may involve trade-offs between extended equipment unavailability during power operation and unavailability of the same equipment during shutdown conditions. The ultimate goal is to find the optimum AOT for each SSC covered in the technical specification with respect to how it constrains plant operation states and how it is used to manage risks of equipment being out of service. In addition, the PSA may be used to support the optimization of maintenance tasks with respect to whether they must be done during outages or	Risk importance measures of affected SSCs, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, ICCDP, ICLERP	The scope of this application is normally confined to a subset of SSCs that are currently included in the ‘base case PSA’ model; otherwise the PSA is updated to incorporate all affected SSCs explicitly. The level of detail of the PSA model in the areas affected by the AOT changes may be greater than that for the rest of the plant. The PSA model must explicitly model the maintenance unavailability for all SSCs when their respective AOTs have been changed. The model shall be capable to properly reflect all effects of system/component unavailability: setting components/system to unavailable state; balanced effect of unavailability of particular redundant train/component (symmetric model, e.g. steam line rupture is represented by rupture on SG1, so the effect of the unavailability of SG1 isolation valve is overestimated and the effect of unavailabilities of other equivalent isolation valves is underestimated). The changes in risk metrics are used to evaluate the risk significance and acceptability of the proposed change and the incremental risk metrics are used to evaluate the acceptability of the new proposed AOT. Example: One of the most common examples is an extension of the EDG AOTs to permit on-line overhauls of the components during power operation.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
whether on-line maintenance is appropriate.		
4.2.2 Risk informed optimization of TS The technical specifications define limits and conditions for operation, testing, and maintenance activities as a way to assure that the plant is operated safely. From time to time, the plant operator may need a TS exemption due to operational burdens and constraints. This application is used to optimize TS provisions. Beside risk insights, other non-risk based parameters may have to be used as constraints in the optimization process.	Risk importance measures of affected SSCs, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, ICCDP, ICLERP	This application is similar to Item 4.2.1 depending on the nature of the TS action to be changed. This application involves the definition of constraining parameters beside risk metrics to assure efficient results (e.g. cost-benefit correlations). An example is a proposal to remove as technical specification requirement to test an operable EDG every hour while a redundant EDG train is out of service.
4.2.3 Determination and evaluation of changes to surveillance test intervals PSA based evaluation of surveillance test intervals (STIs) considers the risk from unavailability due to undetected failures, and the risk from unavailability due to tests and test induced failures. The goal is to optimize the STIs with respect to their impact on equipment reliability and how these tests impact the cost of operations. Human errors during STIs that may have an adverse impact on safety, for example by leading to plant trips and initiating events normally is considered in deciding this optimization.	Risk importance measures (e.g. F-V, RAW) of affected SSCs, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	The scope of this application is normally confined to a subset of SSCs that are currently included in the 'base case PSA' model; otherwise the PSA is updated to incorporate the affected SSCs explicitly if they can be used in accident mitigation. The level of detail of the PSA model in the areas affected by the STI changes may be greater than that for the rest of the plant. The PSA model must explicitly model test unavailability of the SSC and provide a capability to predict the impact of changes to an STI for each affected component unavailability. Risk importance measures can be used to prioritize and rank the candidates for STI change. The change in risk metrics is used to evaluate the risk significance and acceptability of the proposed change and the incremental risk metrics are used to evaluate the acceptability of the new proposed STI. An understanding of how human errors during testing contribute to initiating event frequencies and component failures is needed to balance the positive and negative aspects of surveillance testing. Unavailability of equipment due to human errors to properly restore normal alignments after testing is to be taken into account. If it is known that a test may lead to a higher probability of an initiating event (initiating event frequency is related to test frequency) then this relationship must be taken into account

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
		if the test frequency is changed. A typical example is the test of safety injection trains by running one train via a full capacity bypass line back to the suppression pool (BWR) or back to the borated water storage tank (PWR). Typically, these systems are automatically reconfigured from the test configuration and started when a real demand happens. Thus, when increasing test frequency, there is a trade-off between reduced component unavailability, increased unavailability of equipment during the test due to realignment of valves, actuation of control circuits, opening of AC or DC circuit breakers, etc.
4.2.4 Risk informed in-service testing Use of PSA to support the surveillance programme, taking into account the relative risk significance of the components to be tested, is in the focus of the application. This application is normally limited to pumps and valves in safety related systems, but in principle can be applied to any component in the surveillance programme. The relative risk significance is assessed using a blend of probabilistic and deterministic methods before any test interval is changed and the aggregate impact of the changes is evaluated. This results in relaxation of testing requirements for low risk significant SSCs and SSC functions and increased requirements for higher risk significant SSCs yielding an optimized testing programme.	Risk importance measures (e.g. F-V, RAW) of affected SSCs, $\Delta CDF/FDF_{AVE}$, $\Delta LERF_{AVE}$	Risk importance measures from the base PSA used to help prioritize candidate changes to surveillance programme for selected pumps and valves, change in CDF/FDF and LERF used to justify acceptable risk impacts and to determine risk significance. Explicit model of test and maintenance unavailabilities and capability to predict or bound the impact of programme changes on component unavailability due to a random failure and test and maintenance unavailabilities needed to support this application. The PSA can be used to analyse how a change in test intervals affects the plant risk taking into account negative effects such as potentially increased frequency of plant transients, e.g. testing strategy for pressurizer relief valves, MSIVs, etc.
4.2.5 Risk informed in-service inspections The risk informed in-service inspection (RI-ISI) methodology consists of ranking the elements for inspection, such as welds in piping systems,	Component failure rates for different inspection strategies (e.g. obtained using PFM or Markov	This application is normally limited to piping system inspections, but in principle can be applied to any passive component covered in the In-Service Inspection (ISI) programme. These passive components are normally not explicitly modelled in a ‘base case PSA’. Hence, special analyses must be performed to estimate component (e.g.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
according to their risk significance and developing the inspection strategy (frequency, method, sample size, etc.) commensurate with their risk significance. It provides a framework for effective allocation of inspection resources and helps to focus the inspection activities where they are most needed. In addition, an understanding of the most likely degradation mechanisms is developed, which is used to focus required inspections to use the most appropriate inspection methods for the anticipated damage mechanisms.	model), CCDP/CFDP, CLERP, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	weld) level failure rates as a function of level and type of inspection, and consequences of pipe failure in terms of the CCDP/CFDP and CLERP due to the loss of function and secondary flooding and other consequences of system pipe breaks. These special analyses are used to develop risk importance measures or alternative risk ranking matrices which are used to help prioritize candidate changes to ISI programme for selected weld locations, change in CDF/FDF and LERF used to justify acceptable risk impacts and to determine risk significance. The base PSA model must be capable of supporting estimates of the CCDP/CFDP and CLERP of any assumed failure mode within the scope of the piping systems selected for the RI-ISI programme. To date, most examples involve in-service inspections of welds in NPP piping systems in which case the number, frequency, and method of non-destructive examination (NDE) are varied to improve the allocation of inspection resources to the most risk significant pipe elements and to manage the risk of inspections with respect to pipe ruptures. Future examples cover the breadth of SSCs currently covered in ISI programmes.
4.3 Establishment of graded QA programme for SSC		
4.3.1 Categorization of SSC for equipment risk significance evaluation PSA provides the necessary insights that are used to determine the relative safety significance of plant equipment. These probabilistic insights are for example utilized to help identify low/high safety significant SSCs that are candidates for reductions/improvements in QA treatment.	Risk importance measures of affected SSCs (e.g. F-V, RAW)	Risk importance measures are used to classify the risk and safety significance of SSCs. This information is considered in connection with the current safety classification of SSCs and associated QA and special treatment requirements; this is used to identify and rank candidate SSCs for proposed change in QA and special treatment requirements. An example is placing all plant SSCs into different categories based on safety related classification and risk importance using F-V and RAW type of measures.
4.3.2 Evaluation of risk impact of changes to QA requirements Changes in QA treatment of SSCs are investigated or explored within the framework of PSA.	Risk importance measures (e.g. F-V, RAW) of affected SSCs, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	In addition to the discussion provided in Item 4.3.1, sensitivity studies are required to assure robust decision making. Change in risk metrics are used to determine the risk significance and risk acceptability of the proposed change.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
		An example is evaluating the change in risk associated with relaxation of QA requirements.
4.4 Risk informed special site protection measures		
4.4.1 Risk informed fire protection Risk informed fire protect (RI-FP) is performed as an enhancement of the existing deterministic fire protection programme, or to allow for risk informed deviations from deterministic requirements.	CDF/FDF$_{AVE}$, LERF$_{AVE}$, risk, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	This may include the demonstration that the performance of local manual actions (outside the control room) following a fire is acceptable, or the risk impact due to fire protection features that do not fully meet code (e.g. partial area suppression, fire barriers less than the required rating, etc.) do not result in a significant increase in risk. The starting point for RI-FP is to demonstrate that the overall Fire Risk is acceptable. The PSA is then used to perform delta-CDF/LERF calculations for any deviation or condition that does not fully meet the deterministic requirements. Enhancement to the base Fire PSA may be needed in order to generate accurate risk estimates for the impacted fire scenarios. These enhancements depend on the risk calculations performed, but may include: Modelling of spurious operations in detail, including those potentially resulting in undesired operator actions. Plant specific estimates for fire protection features, such as detection and suppression availability. Performance of detailed fire modelling for both significant and selected non-significant scenarios in order to remove conservatism in the PSA. Hazard and scenario specific definition and analysis of each HFE in order to more accurately assess the impact for the selected operator actions. Accounting for equipment reliability impacts due to potential exposure to fire, smoke or heat as a result of the Fire. Overall, a more detailed Fire PSA is needed to support RI-FP.
4.4.2 Risk informed internal flood protection	CDF/FDF$_{AVE}$, LERF$_{AVE}$,	Risk informed Flooding Protection is envisioned to be similar to RI-FP above, with

