IAEA-TECDOC-1511

Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants

IAEA
International Atomic Energy Agency

July 2006

IAEA SAFETY 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, and also general safety (i.e. all these areas of safety). The publication categories in the series are **Safety Fundamentals, Safety Requirements** and **Safety Guides**.

Safety standards are coded according to their coverage: nuclear safety (NS), radiation safety (RS), transport safety (TS), waste safety (WS) and general safety (GS).

Information on the IAEA's safety standards programme is available at 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 P.O. Box 100, A-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 e-mail to Official.Mail@iaea.org.

OTHER SAFETY 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 and protection in nuclear activities are issued in other publications series, in particular the **Safety Reports Series**. Safety Reports provide practical examples and detailed methods that can be used in support of the safety standards. Other IAEA series of safety related publications are the **Provision for the Application of Safety Standards Series**, the **Radiological Assessment Reports Series** and the International Nuclear Safety Group's **INSAG Series**. The IAEA also issues reports on radiological accidents and other special publications.

Safety related publications are also issued in the **Technical Reports Series**, the **IAEA-TECDOC Series**, the **Training Course Series** and the **IAEA Services Series**, and as **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. Security related publications are issued in the **IAEA Nuclear Security Series**.

IAEA-TECDOC-1511

Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants

IAEA
International Atomic Energy Agency

July 2006

The originating Section of this publication in the IAEA was:

Safety Assessment Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

DETERMINING THE QUALITY OF PROBABILISTIC SAFETY ASSESSMENT (PSA) FOR APPLICATIONS IN NUCLEAR POWER PLANTS

IAEA, VIENNA, 2006
IAEA-TECDOC-1511
ISBN 92–0–108706–3
ISSN 1011–4289

Printed by the IAEA in Austria
July 2006

FOREWORD

Probabilistic safety assessment (PSA) of nuclear power plants (NPPs) complements the traditional deterministic analysis and is widely recognized as a comprehensive, structured approach to identifying accident scenarios and deriving numerical estimates of risks dealing with NPP operation and associated plant vulnerabilities. Increasingly, during the last years, PSA has been broadly applied to support numerous applications and risk-informed decisions on various operational and regulatory matters. The expanded use of PSA in the risk-informed decision making process requires that PSA possess certain features to ensure its technical consistency and quality.

This publication is aimed to further promote the use and application of PSA techniques in Member States. The publication provides a comprehensive list of PSA applications and describes what technical features (termed 'attributes') of a PSA should be satisfied to reliably support the PSA applications of interest. A consideration has been also given to the basic set of attributes characterizing a 'base case PSA' that is performed with the purpose of assessing the overall plant safety.

This publication can support PSA practitioners in appropriate planning of a PSA project taking into account possible uses of the PSA in the future. The publication can be also used by reviewers as an aid in assessing the quality of PSAs and judging the adequacy of a PSA for particular applications. In addition, it is also foreseen to use the publication to support the independent peer reviews conducted by the IAEA in the framework of the International Probabilistic Safety Assessment Review Team (IPSART) safety service.

The IAEA acknowledges the work of all of the participating experts and wishes to thank them for their valuable contribution to this publication. The IAEA would like to especially thank K. Fleming of Karl N. Fleming Consulting Services (USA), R. Gubler of Ingburo Dr. Reinhard Gubler (Switzerland), P. Hellstrom of Relcon (Sweden), A. Lyubarskiy of SEC NRS (Russian Federation), G. Parry of the US NRC (USA), and G. Schoen and R. Schultz of HSK (Switzerland), for the active support and effective contribution to the IAEA project on development of this TECDOC.

The IAEA officer responsible for the preparation of this publication was I. Kouzmina of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

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.

CONTENTS

1. INTRODUCTION

1.1. Background

To date, probabilistic safety assessments (PSAs) have been performed for the vast majority of nuclear power plants (NPPs) worldwide and are under various stages of development for most of the remaining NPPs. PSA provides a comprehensive, structured approach to identifying accident scenarios and deriving numerical estimates of risks. In addition to the traditional deterministic analysis, it is a powerful tool for identification of significant accident sequences[1] and associated plant vulnerabilities dealing with the design and operation of the plant. General guidance on performance and independent verification of the safety assessments for NPPs, both deterministic and probabilistic, is provided in the IAEA Safety Standards, e.g. in Ref. [1].

PSA is increasingly being used in many countries, in a complementary manner to the traditional deterministic analysis and defence-in-depth considerations, as part of the decision making process to assess the level of safety of nuclear power plants and to support various risk-informed applications. Regulatory bodies in many countries require that a PSA be performed for licensing purposes. PSA has reached the point where, if performed to acceptable standards, it can considerably influence the design and operation of nuclear power plants. The quality of PSA is then becoming a matter of the 'robustness' of the decisions.

In order to promote the use and application of PSA techniques in Member States, the IAEA has developed detailed technical guidance on how to carry out PSA for nuclear power plants. There are publications describing the overall process and procedures of performing a PSA (see Refs [2-4]). For specific PSA areas or tasks where it was felt that more detailed guidance is needed, separate publications have been produced, such as for common cause failure (CCF) modelling (see Ref. [5]) or human reliability analysis (HRA) (see Ref. [6]). The publications provide information and recommendations and reflect accepted practices consistent with the knowledge at the time they were written. Reference [2], for example, provides procedures for conducting Level-1 PSAs for internal events for full power initial conditions in accordance with the state of the art of PSA in the beginning of nineties. That publication has been successful in helping to standardize the framework, terminology, content and format of documentation of PSAs in IAEA Member States, while providing for flexibility to introduce new and alternative methods.

Increasingly, during the last years PSA has been broadly applied to support numerous applications, such as risk-informed changes to technical specifications, risk-based plant configuration control, maintenance program optimization, etc. The IAEA has developed a technical document (see Ref. [7]), which summarizes information on up-to-date PSA applications and includes technical and methodological aspects, examples, and limitations, as well as the regulatory perspective on the use of PSA and numerical goals and acceptance criteria for decision making. A number of applications require specific features of the PSA and of certain PSA elements. A Technical Committee meeting, held in Vienna, May 28–June 1, 2001, on quality and consistency of PSAs identified the need for guidance on a

[1] In this publication, it is assumed that the user will define an objective criterion to identify what is a significant accident sequence. An example of such a criterion is the following: a significant accident sequence is one of the set of sequences, defined at the functional or systemic level, that, when ranked in decreasing order of frequency, comprise a significant percentage (e.g. 95%) of the core damage frequency (CDF), or that individually contributes more than a measurable percentage (e.g. 1%) to CDF.

process to review a PSA to determine its *technical adequacy* for addressing specific applications, or in other words, to provide guidance to assure that a PSA is of sufficient quality to support the application. The same idea was highlighted at the Conference on Topical Issues in Nuclear, Radiation and Radioactive Waste Safety (IAEA, September 2001) that emphasized the necessity to ensure a high quality of PSAs for the support of risk-informed decision making. The meaning of 'high quality' in this context was meant to be different for each PSA and to be defined as being commensurate with the intended use of a PSA. The present publication is a response to those recommendations.

The publication takes into consideration the advanced worldwide experience in the area of PSA quality assessment and verification, and in particular the ASME Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications (Ref. [8]). The starting point for the development of the technical attributes presented here in Sections 4 through 12 as the basis for the assessment of technical adequacy of a PSA was the set of requirements for the Capability Category II PSA presented in the ASME Standard (Capability Category II requirements are representative of currently accepted good industry practices in the USA.)

1.2. Objectives of the report

Various applications of PSA require that PSAs used to support those applications have certain characteristics in terms of their scope, degree of detail, technical adequacy of the modelling, the capability and flexibility to perform the required calculations, the capability to support interpretation of the results, the quality and type of the data used, and of the 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 the 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 quality of the PSA used to support an application as discussed in the next section. General attributes are formulated for a 'base case PSA' that in the framework of this publication is defined to be that PSA that is used to assess the overall plant safety level. Special attributes are provided for specific applications where appropriate.

The notion of 'PSA quality' should be distinguished from the notion of 'quality assurance'. 'PSA quality' for a specific purpose 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 quality assurance programme needs to be established that also addresses applications of PSA. How to set up and effectively apply an appropriate quality assurance programme for PSA and its applications is described in the publication 'A framework for a quality assurance programme for PSA', IAEA-TECDOC-1101, Ref. [9]. As distinct from that publication, the present TECDOC focuses on the technical information regarding approaches, methodology and data to obtain appropriate technical PSA features for specific applications. Thus, for a specific PSA application with a particular PSA, the approach provided in the publication can be used as a basis to formulate a specific technical framework for carrying out the PSA application. For these reasons this publication concentrates on technical PSA aspects. In Figure 1 the overall framework for the assurance of the quality of PSA results for 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 the PSA-related services and International Probabilistic Safety Assessment Review Team (IPSART)

missions being conducted by the IAEA on request of Member States, in addition to the existing guidelines, i.e. Ref. [10].