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
Risk informed flood protect is performed as an enhancement of the existing deterministic programmes, or to allow for risk informed deviations from deterministic requirements.	risk, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	likely enhancements to the flooding PSA model to ensure a more detailed model is used. Enhanced reliability modelling of flooding features may be required, such as level alarms, isolation features, etc.
4.4.3 Risk informed defence in depth for individual and correlated site hazards Risk informed defence-in-depth evaluates an existing hazard (e.g. Fire, Flood, and Seismic) to ensure there is adequate DID for each hazard sequence above a specified frequency.	ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk	The analysis of RI-DID is similar to that described in 2.3 above. There are several methods used to evaluate the robustness of NPPs against external hazards that utilize information obtained from PSA. In particular Fault Sequence Analysis (FSA) method currently being developing by the IAEA could be used [50]. In this method the MCSs obtained from Level 1 internal events PSA model are reviewed to verify whether one or several MCSs exist in which all components represented by basic events fail given the hazard or set of hazards of certain intensity. Another approach for advanced plants is the review of the Safety Functional Capability for each hazard to ensure all hazard events (above a specified frequency) can be mitigated using two available safety functions. Initially, this involves the review of CCDP/CFDP (or CLERP) results to ensure there are two systems credited for each analysed hazard initiating event. However, for spatial events, additional analysis would be performed to ensure that at least one train is available given a credited barrier (for fire or flooding) or other feature fails. Important to this application is enhancing the hazard-specific PSA to remove conservatism where DID is initially shown as inadequate. This may include additionally modelling of plant features, enhanced seismic fragility analysis, etc. For spatial events such as fires and floods, additional modelling of multi compartment scenarios may be needed.
5. OVERSIGHT ACTIVITIES		
5.1 Performance monitoring		
5.1.1 Planning and prioritization of inspection activities (regulatory and industry)	CDF/FDF$_{AVE}$, LERF$_{AVE}$,	The insights from baseline PSA results are used to support setting the agenda and

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
PSA based ranking of design and operational features is used to focus resources for regulatory and industry inspections on important issues and equipment.	QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CCDP/CFDP, CLERP	priorities for specific inspections so that the areas of the plant and operator actions that are most risk significant reflect the highest priority. An example could be the decision to focus the scope of an inspection on the material condition of SSCs found to be responsible for the dominant risk sequences in the plant's PSA.
5.1.2 Long term risk based performance indicators The long term risk based indicators focus on monitoring plant behaviour in order to get insights on the past history of NPP safety and to update the calculated average CDF/FDF. Long term use includes analysis of past plant behaviour integrating the events occurred, failures and unavailabilities. This information (including CDF/FDF trends, comparison between expected and calculated CDF/FDF, etc.) is of interest to regulators and high-level plant management. Long term risk based indicators can also help to pinpoint aging effects on components and systems. This information is important for the plant staff and can initiate design changes or modifications to testing and maintenance strategies, etc. Similarly, long term risk indicators can be drawn up for planning purposes. For long term planning, the assumptions regarding planned design changes, expected component behaviour, etc. can be introduced in the PSA models and data and can be analysed to obtain the expected average CDF/FDF for the next period.	CDF/FDF$_{AVE}$, LERF$_{AVE}$, CDF/FDF(t), LERF(t), QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk	The PSA results can be used to determine the appropriate set of performance indicators. For example, the high risk significant SSCs can be used to define SSC unavailability and failure performance metrics that are highly correlated to significant CDF/FDF and LERF impacts. If these risk metrics are updated over a long period of time, aging effects may be indicated. Special indicators might be useful that are derived from plant specific data and operating experience. For this purpose, the use of plant specific component reliability data is important. The components and SSC to be analysed can be derived with the use of importance measures. Risk Monitor can be used as a supporting tool to derive averaged CDF/FDF estimates derived by integration of instantaneous CDF/FDF for the observed POSs. An example is the trending of the number of failures or unavailable hours of a highly risk significant SSCs.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
5.1.3 Short term risk based performance indicators Risk based indicators for short term use requires instantaneous evaluation of risk. This type of application provides information on changes in CDF/FDF due to plant events and risk associated with planned activities.	CDF/FDF$_{AVE}$, LERF$_{AVE}$, CDF/FDF(t), LERF(t), QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk	The PSA results can be used to determine the appropriate set of performance indicators. For example, the high risk significant SSCs can be used to define SSC unavailability metrics that are highly correlated to significant CDF/FDF and LERF impacts. Similar to Item 5.1.2, use of plant specific data is important. Risk Monitor is an appropriate tool to evaluate instantaneous CDF/FDF. An example is the identification of the abnormal conditions for equipment operation leading to increase in their failure probabilities.
5.2 Performance assessment		
5.2.1 Assessment of inspection findings This type of application provides information on changes in risk measures associated with inspection findings. Change in risk metrics and conditional risk metrics can be used to evaluate the risk impact of degradations or issues that are found during the inspections and to evaluate possible corrective actions.	Risk importance measures of all SSCs and HEs, primary contributors to risk, CDF/FDF$_{AVE}$, LERF$_{AVE}$, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	This application is similar to the risk evaluation of significant events in terms of how the PSA is used to evaluate the risk significance of a plant condition that may be considered for different levels of inspections depending on the results. Often, simplified generic PSA models are used to perform a conservative screening evaluation first and if significant, it may be followed up with a more realistic and detailed evaluation. Depending on the area of inspection findings, PSA of different scope might be needed. Example: Use of PSA models to estimate the risk significance of an inspection finding that a fire barrier had been improperly removed from a NPP.
5.2.2 Evaluation and rating of operational events By PSA based extrapolation of operational events to accident scenarios with serious consequences, valuable insights can be gained regarding accidents on the basis of minor incidents, without suffering their real consequences. PSA can be used to analyse plant events, which may initiate a plant trip, degrade or disable safety systems, or	CCDP/CFDP, CLERP, CDF/FDF$_{AVE}$, LERF$_{AVE}$	If the event in question is an initiating event, the PSA model is used to estimate the CCDP/CFDP and CLERP, whose values are used to determine the safety classification of the event. The precursor event analysis is also part of this application. If the event in question impacts the availability of one or more SSCs and/or operator actions but is not an initiating event, the PSA model is used to calculate the CDF/FDF and LERF taking in to account the unavailability of the affected SSCs. Risk Monitor is an appropriate tool to evaluate the impact of such events. The PSA model must be capable of evaluating the appropriate impacts assessed for the event.

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
both simultaneously. The application can then provide an estimate, in terms of a conditional probability, of the available margin for an accident with unacceptable consequences. Thus, the basic purpose of PSA based operational event analysis is to determine how an operational event could have degenerated into an accident with more serious consequences and to derive the conditional probability of core/fuel damage due to such event.		Example: Evaluating the conditional probability of core/fuel damage or large early release from a significant safety event such as an initiating event accompanied by degradation or failure of multiple SSCs and/or human actions.
6. EVALUATION OF SAFETY ISSUES		
6.1 Risk evaluation		
6.1.1 Risk evaluation of corrective measures Based on PSA insights corrective measures regarding safety issues are developed. This may include exploratory investigation on different variants to resolve a particular issue.	ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$	Change in risk metrics are used to determine the risk significance and risk acceptability of the proposed change based on risk characterization. Example: Risk evaluation of measures taken to reduce the risk of reactor vessel head corrosion.
6.1.2 Risk evaluation to identify and rank safety issues As a result of a PSA, important new plant specific safety issues and generic issues may be identified. Furthermore, PSA is used for evaluating the relative importance of existing and new safety issues.	CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk, assumptions impacting results	Contributors to risk and risk importance measures are used to identify and rank safety issues. Also safety issues identified outside the PSA can be evaluated by the PSA to determine their risk significance once the issues have been assessed for risk characterization, i.e. determination of affected initiating events, accident sequences, SSCs and operator actions. Some safety issues may require extensions to PSA model to evaluate. Example: Elimination of an item from the list of unresolved safety issues based on risk insights.
6.1.3 Assessment of the safety importance of deviations between an existing plant design and	CDF/FDF$_{AVE}$, LERF$_{AVE}$,	The key issue in this application is the possible impact of changes in the design rules on

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
updated/revised deterministic design rules or new information about the site hazards. Assessment may include investigation of risk significance of deviations from revised design rules; often performed in the framework of a periodic safety review.	QHOs, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, Risk importance measures of affected SSCs and HEs (e.g. F-V, RAW)	risk associated with plant operation. Special model adjustments, model extensions and revisiting assumptions may be required to model the deviation of the plant design from revised deterministic rules of concern. Identification of primary contributors to risk and comparison with safety target values (CDF/FDF, LERF) may be needed. For example, for the operating plants constructed in accordance with the old design rules, PSA results, and risk metrics can be used to justify low risk significance of certain deviations from revised rules.
6.1.4 Assessment of the significant of overall site risk for multiunit accidents A multiunit PSA looks at the combined risk for multiple units operating on the same site, including the potential for a multiunit initiating event and a multiunit release.	CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$,	For multiunit sites, both deterministic and probabilistic safety evaluations have been performed on each reactor unit one at a time with the implicit assumption that the co-located reactors and radiological facilities (or sources) are safe while the reactor unit in question is being analyzed. A multiunit PSA includes an integrated safety assessment of the site and consideration of the potential for accidents involving multiple reactor units and multiple sources of radioactive material, concurrently. Input to a multiunit PSA is a full scope internal and external event PSA. In general, the primary cause of a multiunit accident is due to external hazards, although internal hazards such as fires and floods can also be important, depending on the shared equipment or locations. However, model enhancements are needed to account for possible initiating events, accident sequences and plant response (safe shutdown) following a multiunit initiating event. Additionally, the consideration of potential core damage on one unit in the response of another unit is needed. This includes modelling of plant impacts during all POSs and combinations of POSs.
6.1.5 Assessment of the significant of overall site risk from all radioactive sources.	CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, Dose Frequency	The base PSA includes analysis of possible radioactive releases from the primary core. The scope may or may not include fuel located in the spent fuel pool or similar. When assessing releases from all radioactive sources, the initial enhancement is to analyse stored fuel, either in the fuel pool, dry storage or similar. A PSA of the fuel pool would generally be formed similar to the base PSA, and may utilize much of the