1.3. Quality of a PSA for an application

For the purposes of this publication, PSA quality is defined in general terms in the following way:

"In the context of an application, the PSA is of an appropriate quality if it conforms to a set of attributes that are appropriate for the application."

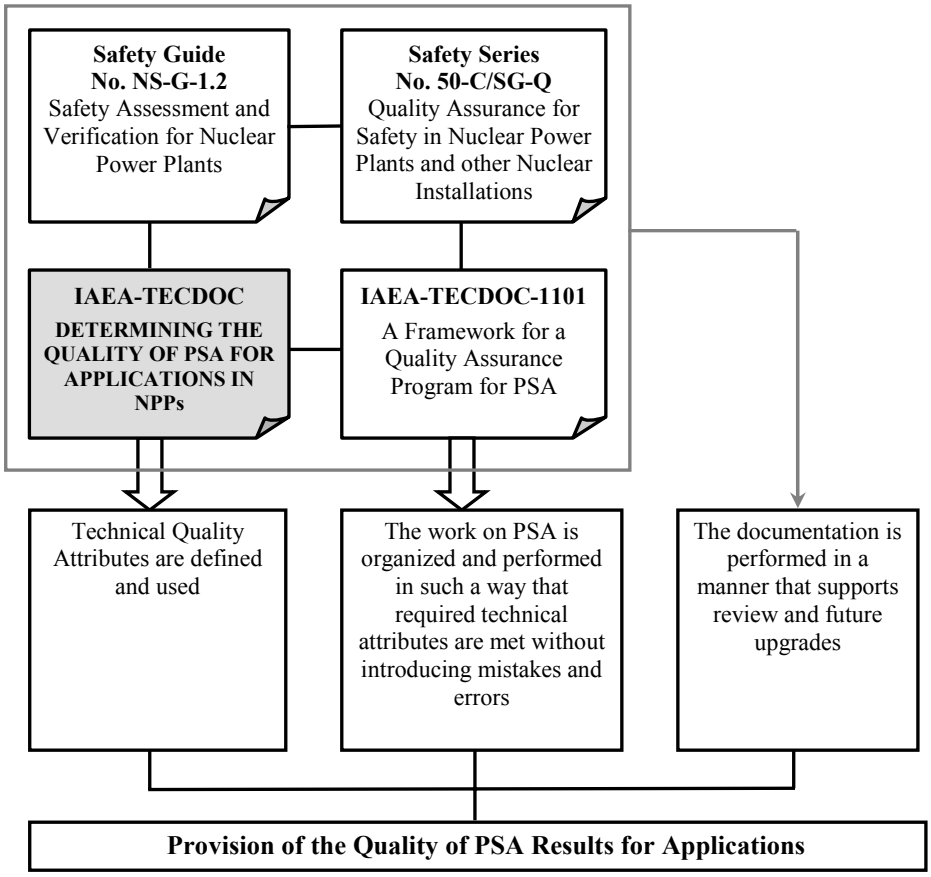

Fig. 1. Framework of PSA quality and supporting IAEA publications.

The key to defining quality then is 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 with which the PSA results are to be compared. The acceptance criteria are generally in the form of a numerical value associated with a specific metric. Examples of metrics are the absolute value of, or increase in, core 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. However, the method for performing the comparison of the results of the PSA with the criterion also has an impact on the attributes required. For example, the criterion may require use only of a mean value, or it may require the full characterization of uncertainty as a probability distribution on the value of the metric. Thus identifying the additional attributes requires an understanding of the method proposed for generating and using the PSA results.

Two types of attributes are defined in this publication:

- ***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 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 Ref. [10], "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 good 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. Special attributes are defined in such a way that, when they are met, the corresponding general attributes will certainly be met. Different PSA applications may require different special attributes.

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.

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 and more plant-specific PSA 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 are needed to perform the analysis of core damage resulting from internal hazards, such as internal fires and floods, or external hazards, such as earthquakes, high winds, etc., and from different plant operating modes, such as low power and shutdown modes. These specialized analyses are identified in

this publication as being separate modules[2] of a PSA. The scope of a PSA is defined by the modules it contains.