Brief description of PSA application	PSA results and metrics used in decision making[17]	Comments on how PSA models can be used to support application and examples
		base PSA modelling of support systems or common systems. Analysis of dry cast storage would be a unique analysis, utilizing an overall similar accident sequence modelling as the base PSA, but with consideration of conditions that would fail the fuel in the cask. This may include the analysis of heavy load drops. Finally, other radioactive sources may need to be considered such as solid or liquid radioactive waste storage and handling, radiation sources such as those used in radiography, or other possible sources.
6.2 Regulatory decisions		
6.2.1 Long term regulatory decisions PSA insights are used to guide long term prioritization of regulatory objectives and requirements, and of related safety research.	CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CCDP/CFDP, CLERP	PSA results are used to develop risk insights, and strategies to maintain or reduce risk levels are revised. Change in risk metrics are used to evaluate possible changes to requirements needed to implement the risk management strategy. Example: Decision to shutdown the plant or terminate plant operation until the necessary global modifications aimed to reduce risk associated with plant operation would be performed.
6.2.2 Interim regulatory decisions PSA is used to alleviate a regulatory concern, while longer-term solutions can be evaluated. Issues that typically require an interim decision are: (a) need for regulatory action in response to an event at a plant, (b) one-time exemptions from TS or other licensing requirements, and (c) temporary modifications to hardware configuration or procedures.	CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk, ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CCDP/CFDP, CLERP	The use of PSA in regard to this application is essentially the same as in Item 6.2.1; depending on the subject of the interim regulatory decision may be dealing with different risk evaluation aspects (see Application Group 6.1). Example: Decision to terminate plant operation until the modifications aimed to reduce risk associated with plant operation would be performed or decision to allow certain changes at the plant aimed to increase cost efficiency of plant operation if insignificant risk increase would be justified.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for Integrated Risk Informed Decision Making Process, INSAG-25, IAEA, Vienna (2011).

[2] THE AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-S-2002, ASME, New York (2002).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 PSA, IAEA Safety Standards Series: Safety Guide No. SSG-3, IAEA, Vienna (2010).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 PSA, IAEA Safety Standards Series: Safety Guide No. SSG-4, IAEA, Vienna (2010).

[5] AMERICAN SOCIETY OF MECHANICAL ENGINEERS and AMERICAN NUCLEAR SOCIETY, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, Addendum B, ASME/ANS RA-Sb-2013, New York (2013).

[6] AMERICAN SOCIETY OF MECHANICAL ENGINEERS and AMERICAN NUCLEAR SOCIETY, Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plant, ASME/ANS RA-S-1.4-2013, New York (2013).

[7] AMERICAN SOCIETY OF MECHANICAL ENGINEERS and AMERICAN NUCLEAR SOCIETY, Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), ASME/ANS RA-S-1.2-2015 (Trial Use), New York (2015).

[8] AMERICAN NUCLEAR SOCIETY, Low Power and Shutdown PRA Methodology, ANSI/ANS 58.22-2015 (Trial Use), LaGrange Park (2015).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice, Safety Series No. 50-P-10, IAEA, Vienna (1996).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series: Safety Requirement No. GS-R-3, Vienna (2006).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for a Quality Assurance Programme for PSA, IAEA-TECDOC-1101, IAEA, Vienna (1999).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, IPERS Guidelines for the International Peer Review Service. Second Edition. Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessments, IAEA-TECDOC-832, IAEA, Vienna (1995).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Accident Progression, Containment Analysis and Estimation of Accident Source Terms, Safety Series No. 50-P-8, IAEA, Vienna (1992).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-Site Consequences and Estimation of Risks to the Public: A Safety Practice, Safety Series No.50-P-12, IAEA, Vienna (1996).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-7, Vienna (1995).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna (2007)

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, IAEA-TECDOC-1200, IAEA, Vienna (2001).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of internal fires in probabilistic safety assessment for nuclear power plants, Safety Reports Series No. 10, Vienna (1998).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment for Seismic Events, IAEA-TECDOC-724, Vienna (1993).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic safety assessments of nuclear power plants for low power and shutdown modes, IAEA-TECDOC-1144, Vienna (2000).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Defining Initiating Events for Purpose of Probabilistic Safety Assessment, IAEA-TECDOC-719, IAEA, Vienna (1993).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Common Cause Failure Analysis in Probabilistic Safety Assessment, IAEA-TECDOC-648, IAEA, Vienna (1992).

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

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants: Safety Guide. Safety Standards Series No. NS-G-3.1, Vienna (2002).

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, External Man-Induced Events in Relation to Nuclear Power Plant Design, Safety Series No. 50-SG-D5 (Rev. 1), Vienna (1996).

[26] ELECTRIC POWER RESEARCH INSTITUTE, Identification of External Hazards for Analysis in Probabilistic Risk Assessment, EPRI 1022997, Palo Alto (2011).

[27] US NUCLEAR REGULATORY COMMISSION, Evaluation of External Hazards to Nuclear Power Plants in the US, Other External Events. Supplement 2, NUREG/CR-5042, Washington (1989).

[28] US NUCLEAR REGULATORY COMMISSION, Procedural and Submittal Guidance of Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, NUREG 1407, Washington (1991).

[29] US NUCLEAR REGULATORY COMMISSION, PSA Procedures Guide, NUREG/CR-2300, Washington (1983).

[30] AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, Guidelines for Chemical Process Quantitative Risk Analysis, 2nd Edition, AIChE/CCPS, New York (2000).

[31] SWEDISH NUCLEAR INSPECTORATE (SKI), Guidance for External Event Analysis, SKI Report 02:27, Stockholm (2003).

[32] FEDERAL ENVIRONMENTAL, INDUSTRIAL AND NUCLEAR SUPERVISION SERVICE, Accounting of External Natural and Man-Induced Impacts on Nuclear Facilities, NP-064-05, Moscow (2005).

[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series: Safety Guide No. SSG-18, Vienna (2011).

[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series: Safety Guide No SSG-9, Vienna (2010).

[35] US NUCLEAR REGULATORY COMMISSION, A Framework for Low Power/Shutdown Fire PRA, NUREG/CR-7114, Washington (2013).

[36] US NUCLEAR REGULATORY COMMISSION, Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts, NUREG/CR-6372, Washington (1997).

[37] US NUCLEAR REGULATORY COMMISSION, Guidelines on Modelling CCFs in PSA, NUREG/CR-5485 prepared by A. Mosleh, D. M. Rasmuson and F. M. Marshall for USNRC, USNRC, Washington (1998).

[38] US NUCLEAR REGULATORY COMMISSION, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, USNRC, Washington (1983).

[39] US NUCLEAR REGULATORY COMMISSION, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, USNRC, Washington (1987).

[40] US NUCLEAR REGULATORY COMMISSION, Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), Revision 1, NUREG-1624, USNRC, Washington (1999).

[41] INTERNATIONAL ATOMIC ENERGY AGENCY, Case Study on the Use of PSA Methods: Station Blackout Risk at Millstone Unit 3, IAEA-TECDOC-593, IAEA, Vienna (1991).

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

[43] INTERNATIONAL ATOMIC ENERGY AGENCY Seismic Evaluation of Existing Nuclear Power Plants, Safety Report Series No. 28, Vienna (2003).

[44] ELECTRIC POWER RESEARCH INSTITUTE, A Methodology for Assessment of Nuclear Power Plant Seismic Margins, Revision 1, EPRI NP-6041-SLR1, Palo Alto (1991).

[45] US NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: an Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, USNRC, Washington, DC (Vol. 1 and Vol. 2: December 1990), (Vol. 3: January 1991).

[46] US NUCLEAR REGULATORY COMMISSION, Interim Reliability Evaluation Program Procedures Guide, NUREG/CR-2728, USNRC, Washington (1983).

[47] US NUCLEAR REGULATORY COMMISSION, Joint Assessment of Cable Damage and Quantification of Effects from Fire (JACQUE-FIRE). Volume 2: Expert Elicitation Exercise for Nuclear Power Plant Fire-Induced Electrical Circuit Failure, NUREG/CR-7150/V2, Washington (2014).

[48] INTERNATIONAL ATOMIC ENERGY AGENCY, Review of Probabilistic Safety Assessments by Regulatory Bodies, Safety Report Series No. 25, IAEA, Vienna (2002).

[49] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Review of Probabilistic Safety Assessment (PSA) – Level 1, IAEA-TECDOC-1135, IAEA, Vienna (2000).

[50] I.Kuzmina, A.Lyubarskiy, P.Hughes, J.Kluegel, T.Kozlik and V.Serebrjakov, "The Fault Sequence Analysis Method to Assist in Evaluation of the Impact of Extreme Events on NPPs", paper presented at Nordic PSA Conference – Castle Meeting-2013, Stockholm, Sweden, April 10-12, 2013.

[51] INTERNATIONAL ATOMIC ENERGY AGENCY, OECD NUCLEAR ENERGY AGENCY, Risk Monitors: The State of the Art in their Development and Use at Nuclear Power Plants, WGRisk, NEA/CSNI/R(2004)20, OECD, Paris (2004).

DEFINITION OF TERMS

Definitions appearing in this list apply for the purposes of this TECDOC only. Definitions marked with (*) are directly taken from the IAEA Safety Glossary.

*Accident**: Any unintended event, including operating errors, equipment failures and other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.

Accident conditions: Deviations from normal operation more severe than anticipated operational occurrences, including those resulting from design basis accidents and severe accidents related to the status of (a) fuel, (b) the reactor coolant system, and (c) radionuclide transport barriers.

Accident consequences: The extent of plant damage or/and the radiological release or/and health effects to the public or/and the economic costs of an accident.

Aleatory uncertainty: The uncertainty inherent in a nondeterministic (stochastic, random) phenomenon. Aleatory uncertainty is reflected by modelling the phenomenon in terms of a probabilistic model. In principle, aleatory uncertainty cannot be reduced by the accumulation of more data or additional information. (Aleatory uncertainty is sometimes called randomness.)

As-built, as-operated: A conceptual term that reflects the degree to which the PSA matches the current plant design, plant procedures, and plant performance data, relative to a specific point in time.

As-designed, as-to-be-built, and as-to-be-operated: A conceptual term that reflects the degree to which the PSA reflects the current status of the plant at the design and construction phase for which the PSA is being performed.

Assumption: A decision or judgment that is made in the development of the PSA model. An assumption either is related to a source of model uncertainty or is related to scope or level of detail. An assumption related to a model uncertainty is made with the knowledge that an alternative assumption exists. An assumption related to scope or level of detail is one that is made for modelling convenience.

At-initiator human failure event: A type of human failure event that causes an initiating event. These are HFEs that directly involve plant personnel actions at the time of the initiating event, including actions correctly performed but that are based on erroneous indications and actions that are performed based on erroneous decision making. These events do not include malicious acts such as sabotage.

At power: Those POSs characterized by the reactor being critical and producing power, with automatic actuation of critical safety systems not blocked and with essential support systems aligned in their normal power operation configuration.

Attributes (of PSA): Characteristics of PSA elements of a full scope Level 1 PSA that assure technical quality and consistency of the PSA. Attributes of the PSA that are irrelative to particular application are termed as ‘general attributes’, attributes of the PSA that is used for particular application(s) are termed as ‘special attributes’.

Availability: The complement of unavailability.

Basic event: An event in a fault tree model that requires no further development because the appropriate limit of resolution has been reached.

Bounding analysis: Analysis that uses assumptions such that the assessed outcome will meet or exceed the maximum severity of all credible outcomes.

Cable failure mode: The behaviour of a cable upon fire-induced failure that may include intractable shorting, intercable shorting, and/or shorts between a conductor and an external ground.

Cliff edge effect: In a nuclear power plant, an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input. Cliff edge could be seen in any situation where the plant conditions suffer a radical undesirable change with a small time step or a small variation in an individual parameter. One example is the case where the supply of cooling water is stable in the 24 hr mission time, but is exhausted a short time thereafter resulting in a complete loss of cooling. Another is the case where a plant is unaffected by an external flood up to a given level, but immediately upon exceeding that level there is extensive loss of safety functions leading to a high likelihood of core damage.[18]

Common cause failure:* Failure of two or more structures, systems and components due to a single specific event or cause.

*Common mode failure**: Failure of two or more structures, systems and components in the same manner or mode due to a single event or cause.

Complementary cumulative distribution function (CCDF): Complement of cumulative distribution function.

Component: A discrete element of a *system*, such as a vessel, pump, valve, or circuit breaker.

Confinement:* Prevention or control of releases of radioactive material to the environment in operation or in accidents.

*Containment**: Methods or physical structures designed to prevent or control the release and the dispersion of radioactive substances.

*Containment system**: The assembly of components of the packaging specified by the designer as intended to retain the radioactive material during transport.

Containment (confinement) bypass: A direct or indirect flow path that may allow the release of radioactive material from the RCS directly to the environment bypassing the containment (confinement or reactor building).

[18] The terminology comes from the idea that someone is walking along a road and everything is just fine until at the end of the road they take one more step and fall off the edge of a cliff.

Containment (confinement) failure: Loss of integrity of the containment (confinement) to perform its safety functions in the mitigation of an accidental release of radionuclides to the environment.

Containment (confinement) failure mode: The manner in which a containment (confinement) radionuclide release pathway is created. It encompasses both those structural failures of containment (confinement or reactor building) induced by containment (confinement or reactor building) challenges when they exceed containment (confinement) capability and the failure modes of containment (confinement) induced by HFEs, isolation failures, or bypass events.

Cumulative distribution function: Integral of the probability density function; it gives the probability of a parameter of being less than or equal to a specified value.

Damage criteria: Those characteristics of the fire-induced environmental effects that will be taken as indicative of the fire-induced failure of a damage target or set of damage targets.

Damage target: See *target*.

Demonstrably conservative analysis: Analysis that uses assumptions such that the assessed outcome will be conservative relative to the expected outcome.

Dependency: Requirement external to an item and upon which its function depends. Dependency exists when the occurrence of given event is determined by, influenced by, or correlated to other events or occurrences.

Design basis earthquake (DBE): A commonly employed term for the earthquake severity specified in the plant design basis and against which those systems, structures, and components required to assure a safe shutdown of the plant in the event of an earthquake are designed. In IAEA seismic safety reports this is referred to as SL-2, but various states use other terms such as SSE (*safe shutdown earthquake*).

Design basis hazard event: A generalized term for specific characteristics of the hazard severity and type that are specified in the plant design basis and against which those systems, structures, and components required to assure a safe shutdown of the plant in the event of a hazard are designed. If no specific characteristics are specified in the plant design basis for a specific hazard, then there is no design basis hazard event for that hazard. Examples include the design basis tornado, expressed as wind speed; the design basis earthquake, expressed as peak ground acceleration (PGA), spectral shape, and time history; the design basis precipitation, expressed as the maximum rate and duration of precipitation (for rainfall or snowfall).

Distribution system: Piping, raceway, duct, or tubing that carries or conducts fluids, electricity, or signals from one point to another.

Electrical overcurrent protective device: An active or passive device designed to prevent current flow from exceeding a predetermined level by breaking the circuit when the predetermined level is exceeded (e.g. fuse or circuit breaker).

End state: The set of conditions at the end of an event sequence that characterizes the impact of the sequence on the plant or the environment.

Epistemic uncertainty: The uncertainty attributable to incomplete knowledge about a phenomenon that affects our ability to model it. Epistemic uncertainty is reflected in ranges of values for parameters, a range of viable models, the level of model detail, multiple expert interpretations, and statistical confidence. In principle, epistemic uncertainty can be reduced by the accumulation of additional information. Epistemic uncertainty is sometimes also called modelling uncertainty.

Equipment: A term used to broadly cover the various components in an NPP. Equipment includes electrical and mechanical components (e.g. pumps, control and power switches, integrated circuit components, valves, motors, fans, etc.), instrumentation and indication components (e.g. status indicator lights, meters, strip chart recorders, sensors, etc.).

Equipment qualification: Generation and *maintenance* of evidence (i.e. data and documentation) to ensure that equipment is capable of operating on demand, under specified *service conditions*, to meet *system* performance requirements.

Expert: An individual who, by virtue of academic qualifications and experience, is duly recognized as having expertise in one or more particular technical areas of a PSA, and , who is capable of evaluating the relative credibility of multiple alternative hypotheses

Event frequency : The expected number of occurrences of an event such as an initiating event or event sequence per unit of time, normally expressed in events per plant-operating-year (or reactor-operating-year) or events per plant-calendar-year (or reactor-calendar-year). For PSAs that are performed on multiunit plants, event frequencies are normally measured on a per–plant-year basis, whereas PSAs that are performed on a single reactor unit are normally measured on a per–reactor-year basis.

Event sequence: A representation of a scenario in terms of an initiating event defined for a set of initial plant conditions followed by a sequence of system, safety function, and operator failures or successes, with sequence termination with a specified end state.

Event tree: A logic diagram that begins with an initiating event or condition and progresses through a series of branches that represent expected system or operator performance that either succeeds or fails and arrives at either a successful or failed end state.

Event tree top event: The conditions (i.e. system behaviour or operability, human actions, or phenomenological events) that are considered at each branch point in an event tree (sometimes called “modelling function” or “modelled function”)

Expert elicitation: A formal, highly structured, and documented process whereby expert judgments, usually of multiple experts, are obtained.

Expert judgment: Information provided by a technical expert, in the expert’s area of expertise, based on opinion or on an interpretation based on reasoning that includes evaluations of theories, models, or experiments.

Exposed structural steel: Structural steel elements that are not protected by a passive fire barrier feature (e.g. fire-retardant coating) with a minimum fire-resistance rating of one hour or less.

External Hazard: See *Hazard (External).*

Extremely rare event: One that would not be expected to occur even once throughout the world nuclear industry over many years (e.g. <10^{-6}/plant-year).

Failure mechanism: Any of the processes that result in failure modes, including chemical, electrical, mechanical, physical, thermal, and human error.

Failure mode:* The manner or state in which a structure, system or component fails (e.g. fails to start, fails to run, leaks, spurious operation).

Failure modes and effects analysis (FMEA): A process for identifying failure modes of specific components and evaluating their effects on other components, subsystems, and systems.

Failure probability: The likelihood that an SSC will fail to perform a specified function required in the PSA for a specific mission time.

Failure rate: Expected number of failures per unit time, evaluated, for example, by the ratio of the number of failures in a population of components to the total time observed for that population.

Fault tree: A deductive logic diagram that depicts how a particular undesired event can occur as a logical combination of other undesired events.

Figure of merit: The quantitative value, obtained from a PSA analysis, used to evaluate the results of an application (e.g. CDF).

Fire analysis tool: Any method used to estimate or calculate one or more physical fire effects (e.g. temperature, heat flux, time to failure of a damage target, rate of flame spread over a fuel package, heat release rate for a burning material, smoke density, etc.), based on a predefined set of input parameter values as defined by the fire scenario being analysed. Fire analysis tools include, but are not limited to, computerized compartment fire models, closed-form analytical formulations, empirical correlations such as those provided in a handbook, and lookup tables that relate input parameters to a predicted output.