Which attributes are met determines to some extent the role the PSA can play in the 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 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.

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 should 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 of the report

The detailed IAEA PSA procedures mentioned above (Refs [2-4]) 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. It should be also mentioned that a number of approaches and techniques described in these procedures, in particular in the Level-1 PSA procedure (see Ref. [2]), have been further developed, so the present publication takes into account the current state of the art regarding various aspects related to PSA methodologies.

In recognition of the different levels of maturity in the state of the art for the various PSA modules, and due to a comprehensive amount of information to be covered, the scope of this publication is restricted to a Level-1 PSA for at power operation for internal events caused by random equipment failures and operator errors. Consideration is not given to other sources of radioactivity except for the reactor core. Level-2 PSA, internal fires and floods, external hazards like earthquakes, tornadoes, and other natural and man-induced hazards are not included in the scope of this publication, and neither is PSA for the shutdown and low power operation modes. These PSA modules could be covered in separate publications later. However, it should be specifically pointed out that applications may require that the scope of the PSA is complete in terms of consideration of all relevant contributors to plant risk and analysis levels. It is not the intent of this publication to address what has to be done to compensate for the limited scope of the PSA in these circumstances. 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.

An emphasis is made on describing the attributes of a ‘base case PSA’ being fundamental 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

[2] A PSA module is a probabilistic safety analysis, which addresses a certain type of hazard (e.g. high winds, earthquakes, internal fires), plant operating mode (full power, low power, shutdown), radioactivity source (reactor core, spent fuel pool), and analysis level (Level-1, Level-2, Level-3).

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.

1.5. Structure of the report

Because this report is oriented towards supporting applications of PSA, first, an overview of current applications is given in Section 2. Section 3 introduces the main PSA elements, and provides a description of the process one should follow to determine whether the PSA is of an appropriate quality for an application of interest. The attributes of the PSA elements are provided in Sections 4 through 12 separately for each PSA element, covering both general attributes (applicable for the 'base case PSA'), and application-specific ones (i.e. special attributes). Section 13 discusses the 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 14. 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 use of PSA models to support specific applications, and examples. Appendix III presents a table linking the PSA elements discussed in Sections 4 through 12 to the list of PSA tasks from the IAEA Procedure Guide on Level-1 Internal Event PSA (see Ref. [2]).

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, for example.

2. The publication focuses on PSA and PSA attributes for vessel type light water reactors (LWRs), although a 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 with other reactor types is discussed below.

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 lifetime is discussed below.

1.6.1. Applicability for reactors other than vessel type LWRs

The present predominant reactor types for nuclear power plants 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 LWRs. Most of the PSA approaches and techniques can also be applied and used for other reactor types such as gas cooled reactors and CANDU (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 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, parts of the core or may extend to the entire core. Accordingly, several Level-1 fuel or core 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 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 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 damage categories requires interpretation and adaptation regarding the description of PSA tasks and associated attributes as given in this publication.

It should be pointed out however 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 should be regarded as being still under development.

1.6.2. Applicability for NPPs in different stages of the plant's lifetime

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 in 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 the full range of PSA techniques can be applied including evaluation and use of 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 on thermal hydraulic analyses, accident progression, accident scenarios might be limited.
- Completeness of initiating events is difficult to ascertain.
- Limited information on man-machine interface (MMI) and on training of operating staff is available.
- Limited information on maintenance practices and procedures.
- Equipment location information is limited or missing (important for CCF modelling and modelling of secondary effects).
- Details on technical specifications (TSs) are missing or limited.

In summary, a considerable number of attributes which 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 variabilities 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 nineties, 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 (see Ref. [7]), published in 2001, identified a number of PSA applications. In this publication, some additional applications have been identified, 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 evaluation:** to provide support for design evaluation
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 design, hardware, 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 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. Typically, used metrics are importance measures, core damage frequency (CDF), large early release frequency (LERF), conditional core damage probability (CCDP), quantitative health objectives (QHO), etc. The metrics most commonly used are defined in Appendix I. Although analysis of the LERF and the QHO typically are not in the scope of a Level-1 PSA (and this publication), these metrics can be derived and used in the decision making process in many PSA applications and therefore for the sake of completeness are also addressed in Appendixes I and II of this publication. It should be noted that some PSA applications require a wider PSA scope, e.g. emergency planning would require in principle a full-scope Level-3 PSA. The PSA scope and metrics used in decision making provide an input to the definition of application-specific PSA quality requirements. In the decision making process the evaluated metrics are compared against some decision criteria that need to be established. The various forms that such decision criteria can take are discussed elsewhere (e.g. see Ref. [7]).

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 against assumed terrorist attack scenarios
2. DESIGN EVALUATION		2.1 Application of PSA to support decisions made during the NPP design (plant under design) 2.2 Assessment of the safety importance of deviations between an existing plant design and updated/revised deterministic design rules
3. NPP OPERATION	3.1 NPP maintenance	3.1.1 Maintenance program optimization 3.1.2 Risk-informed house keeping 3.1.3 Risk-informed support for plant ageing management program
	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 program 3.3.2 Improvement of maintenance personnel training program 3.3.3 Improvement of plant management training program
	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
4. PERMANENT CHANGES TO THE OPERATING PLANT	4.1 Plant changes	4.1.1 NPP upgrades, back-fitting activities and plant modifications 4.1.2 Lifetime 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 optimisation of TS 4.2.3 Determination and evaluation of changes to surveillance test intervals 4.2.4 Risk-informed in-service testing (IST) 4.2.5 Risk-informed in-service inspections (RI-ISI)
	4.3 Establishment of graded QA program for SSC	4.3.1 Equipment risk significance evaluation 4.3.2 Evaluation of risk impact of changes to QA requirements

Application Category	Application Group	Specific Application
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
	6.2 Regulatory decisions	6.2.1 Long term regulatory decisions 6.2.2 Interim regulatory decisions

3. PROCEDURE TO ACHIEVE QUALITY IN PSA APPLICATIONS

This section is devoted to the description of the general approach for the presentation of information in the 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 quality.

3.1. PSA elements and attributes

The PSA features (termed 'attributes' in this publication) are provided for the nine PSA elements that comprise an internal events, at-power, Level-1 PSA. The PSA elements identify the major analysis areas. It should be noted that while the nine PSA elements are identified, this division is to some extent arbitrary because all the analysis areas are interconnected and influence each other.

The PSA elements and associated abbreviations used in this publication are the following:

1.	Initiating Events Analysis	IE	(Section 4)
2.	Accident Sequence Analysis	AS	(Section 5)
3.	Success Criteria Formulation and Supporting Analysis	SC	(Section 6)
4.	Systems Analysis	SY	(Section 7)
5.	Human Reliability Analysis	HR	(Section 8)
6.	Data Analysis	DA	(Section 9)
7.	Dependent Failures Analysis	DF	(Section 10)
8.	Model Integration and Core Damage Frequency Quantification	MQ	(Section 11)
9.	Results Analysis and Interpretation	RI	(Section 12)

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.

The general and special attributes are defined as follows:

- *General attributes* describe the main features of the analyses, documentation, and data to be considered in the 'base case PSA'. These features are described based on the state of the art, as defined by generally accepted good practice, of a PSA constructed to evaluate the core damage frequency.

- *Special attributes* describe information on specific features of PSA elements to be satisfied in order that the PSA could be considered as appropriate for a specific application.

It is assumed that the general attributes characterise a contemporary state of the art Level-1 internal events at-power PSA performed with the aim to assess the overall NPP safety. Special attributes provide elevated capabilities within particular PSA elements to meet special features of PSA applications. Sections 4-12 present general and special attributes for

the nine 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 of 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 13 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

(1) 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'.

(2) 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 – an 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 PSA guidelines

The PSA elements #1 through 9 applicable to a Level-1 at-power internal event PSA are principally addressed in the IAEA Level-1 PSA Procedure Guide (see Ref. [2]). In order to provide a link between that publication and the present publication, a mapping of the PSA tasks from Ref. [2] to the PSA elements considered in this publication is provided in Appendix III.

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

- Human Reliability Analysis (Ref. [6])
- Initiating Events Analysis (Ref. [11])
- Dependent Failures Analysis (Ref. [5]).

3.4. The procedure for use of the TECDOC

This publication has two major uses:

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

(2) Support the use of PSA applications in planning of a PSA project, to make sure that appropriate quality of the Level-1 internal events PSA 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, a 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 4-12 characterizing a 'base case PSA' have been met. If not, refinements should be considered for the PSA to bring it in compliance with the general attributes. Alternatively, the developer could provide a supplementary justification 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 the special attributes needed for this PSA application have been met. Section 13 of this publication should be consulted regarding the practical steps for identification of a set of special attributes of the PSA elements relevant for the application of interest. A determination needs to be made whether the special attributes have been made. If not, refinements should be considered for the PSA to bring it in compliance with the special attributes.