Fire zone: A portion of a building or plant that is separated from other zones by rated fire barriers adequate for the fire hazard severity associated with that zone.

Fire barrier: A continuous vertical or horizontal construction assembly designed and constructed to limit the spread of heat and fire and to restrict the movement of smoke.

Fire compartment: A subdivision of a building or plant that is a well-defined enclosed room, not necessarily bounded by rated fire barriers. A fire compartment generally falls within a fire zone and is bounded by non-combustible barriers where heat and products of combustion from a fire within the enclosure will be substantially confined. Boundaries of a fire compartment may have open equipment hatches, stairways, doorways, or unsealed penetrations. This is a term defined specifically for fire risk analysis and maps plant fire zones, defined by the plant and based on fire protection systems design and/or operations considerations, into compartments defined by fire damage potential. For example, the control room or certain areas within the turbine building may be defined as a fire compartment.

Fire-induced initiating event: That initiating event assigned to occur in the internal fire PSA plant response model for a given fire scenario.

Fire modelling: The process of exercising a fire analysis tool including the specification and the verification of input parameter values, performance of any required supporting calculations, actual application of the fire analysis tool itself, and the interpretation of the fire analysis tool outputs and results.

Fire protection feature: Administrative controls, fire barriers, means of egress, industrial fire brigade personnel, and other features provided for fire protection purposes.

Fire protection programme: The integrated effort involving equipment, procedures, and personnel used in carrying out all activities of fire protection. It includes system and facility design, fire prevention, fire detection, annunciation, confinement, suppression, administrative controls, fire brigade organization, inspection and maintenance, training, quality assurance, and testing.

Fire protection system: Fire detection, notification, and suppression systems designed, installed, and maintained in accordance with the applicable fire codes and standards

Fire-resistance rating: The time, in minutes or hours, that materials or assemblies have withstood a fire exposure as established in accordance with an approved test procedure appropriate for the structure, building material, or component under consideration.

Fire scenario: A set of elements that describes a fire event. The elements usually include a physical analysis unit, a source fire location and characteristics, detection and suppression features to be considered, damage targets, and intervening combustibles.

Fire scenario selection: The process of defining the fire scenarios to be analysed in the internal fire PSA that will represent the behaviour and consequences of fires involving one or more fire ignition sources. Fire scenario selection includes the identification of a fire ignition source (or set of fire ignition sources); secondary combustibles and fire spread paths; fire damage targets, detection and suppression systems, and features to be credited; and other factors that will influence the extent and timing of fire damage.

Fire suppression system: Permanently installed fire protection systems provided for the express purpose of suppressing fires. Fire suppression systems may be either automatically or manually actuated. However, once activated, the system should perform its design function with little or no manual intervention.

Fire wrap: A localized protective covering designed to protect cables, cable raceways, or other equipment from fire-induced damage. Fire wraps generally provide protection against thermal damage.

Flood zone (area): A zone (area) within a plant that is defined for the purpose of performing an Internal Flood PSA. Flood zones are normally defined in terms of one or more of the following: building types; location within a building; and the physical barriers that delay, restrict, or prevent the propagation of floods to adjacent areas.

Flood-induced event sequence: An event sequence that includes a *flood-induced initiating event* (and the potential for undesired consequences), with a specified end state.

Flood-induced initiating event: An initiating event (e.g. transient or LOCA) that is caused indirectly by a flood (e.g. flood damages SSCs that in turn cause a reactor trip transient or exigent plant shutdown due to loss of function of one or more SSCs due to the flood).

Flood propagation path: A physical pathway that would allow the progression of a flood and associated flood damage within and among different *flood zones.*

Flood rate: The flow rate of water or steam across the breach or opening in the pressure boundary of the *flood source* during the flood event. Depending on the context, the flood rate may be a time dependent rate, a maximum rate, or an average rate over the duration of the flood.

Flood scenario: A description of an event that results in a *flood-induced initiating event.* The factors considered in the definition of a flood scenario include flood area; flood source; flood rate; flood propagation path; impact on plant SSCs; human actions considered in flood initiation, mitigation, and termination; and means of detection (sensors, alarms, indications, etc.).

Flood source: An inventory of water or steam normally contained within a system, tank, component, reservoir, river, lake, or ocean that provides the potential for flooding-induced failure of SSCs in the event the flood source container or pressure or retention boundary is breached.

Flood volume: The total flood volume of water released from the source from flood initiation to termination or to a specific point in time during a *flood scenario,* unless specified as the localized volume in specific flood areas for scenarios that involve multiple flood areas. Flood volume is normally used to calculate the nominal flood height, which is associated with the submergence failure cause. Water spray volumes are generally different from flood volumes, but spray water may accumulate and contribute to flood volumes.

Fragility: The conditional probability of SSC failure to perform its PSA required function at a given hazard input level (i.e. for a given hazard event).

Frequency (probability) of exceedance: The frequency (probability) that a specified intensity of the hazard will be exceeded at a site or in a region during a specified exposure time.

Front-line system: A system (safety or non-safety) that is capable of directly performing one of the accident-mitigating functions (e.g. core heat removal, reactivity control, or reactor vessel pressure control) modelled in the PSA.

Full power or nominal full power: A POS during which the reactor power is at or near its normal designed value. In this POS, the primary system configuration (power level, pressure, temperature, boundaries, etc.) is maintained essentially constant. The “low-power” state is defined to include all at-power operations below nominal full power.

Fundamental safety functions: See *key safety functions.*

Fussell-Vesely (F-V) importance measure: For a specified basic event, F-V importance is the fractional contribution to the total of a selected figure of merit (e.g. CDF) for all event sequences associated with the figure of merit containing that basic event. For PSA quantification methods that include non-minimal cut sets and success probabilities, the F-V importance measure is calculated by determining the fractional reduction in the total figure of merit brought about by setting the probability of the basic event to zero.

Ground acceleration: Acceleration at the ground surface produced by seismic waves, typically expressed in units of g, the acceleration of gravity at the earth's surface.

Harsh environment: An abnormal environment (e.g. high or low temperature, humidity, corrosive conditions) expected as a result of the event sequences modelled in the PSA.

Hazard: Any occurrence that has the potential to result in an initiating event. Hazards are divided into internal and external to the plant hazards.

Hazard (Internal):* Hazards originating from the sources located on the site of the nuclear power plant, both inside and outside plant buildings. Examples of internal hazards are random equipment failures and/or human failures, internal fires, internal floods, turbine missiles, on-site transportation accidents and releases of toxic substances from on-site storage facilities that can cause equipment damage or/and human error. Internal hazards caused by random equipment failures or/and human errors are known usually called internal events.

Hazards (External): Hazards* originating from the sources located outside the site of the nuclear power plant. Examples of external hazards are seismic hazards, external fires (e.g. Fires affecting the site and originating from nearby forest fires), external floods, high winds and wind induced missiles, off-site transportation accidents, releases of toxic substances from off-site storage facilities and severe weather conditions.

Hazard analysis: The process to determine an estimate of the expected frequency of occurrence (over some specified time interval) of various levels of some characteristic measure of the intensity of a hazard (e.g. PGA to characterize ground shaking from an earthquake). The time period of interest is typically 1 year, in which case the estimate is called the annual frequency of occurrence.

Hazard event: An event brought about by the occurrence of the specified hazard and that directly or indirectly causes an initiating event and may further cause safety system failures or operator errors that may lead to core damage or large early release. A hazard event is described in terms of the specific levels of severity of impact that a hazard can have on the plant. For example, an internal flood event would be expressed in terms of the specific flood source and its local impact, such as the resulting water levels in affected plant areas, or the extent of the area subjected to spray; a seismic event would be expressed in terms of spectral acceleration and associated spectral shape; a transient event would be expressed in terms of the plant systems affected by the event.

Hazard group: A group of similar hazards that are assessed in a PSA using a common approach, common methods, and common sources of likelihood data for characterizing the effect on the plant. Typical hazard groups considered in an NPP PSA include internal events, internal floods, seismic events, internal fires, high winds, external flooding, etc.

High confidence of low probability of failure (HCLPF) capacity: A measure of seismic margin. In seismic PSA, this is defined as the earthquake motion level at which there is a high (95%) confidence of a low (at most 5%) probability of failure, which is equivalent to the 1% mean probability of failure. Using the lognormal fragility model, the HCLPF capacity is expressed as: $Am*exp[-1.65\sigma_{\mathbf{R}} + \sigma_U)]$. The HCLPF can be evaluated deterministically using the CDFM approach.

High-energy line: A pipe or piping system component is classified as high energy if it contains water or steam at maximum operating temperature exceeding 94°C or maximum operating pressure exceeding 1.9 kPa.

High winds: Tornadoes, hurricanes (or cyclones or typhoons), extratropical (thunderstorm) winds, and other wind phenomena depending on the site location.

Hot short: Individual conductors of the same or different cables coming in contact with each other where at least one of the conductors involved in the shorting is energized resulting in an impressed voltage or current on the circuit being analysed.

Human error: Any human action that exceeds some limit of acceptability, including inaction where required, excluding malevolent behaviour. Failure of a human action to be completed as desired, resulting in an undesired condition. Human errors can be classified as either errors of omission or errors of commission. An error of omission would be failure to perform a system-required task or action. An error of commission would be incorrectly performing a system-required task or action, or performing an extraneous task that is not required and might lead to worsening the accident progression or cause an initiating event.

Human error probability (HEP): A measure of the likelihood that plant personnel will fail to initiate the correct, required, or specified action or response in a given situation, or by commission performs the wrong action. The HEP is the probability of the HFE.

Human failure event (HFE): A basic event that represents a failure or unavailability of a component, system, or function as the result of human error.

Human reliability analysis (HRA): A structured approach used to identify potential HFEs and to systematically estimate the probability of those events using data, models, or expert judgment.