The procedure for determination of quality of PSA for applications is illustrated in Figure 2. For Steps 2 and 3 depicted in the figure, this publication covers only a Level-1 internal events at-power PSA. In case a PSA includes more PSA modules (e.g. internal floods, fires, shutdown PSA, etc.), other publications should be consulted regarding the technical features of the analyses, e.g. Ref. [8] for internal floods, Ref. [12] for external hazards.

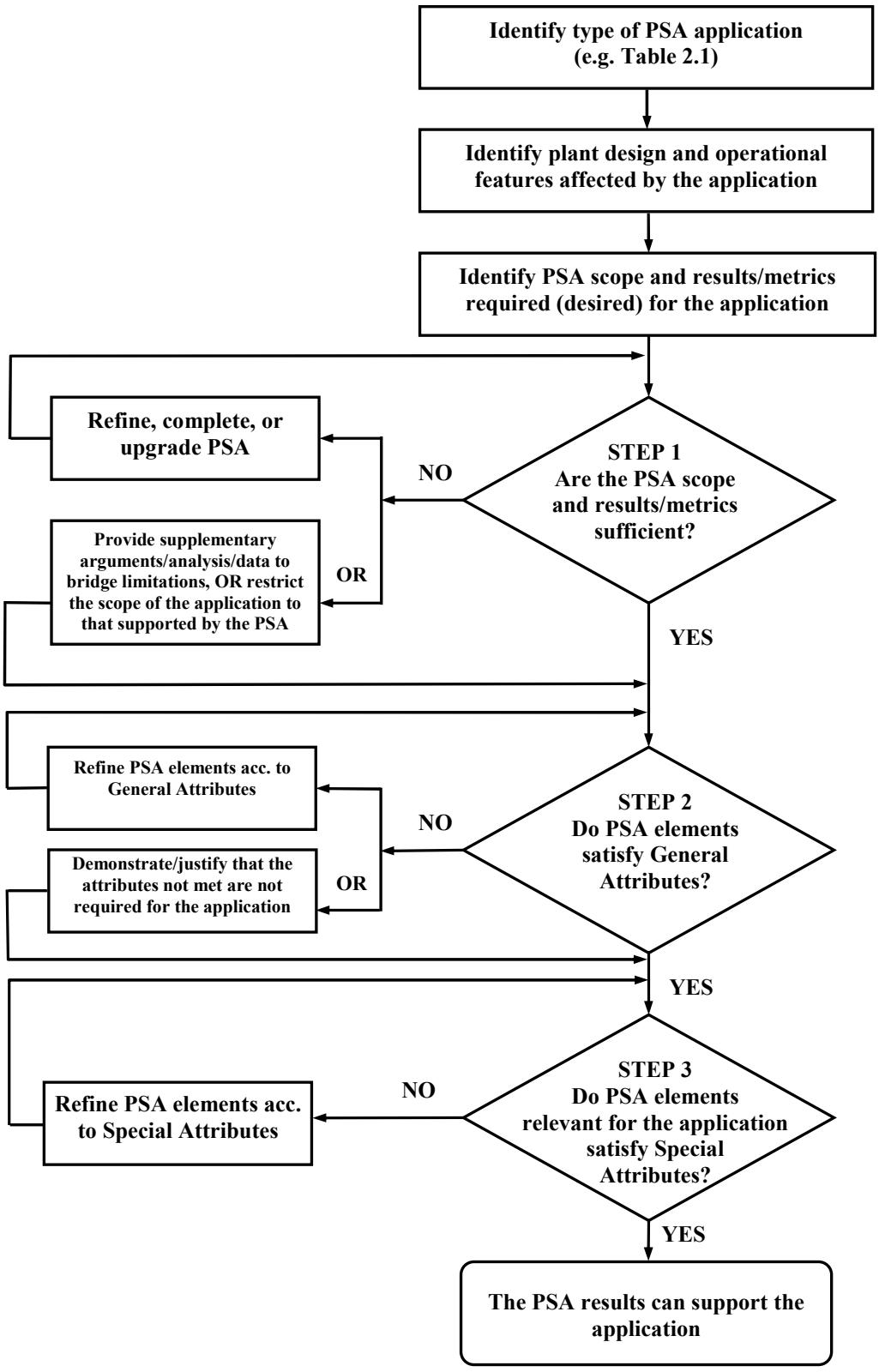

Fig. 2. General procedure for determination of quality of PSA for applications.