Ignition frequency: Frequency of fire occurrence generally expressed as fire ignitions per reactor-year.

Ignition source: Piece of equipment or activity that causes fire.

Initiating event: An event that perturbs the steady state operation of the plant and could directly lead to undesirable end state and/or radioactive material release or could degrade the reliability of a normally operating system, cause a standby mitigating system to be challenged, or require that the plant operators respond in order to mitigate the event or to limit the extent of plant damage caused by the initiating event. These events include human-caused perturbations and failure of equipment from either internal hazards or external hazards (see *Hazards (Internal)* and *Hazards (External)*). An initiating event is defined in terms of the change in plant status that results in a condition requiring shutdown or a reactor trip when the plant is at power, or the loss of a key safety function for non-power modes of operation.

Initiator: See *initiating event.*

Intensity: A measure of the severity of a *hazard.*

Interfacing systems loss of coolant accident (ISLOCA): A LOCA that bypasses the containment when a breach occurs in a system that interfaces with the RCS at a location outside the containment and the breach either cannot be or is not isolated.

Internal events: The subset of i*nternal hazards* that are initiating events resulting from random mechanical, electrical, structural, or human failures. By historical convention, LOOP is considered to be an internal event, except when the loss is caused by an external hazard that is treated separately (e.g. seismically induced LOOP).

Internal fire event: An event brought about by the occurrence of a fire within the plant boundary, and which directly or indirectly causes an initiating event and may further cause safety system failures or operator errors that may lead to core/fuel damage or large early release. Internal fire events are generally defined in terms of location, ignition source, heat release rate profile, and extent of propagation.

Internal hazards. See *Hazard (Internal)*

Key safety functions: The minimum set of safety functions that must be maintained to prevent an undesirable end state and/or a radioactive material release. The specific set of safety functions necessary to prevent each release category is reactor specific, but include: (i) *control of reactivity*, (ii) *cooling of radioactive material* (i.e. removal of heat from the reactor and from the fuel store) and (iii) *confinement of radioactive material* (including shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases).

Key source of uncertainty: A source of uncertainty that is related to an issue for which there is no consensus approach or model and where the choice of approach or model is known to have an impact on the risk profile (e.g. CDF, the set of initiating events and event sequences that contribute most to the frequency of end states) or a decision being made using the PSA. Such an impact might occur, for example, by introducing a new functional event sequence or a change to the overall CDF estimates significant enough to affect insights gained from the PSA.

Low power: A POS (or set of POSs) during which the reactor is at reduced power, below nominal full power conditions. In these POSs, the power level may be changing as the reactor is shutting down or starting up, or the power level may be constant at a reduced level. The power level that distinguishes nominal full power from low power is the power level below which major plant evolutions are required to reduce or increase power that significantly increase the likelihood of a plant trip.

Master logic diagram: Summary fault tree constructed to guide the identification and grouping of initiating events and their associated sequences to ensure completeness.

'Mature' plant: A facility belonging to the family of similar facilities with long cumulative operational experience.

Mission time: The time period that a system or component is required to operate in order to successfully perform its function.

Mitigating structure, system, and component: An SSC that performs a function to mitigate the consequences of an event such as by protecting a barrier to radionuclide transport, performing a safety function, or limiting or preventing a release of radioactive material from a source.

Multicompartment fire scenario: A fire scenario involving targets in a room or fire compartment other than, or in addition to, the one where the fire was originated.

Mutually exclusive events: A set of events where the occurrence of any one precludes the simultaneous occurrence of any remaining events in the set.

Non-safety related SSC: Those SSCs that are (1) capable of performing a safety function, (2) are modelled in the PSA to prevent or mitigate one or more event sequences, and (3) are not credited in the design basis-accident analysis.

Operating time: Total time during which components or systems are performing their designed function.

Outage: The entire set of POSs with the plant subcritical. This term is used interchangeably with the term “shutdown”

Outage types: Term used to describe the general cause of the plant being subcritical. Different outage types result from maintenance and refuelling requirements that necessitate different LPSD evolutions and resulting POSs. For example, a *refuelling outage* type may involve fuel movement operations, whereas a maintenance outage conducted to repair piping would be a different outage type.

Peak ground acceleration (PGA): Maximum value of acceleration displayed on an accelerogram; the largest ground acceleration produced by an earthquake at a site. As used in PSA, peak ground acceleration generally refers to the acceleration at zero period (i.e. “infinite” frequency” in the horizontal direction (see also *spectral acceleration).*

Per calendar-year: Units for the frequency of an initiating event, event sequence, undesirable end state or release category, the calculation of which includes contributions from each POS, taking into account the fraction of time spent in that POS, normalized to one calendar year.

Performance-shaping factor (PSF): A factor that influences HEPs as considered in a PSA’s HRA and includes such items as level of training, quality/availability of procedural guidance, time available to perform an action, etc.

Physical analysis units: The spatial subdivisions of the plant upon which an internal flood or fire analysis is based. The physical analysis units are generally defined in terms of flood or fire zones and/or fire compartments.

Plant: A general term used to refer to a nuclear power facility (for example, “plant” could be used to refer to a single-unit or a multiunit facility).

Plant configuration: Plant conditions including operating mode, reactor power and decay heat level, RCS conditions (e.g. temperature, pressure), RCS status (e.g. pressure boundary open or closed), reactor building status, fire and flood barrier status, equipment alignment (e.g. number of pumps operating, number of pumps in standby), and equipment in service or out of service for test and maintenance.

Plant damage state (PDS): The characteristics of the final state of an event sequence with respect to event progression, containment, confinement or reactor building status,, and mitigating system operability.

Plant evolution: A series of connected or related activities where the plant transitions from one POS to another, e.g. a transition from full power to low-power level, or shutdown, or changes to the plant conditions with various combinations of equipment out of service for maintenance.

Plant Operational Mode: A particular plant configuration with specified operational characteristics. See also *plant operating state.*

Plant operating state (POS): A standard configuration of the plant during which the plant conditions are relatively constant, are modelled as constant, and are distinct from other configurations in ways that impact risk. POS is used to discretize the plant conditions for specific phases of an LPSD evolution. Examples of such plant conditions include, e.g. core decay heat level, primary coolant level, primary temperature, primary vent status, reactor building status, and decay heat removal mechanisms.

Plant response model: A Boolean representation of the combinations of equipment, system, function, and operator failures or successes, of an accident that when combined with an initiating event can lead to undesired consequences, with a specified end state (e.g. release category).

Plant specific data: Data consisting of observed sample data from the plant being analysed.

Plant transition mode: See *transition modes (or transition states)*

Point estimate: Estimate of a parameter in the form of a single number.

Post-initiator human failure events: Human failure events that represent the impact of human errors committed during response to abnormal plant conditions.

Pre-initiator human failure events: Human failure events that represent the impact of human errors committed during actions performed prior to the initiation of an accident (e.g. during maintenance or the use of calibration procedures).

Prior distribution (priors): The prior distribution is a key part of Bayesian inference and represents the information about an uncertain parameter P that is combined with the probability distribution of new data to yield the posterior distribution, which in turn is used for future inferences and decisions involving P.

*Probabilistic safety assessment (PSA)**: A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk.

Probabilistic safety assessment (PSA) application: A documented analysis based in part or whole on a plant specific PSA that is used to assist in decision making with regard to the design, licensing, procurement, construction, operation, or maintenance of an NPP.

Probabilistic safety assessment (PSA) maintenance: The update of the PSA models to reflect plant changes such as modifications, procedure changes, or plant performance (data).

Probabilistic safety assessment (PSA) upgrade: The incorporation into a PSA model of a new methodology or changes in scope or capability that impact the significant event sequences. This could include items such as new human error analysis methodologies, new data update methods, new approaches to quantification or truncation, or new treatment of CCF.

Probability of exceedance: See *frequency of exceedance.*

Probability of non-suppression: Probability of failing to suppress a fire before target damage occurs.

Quantitative Health Objective(s): The term for numerical criteria for the acceptable levels of risk to public health and safety in the population surrounding NPPs that satisfy safety goals.

Raceway: An enclosed channel of metallic or non-metallic materials designed expressly for holding wires, cables, or bus bars.

Rare event: Event that might be expected to occur only a few times throughout the world nuclear industry over many years (e.g. $<10^{-4}$/reactor-year).

Reactor-year: A calendar-year in the operating life of one reactor, regardless of power level.

Recovery: Restoration of a function lost as a result of a failed SSC by overcoming or compensating for the failure.

Refuelling outage: An outage type that occurs on a periodic basis, during which a portion of the spent nuclear fuel is replaced with new (unburned) fuel.

Release category: The grouping of one or more event sequences based on common or similar *mechanistic source terms*. In this context, "similar" depends on the level of fidelity of the analysis and the number of release categories used to span the entire spectrum of possibilities within the scope of the PRA model. Similarity is generally measured in terms of the overall (cumulative) release of activity to the environment, the time at which the release begins, and (in certain applications) other physical characteristics of the source term.

Reliability: A performance attribute of an SSC defined as the probability the SSC successfully performs its safety function(s) over a specified mission time and in accordance with a set of specified success criteria; the complement of unreliability.

Repair: Restoration of a failed SSC by correcting the cause of failure and returning the failed SSC to its modelled functionality.

Repair time: The period from identification of a component failure until it is returned to service.

Response: A reaction to a cue for action in initiating or recovering a desired function.

Response spectrum: A curve calculated from an earthquake accelerogram that gives the value of peak response in terms of acceleration, velocity, or displacement of a damped linear oscillator (with a given damping ratio) as a function of its period (or frequency).

Risk: Frequency and consequences of an event, as expressed by the "risk triplet" that is the answer to the following three questions: (1) What can go wrong? (2) How likely is it? And (3) What are the consequences if it occurs?

Risk achievement worth (RAW) importance measure: For a specified basic event, RAW importance reflects the increase in a selected figure of merit (e.g. CDF) when an SSC is assumed to be unable to perform its function due to testing, maintenance, or failure. It is the ratio or interval of the figure of merit, evaluated with the SSC's basic event probability set to one, to the base case figure of merit, evaluated with the base case *basic event* probability.

Risk metrics: A measure that is used to express the risk quantity of interest.

Safe stable state: A plant state, following an initiating event, in which plant conditions are controllable at or near desired values and within the success criteria for maintenance of safety functions. A safe stable state is achieved when the following criteria are met:

- All required safety functions are successfully performed during the defined mission time

- The safety functions are not expected to be lost at a point close-in-time after the specified mission time (i.e. there is compelling evidence that the successful safety functions have adequate operating capacity to be maintained for an indefinite period following the end of the specified mission time, or that there are adequate alternative means of performing the safety functions that can be implemented with high confidence after the specified mission time). See also *cliff edge effect.*

Safe stable states correspond to successful plant response end states in the PSA modelling of event sequences.

Safety features: Design features of a reactor that are provided specifically to support one or more safety functions or to support another SSC that provides a safety function.

Safety features, engineered: Safety features applied in the design of reactor systems in addition to the selection of materials and design characteristics of the reactor fuel, reactor coolant, and moderator (if any) that support one or more safety functions. Engineered safety features may involve the use of active and/or passive SSCs.

Safety function: See *key safety function.*

Safety related SSC: Those SSCs that are (1) specifically designed to perform a safety function, (2) are designed to prevent or mitigate one or more event sequences and (3) are credited in the design basis-accident analysis.

Screening: A process that eliminates items from further analysis based on their negligible contribution to the probability of an event sequence or its consequences. Note that screened items may be retained in the PSA model with conservative screening frequencies or probabilities.

Screening criteria: The values and conditions used to determine whether an item is a negligible contributor to the probability of an event sequence or its consequences.

Secondary combustible: Combustible or flammable materials that are not a part of the fire ignition source that may be ignited if there is fire spread beyond the fire ignition source.

Seismic equipment list (SEL): The list of all SSCs that require evaluation in the seismic fragilities task of a seismic PSA.

Seismic Event: An event brought about by the occurrence of an earthquake, and which directly or indirectly causes an initiating event and may further cause safety system failures or operator errors that may lead to core/fuel damage or large early release. Seismic hazard events are generally defined in terms of peak ground acceleration and response spectrum at the site

Seismic response spectrum: A plot of a ground response parameter (for example, spectral acceleration or spectral velocity) that has an equal likelihood of exceedance at different frequencies.

Seismic source: A general term referring to both seismogenic sources and capable tectonic sources. A seismogenic source is a portion of the earth assumed to have a uniform earthquake potential (same expected maximum earthquake and recurrence frequency), distinct from the seismicity of the surrounding regions. A capable tectonic source is a tectonic structure that can generate both vibratory ground motion and tectonic surface deformation such as faulting or folding at or near the earth's surface. In a PSHA, all seismic sources in the site region with a potential to contribute to the frequency of ground motions (i.e. the hazard) are considered.

Severity: In the context of a hazard, severity refers to the level of potential impact on the plant from a specific manifestation of the hazard (i.e. hazard event). This is also sometimes referred to as the intensity, magnitude, energy, force or size of the hazard event.

Severity factor: Severity factor is the probability that fire ignition would include certain specific conditions that influence its rate of growth, level of energy emanated, and duration (time to self-extinguishment) to levels at which target damage is generated.

Shutdown: The collection of POSs during which the reactor is subcritical. This term is interchangeable with the term “outage.”

Significant basic event: A basic event that contributes significantly to the computed risks for a specific source of radioactive material, POS, and hazard group or the total integrated risk. It typically defined as any basic event that has an F-V importance greater than 0.005 or a RAW importance greater than 2. When alternative numerical criteria are used the reason for their selection need to be justified.

Significant contributor: Any discrete element of the PSA model whose contribution to total risk is greater than a specified value. The specified value depends on a given risk metric that may be expressed as the total integrated risk, or risk associated with a specified part of the risk model; (e.g. a specific source of radioactive material, POS, hazard group, event sequence, or release category).

Significant contributors can be any of these elements as they contribute to each other or to the total, or could be cutsets, basic events, initiating events, hazard events, or other such PSA element. For each specific case the criteria for significance need to be defined in terms of relative importance of the element comparing to overall results for a given risk metrics.

As a general rule, the summed percentage of significant contributors can be 95% and the individual contribution of any significant contributor can be 1% of the risk metric selected.

Significant cut set: One of the set of cut sets resulting from the analysis of a specific hazard group that, when rank-ordered by decreasing frequency, sum to a specified percentage of the risk metrics value (e.g. CDF) for that hazard group, or that individually contribute more than a specified percentage of the risk metrics. Typically, the summed percentage is 95%, and the individual percentage is 1% of the applicable hazard group. Cut set significance may be measured relative to overall risk metrics values or relative to an individual event sequence frequency of the applicable hazard group. For hazard groups that are analysed using methods and assumptions that can be demonstrated to be conservative or bounding, alternative numerical criteria may be more appropriate and, if used, need to be justified.

Significant event sequence: One of the set of event sequences included in a PSA model, defined at the functional or systematic level, that, when rank-ordered by decreasing frequency, contributes a specified percentage of the risk metrics value (e.g. CDF), or that individually contributes more than a specified percentage of the risk metrics value (e.g. CDF) or other risk metric calculated in the PSA. Depending on the context, significance may be measured in terms of the total integrated risk or for the risk associated with a specific source of radioactive material, POS, and hazard group. Typically the aggregate percentage for the set is 95%, and the individual event sequence percentage is 1%. For hazard groups that are analysed using methods and assumptions that can be demonstrated to be conservative or bounding, alternative numerical criteria may be more appropriate and, if used, need to be justified.

Significant plant operating state: One of the set of accident classes represented by a specific POS and hazard group that, when rank ordered by decreasing frequency, contributes a specified percentage of a specific risk metrics value (e.g. CDF) for that hazard group or that individually contributes more than a specific percentage of a specific risk metrics value (e.g. CDF) for that hazard group. Typically the summed percentage for the set is 95%, and the individual event sequence percentage is 1% of the applicable hazard group risk matric value (e.g. CDF).

Spatial interaction: An interaction between two or more systems, structures, or components that could cause an SSC to fail to perform its intended safety function. It is the physical interaction of a structure, pipe, distribution system, or other component with a nearby SSC credited in the PSA to perform a safety function that results in the loss of function of the impacted SSC. Spatial interactions can be induced by internal or external hazards.

Source term, mechanistic: A source term that is calculated using models and supporting scientific data that simulate the physical and chemical processes that describe the radionuclide inventories and the time dependent radionuclide transport mechanisms that are necessary and sufficient to predict the source term.

Source term: The characteristics of a radionuclide release at a particular location, including the physical and chemical properties of released material, release magnitude, heat content (or energy) of the carrier fluid, and location relative to local obstacles that would affect transport away from the release point, and the temporal variations in these parameters (e.g. time of release duration, etc.).

Spectral acceleration: Spectral acceleration, in general, given as a function of period or frequency and damping ratio (typically 5%), is equal to the peak relative displacement of a linear oscillator of frequency f attached to the ground, times the quantity $(2\pi f)2$. It is expressed in gravitational acceleration (g) or centimetres per second squared (cm/s^2).

Split fraction: A unitless quantity that represents the conditional (on preceding events) probability of choosing one direction rather than the other through a branch point of an event tree.

Standby system: A system that is not normally operating but is intended to be ready to operate upon demand.

Start-up: A POS during which the reactor power level is increased from low power to full power following a plant outage.

Station blackout (SBO): Complete loss of AC electric power to the essential and nonessential switchgear buses in an NPP.

Structure, system, and component, active: An SSC whose function depends on mechanical movement or an external input such as actuation signal, or supply of motive power. Example active SSCs include pumps, gas blowers, control rods, and relief valves.

Structure, system, and component, passive: An SSC whose function does not depend on mechanical movement or an external input such as actuation signal, or supply of motive power. Example passive SSCs include the RPV, RCPB, operation of rupture disks and mechanical safety valves, and dropping of control rods by gravity, when the SSC functions are accomplished without the need for any active SSCs.

Success criteria: Criteria for establishing the minimum number or combinations of systems or components required to operate, or minimum levels of performance per component during a specific period of time, to ensure that the safety functions are satisfied.

Success path: A set of systems and associated components that can be used to bring the plant to a stable hot or cold condition to achieve a safe stable state. (See *safe stable state.*)

Support system: A system that provides a support function (e.g. electric power, control power, or cooling) for one or more other systems.

System failure: Loss of the ability of a system to perform its function.

System time window: See *time available.*

Target: May refer to a fire damage target and/or to an ignition target. A fire damage target is any item whose function can be adversely affected by the modelled fire. Typically, a fire damage target is a cable or equipment item that belongs to the internal fire PSA cable or equipment list and that is included in event trees and fault trees for fire risk estimation. An ignition target would be any flammable or combustible material to which fire might spread.

Technical quality (PSA): The extent to which the technical characteristics of a PSA satisfy the required attributes to be used in risk informed decision making, as presented in this publication.

Time available: The time period from the presentation of a cue for human action or equipment response to the time of adverse consequences if no action is taken. This term is interchangeable with the term “time window” or “system time window” when used in HRA.

Time window: The time needed by operators to successfully perform and complete a human action. This term is interchangeable with the term “time available” and “system time window.”

Top event: Undesired state of a system in the fault tree model (e.g. the failure of the system to accomplish its function) that is the starting point (at the top) of the fault tree.

Transient combustible: Combustible materials that are not fixed in place or an integral part of an operating system or component. (Note that the term “component” as used in this definition is considered interchangeable with the terms “equipment” or “piece of equipment” as those terms are used in this publication.)