4. PSA ELEMENT 'IE': INITIATING EVENTS ANALYSIS

4.1. Main objectives

The initiating events analysis is a highly iterative, multi-purpose 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 a reasonably complete set of the events that interrupt normal plant operation and that require successful mitigation to prevent core damage, so that no significant contributor to core 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);
- 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.
- 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 system models (mainly refers to system initiators and includes checking system failures which may create an initiating event).
  - 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.

4.2. Initiating events analysis tasks and their attributes

The main tasks for the PSA element 'IE Analysis' are listed in Table 4.2. Tables 4.2-A through 4.2-H present the description of general and special attributes for these tasks.

Table 4.2 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	Handling the Effects of Plant Modifications
IE-G	IE Frequencies Quantification
IE-H	Documentation

Table 4.2-A Attributes for IE Analysis: Task IE-A 'Identification of IE Candidates'

Task / GA	Description 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 is defined which is as complete as possible.	
IE-A01	IE definition is clear and covers any plant disturbances that require mitigation to prevent core damage.	COMMENT: The following IE definition is generally used: "IE is an event which could directly lead to core damage or challenges normal plant operation and requires successful mitigation to prevent core damage". The initiating events identified typically include transients of various types, Loss of Coolant Accidents (LOCAs), interfacing systems LOCAs, steam generator tube ruptures, and support system initiators.
IE-A02	All plant operations modes with 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 nominal power level. EXAMPLES: At some plants (e.g. VVER-440 NPPs) the following differences related to plant power operation mode exist: 1) Event involving boron dilution due to erroneous connection of a disconnected loop is possible only at the level lower than nominal power. 2) Trip of 3 MCPs leads to reactor scram only at power level below 75% from nominal. 3) Trip of 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. 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	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. COMMENT: 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.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	applicable to the investigated unit. 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 effect analysis [FMEA]). 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 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 design basis accidents (DBAs) and beyond design basis accidents (BDBAs) are reviewed.	
IE-A04	Initiating events resulting from multiple failures 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 10.2-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 have been overlooked. Interview information from similar plants is also used.	RATIONALE: Interview of experienced plant personal may give additional knowledge on real plant behaviour and may help to identify IEs overlooked with the use of methods listed in IE-A03.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-A06	System or equipment failures or combinations of these are screened 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. (See also Table 10.2-D, Task DF-D). All system initiators that at the same time result in post-trip function failures are identified.	COMMENT: These types of events are known as common cause initiators or system initiators. 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. 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 alternate current (AC) or direct current (DC) busbars. Loss of auxiliary systems. Some failures within auxiliary systems may cause (or 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).

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	Special Attribute IE-A06-S1:	*Events caused by operator errors are identified and further evaluated.*	*RATIONALE: 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 error associated with the initiating event and those actions required to respond to the event.*
IE-A07	Events caused by equipment damage during on power refuelling process are considered as potential IEs.		COMMENT: Applicable for the plants with at-power refuelling (i.e. CANDU, RBMK, AGR, MAGNOX, vessel type heavy water reactor [Attucha]).
IE-A08	Initiating event precursors and run-back events (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 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-A09	Events that have occurred at conditions other than at power operation (i.e. during shutdown conditions) are identified and examined on the applicability for at power operation.		RATIONALE: The IEs have occurred at shutdown conditions may have a potential to occur at power operation. These events should be included in the list of IEs, unless it is justified that the IE cannot physically occur at power operation. However, the use of these events in data treatment should be made with care.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-A10	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. 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-A11	Multi-unit site initiators are identified and included in the list of IEs as 'Multi-units initiators'.	RATIONALE: An IE may be caused by system/equipment failures at another unit at 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. EXAMPLE: For the multi-units 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. COMMENT: Multi-units 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 4.2-C, General Attribute IE-C08).
IE-A12	The events dealing with failures of individual support systems (or trains) that can cause a plant trip are included in the list of IEs.	COMMENT: Failures of support system train(s) that may cause an initiating event should be included in the IE list in addition to the failure of whole system. If only the failure of whole support system is included in the IE list as a single most conservative event, the frequency of such events may be underestimated.
IE-A13	The list of potential initiating events is developed based on the results of the analyses within the task IE-A.	