Transition: A change in plant configuration, for example, a change in plant configuration to prepare for refuelling.

Transition modes (or transition states): A set of plant conditions in which the plant configuration is changing between normal, full power heat removal to DHR via an RHR system. For a refuelling outage, transition states would include low power (shutdown, startup) and hot standby/shutdown.

Truncation value: The numerical cut-off value of probability or frequency below which results are not retained in the quantitative PSA model or used in subsequent calculations (such limits can apply to initiating event frequencies, event sequences/cut sets, system-level cut sets, and sequence/cut set database retention).

Unavailability: The probability that a system or component is not capable of supporting its function at a specified or random point in time including, but not limited to, the time it is disabled for test or maintenance.

Uncertainty: A representation of the confidence in the state of knowledge about the parameter values and models used in constructing the PSA.

Uncertainty analysis: The process of identifying and characterizing the sources of uncertainty in the analysis, and evaluating their impact on the PSA results and developing a quantitative measure to the extent practical.

Unreliability: The probability that a system or component will not perform its specified function under given conditions upon demand or for a prescribed interval of time, referred to as the mission time.

Variability: A measure of the spread of a data set.

Walkdown: Inspection of local areas in an NPP where systems and components are physically located to ensure accuracy of procedures and drawings, equipment location, operating status, installation characteristics and environmental effects or system interaction effects on the equipment that could occur during accident conditions.

ABBREVIATIONS

AC	alternating current
AGR	advanced gas-cooled reactor
ANS	American Nuclear Society
AOT	allowed outage time
AS	accident sequence
ASME	American Society of Mechanical Engineers
ATHEANA	a technique for human event analysis
ATWS	anticipated transient without scram
BDBA	beyond design basis accident
BDD	binary decision diagram
BWR	boiling water reactor
CANDU	Canada deuterium uranium
CCCG	common cause component group
CCDP	conditional core damage probability
CCF	common cause failure
CCI	common cause initiator
CCW	component cooling water
CDF	core damage frequency
CDFM	combined density factor model
CFDP	conditional fuel damage probability
CLERP	conditional large early release probability
CT	cooling tower
DBA	design basis accident
DBE	design basis earthquake
DC	direct current
DG	diesel generator

DHR	decay heat removal
ECCS	emergency core cooling system
EDG	emergency diesel generator
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
EPZ	emergency planning zone
ESF	engineered safety feature
ET	event tree
FDF	fuel damage frequency
FHA	fire hazard analysis (or assessment)
FMEA	failure modes and effects analysis
FT	fault tree
F-V	Fussell-Vesely (importance measure)
GA	general attribute
HAZOPS	hazards and operability study
HCLPF	high confidence of low probability of failure
HE	human error
HELB	high-energy line break
HEP	human error probability
HFE	human failure event
HMI	human machine interface
HPCI	high pressure coolant injection
HPECC	high pressure emergency core cooling
HRA	human reliability analysis
HRR	heat release rate
HTGR	high temperature gas cooled reactors
HVAC	heating, ventilation, and air-conditioning

I&C	instrumentation and control
IAEA	International Atomic Energy Agency
ICCDP	incremental conditional core damage probability
ICFDP	incremental conditional fuel damage probability
ICLERP	incremental conditional large early release probability
ID	identifier
IE	initiating event
IPSART	international probabilistic safety assessment review team
IRIDM	integrated risk informed decision making
ISI	in-service inspection
ISLOCA	interfacing systems loss-of-coolant accident
ISLOCA	interfacing system LOCA
LCO	limiting condition of operation
LER	licensee event report
LERF	large early release frequency
LOCA	loss of coolant accident
LOOP	loss of off-site power (also referred to as LOSP)
LPSD	low power and shutdown
LWR	light water reactor
MAGNOX	magnesium-aluminium alloy reactor
MCP	main coolant pump
MCR	main control room
MOV	motor-operated valve
MSIV	main steam isolation valve
MCDF	multiunit core damage frequency
MFDF	multiunit fuel damage frequency
NDE	non-destructive examination

NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
OBE	operating-basis earthquake
OOS	out of service
P&IDs	piping and instrumentation drawings (or diagrams)
PCS	power conversion system
PDS	plant damage state
PFM	probabilistic fractural mechanics
PGA	peak ground acceleration
PMF	probable maximum flood
PORV	pressurizer power operated relief valve
POS	plant operating state
PRA	probabilistic risk assessment
PSA	probabilistic safety assessment
PSF	performance-shaping factor
PSHA	probabilistic seismic hazard analysis
PWR	pressurized water reactor
QA	quality assurance
QHO	quantitative health objective
RAW	risk achievement worth (importance measure)
RBMK	high power channel type reactor (Reactor Bolshoy Moshchnosty Kanalny)
RCPB	reactor coolant system pressure boundary
RCS	reactor coolant system
RHR	residual heat removal
RI	risk informed
RI-ISI	risk informed in-service inspection

RLE	review level earthquake
RPS	reactor protection system
RPV	reactor pressure vessel
RRS	required response spectrum
RRW	risk reduction worth (importance measure)
SA	special attribute
SAMG	severe accident management guideline
SAR	safety analysis report
SBO	station blackout
SCCDF	site complementary cumulative distribution function
SCDF	site core damage frequency
SEL	seismic equipment list
SFDF	site fuel damage frequency
SFR	seismic fragility analysis
SG	steam generator
SGSV	steam generator safety valve
SLERF	site early release frequency
SLOCA	small LOCA
SM	safety margin
SMA	seismic margins analysis
SORV	stuck open relief valve
SQRT	seismic qualification review team
SRCF	site release category frequency
SRT	seismic review team
SSA	safe shutdown analysis
SSC(s)	structure(s), system(s), and component(s)
SSE	safe shutdown earthquake

SSEL	safe shutdown equipment list
SSI	soil-structure interaction
STI	surveillance test interval
SW	service water
TECDOC	technical document
THERP	technique for human error rate prediction
TS	technical specification
WWER	water moderated water cooled energetic reactor

CONTRIBUTORS TO DRAFTING AND REVIEW

Ahmed, S.	Karachi Nuclear Power Plant (KANUPP), Pakistan
Alzbutas, R.	Lithuanian Energy Institute (LEI), Lithuania
Amico, P.	Jensen Hughes, United States of America
Beltran, F	International Atomic Energy Agency
Berg, P.	Bundesamt für Strahlenschutz, Germany
Bucevicius, N.	State Nuclear Power Safety Inspectorate (VATESI), Lithuania
Cho, N.	Korea Atomic Energy Research Institute, South Korea
Cimesa, S.	Slovenian Nuclear Safety Administration, Slovenia
Coman, O.	International Atomic Energy Agency
Contri, P.	Ingeneria & Ricera SpA (ENEL), Italy
De Castro Silva, L.	Electrobras Electronuclear, Brazil
Dincu, D,	CNCAN, Romania
Fleming, K.	Karl N. Fleming Consulting Services, United States of America
Frisoni, L.	ENEL Ingegneria e Innovazione S.p.A.
Godinez, V.	Instituto de Investigationes Nucleares, Mexico
Harbachova, N.	Joint Institute of Power and Nuclear Research "Sosny", Belarus
Hellmich, M.	Bundesamt für Strahlenschutz (BfS), Germany
Hellstroem, P.	Swedish Regulatory Safety Authority, Sweden
Henneke, D.	GE-Hitachi, United States of America
Kanetsyan, G.	Nuclear and Radiation Safety Center (N&RSC), Armenia
Koreniak, A.	Department for Nuclear and Radiation Safety (Gosatomnadzor), Belarus
Kussman, H.	National Nuclear Regulatory Authority (NNR), South Africa
Kuzmina, I.	International Atomic Energy Agency

Lyubarskiy, A.	International Atomic Energy Agency
Martisauskas, L.	Lithuanian Institute of Energy, Lithuania
Navarro, N.	Audoridad Regulatoria Nuclear, Argentina
Nevmerzhytskyy, V.	Rovno Nuclear Power Plant, Ukraine
Nikitin, I.	Leningrad Nuclear Power Plant, Russian Federation
Parry, G.	Erin Engineering, United States of America
Pechenezhska, O.	Zaporozhye Nuclear Power Plant, Ukraine
Peinador-Veira, M.	European Commission Joint Research Centre, Belgium
Piagentini, A.	Ingeneria & Ricera SpA (ENEL), Italy
Preston, J.	Consultant, United Kingdom
Ravindra, R.	M.K. Ravindra Consulting, United States of America
Rebleanu, I.	National Commission for Nuclear Activities Control (CNCAN), Romania
Samokhin, G.	Scientific and Engineering Center for Nuclear and Radiation Safety, Russian Federation
Sargsyan, S.	Armenian Nuclear Power Plant (ANPP), Armenia
Shestakov, I.	JSC OKB Gidropress, Russian Federation
Siess, G.	National Centre for Nuclear Research, Poland
Simurka, P.	VUJE, Slovakia
Sopira, V.	Relko Ltd., Slovakia
Spitzer, C.	International Atomic Energy Agency
Staron, E.	National Atomic Energy Agency (PAA) Nuclear Safety, Poland
Stefanov, E.	Kozloduy NPP, Bulgaria
Suran, P.	VUJE, Slovakia
Szikszai, T.	Ri-Man Consulting, Hungary
Szoke, M.	EDF Energy, United Kingdom

Tokmachev, G.	Atomenergoproject, Russian Federation
Volkanovski, A.	Jozef Stefan Institute, Slovenia
Wells, P.	International Atomic Energy Agency
Yurkin, P.	International Atomic Energy Agency
Zhang, Q.	State Nuclear Power Technology Corporation (SNPTC), China

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

International Atomic Energy Agency
Vienna
ISBN 978–92–0–107316-7
ISSN 1011–4289