Table 4.2-B Attributes for IE Analysis: Task IE-B 'IE Screening and Final IEs List Identification'

Task / GA	Description 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 identified events are subjected to a screening analysis in order to screen out events not applicable for the unit under consideration and to compile a final list of IEs.		
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 correspond to the accepted IE definition. 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 frequency of a significant accident sequence, and the event does not involve either an ISLOCA, containment 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 is not an immediate occurrence. That is, the event does not require the plant to transfer to shutdown conditions until sufficient time has expired during which the initiating event conditions, with a high degree of certainty (based on supporting calculations), are 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.
	Special Attribute 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 lead to an increase of 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 should be assessed by FT modelling, are identified (e.g. support system failures, CCI, etc.).		RATIONALE: Fault tree modelling allows to properly take into account support or auxiliary system dependencies and comprehensively account for different causal mechanisms to estimate IEs frequencies.
IE-B03	The final list of IEs is developed. All events, which were not screened out are included in the final list.		

Table 4.2-C Attributes for IE Analysis: Task IE-C 'IE Grouping'

Task / GA	Description 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 CDF (e.g. manageable number of accident sequence model and sufficient information for frequency estimation). The different IE groups are characterized by different impacts on plant performance, safety functions, and possibilities for recovery.		COMMENT: IEs are grouped in separate group if it is important for 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 is used). (See also Sections 5 and 6).		RATIONALE: Grouping can be performed only based on similarity of accident progression and success criteria of all event included in the group.
IE-C02	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 similar accident progression in terms of 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.		RATIONALE: Meeting of the required conditions ensures that any specific feature of the IE included in the group was not treated in optimistic manner and therefore no potential insights of the PSA are overlooked. COMMENT: Those IEs that have significantly different environmental impact or could have 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 are usually modelled as a separate groups.
	Special Attribute 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 realistic representation of plant response towards severe IEs with low frequency is required.*
	Special Attribute 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 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 pressurizer for SLOCA and only low pressure in pressurize for pressurizer leak).*

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
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 should 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 should be grouped differently. (See also IE-C02-S1.)	RATIONALE: This attribute helps to avoid excessive conservatism.
IE-C05	Each common cause initiator is 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 between several units are considered as separate groups.	RATIONALE: The capacity of mitigation systems may be significantly different when more than one unit is affected by the IE. EXAMPLE: Common cooldown system at VVER-440/230 could not provide efficient cooling if both units are put into shutdown conditions simultaneously.
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 separate groups unless the impact is bounded by the worst-case location.	EXAMPLES: 1) For some plants, where LOCA isolation is possible, LOCA in isolable and non-isolable parts can be considered. 2) For steamlines breaks outside and inside containment, the environmental conditions important for operation of other equipment may be significantly different.
IE-C08	A list of IE groups is compiled. A representative IE for further modelling of each IE group is 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 4.2-D Attributes for IE Analysis: Task IE-D 'Collecting and Evaluating Generic Information for IE Frequencies Assessment'

Task / GA	Description 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 IE frequencies assessment 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.
IE-D01	Generic information required for the IE frequency estimation is collected in order to account for a broader experience. Basically 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) Unit operating mode to which IE recorded is related 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 task IE-B. Generic information is traced to the primary source to avoid inadvertent double counting of information and to assure that no information from the plant is contained in the generic information. This is important from the viewpoint of consistent Bayesian updating. (See also Table 4.2-H, Task IE-H).	RATIONALE: Applicability of data from plants of different design should be investigated and boundaries of the IEs in the generic source should be compared with plant-specific IEs boundaries
IE-D02	The collection and evaluation of generic information include an understanding and assessment of the applicability and the 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 should be given on the possibility to apply Bayesian updating process.

Table 4.2-E Attributes for IE Analysis: Task IE-E 'Collecting of Plant-Specific Information'

Task / GA	Description 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 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.	
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, with the possibility to extract the following data: - number of IEs for each IE group; - number of precursors for the IEs; - number of run-back events; - unit operation mode; - duration of IE (e.g. for offsite power); - time period of data collection; - description of the event.	COMMENT: Duration of an IE may be important for estimation of frequencies of the IEs of certain duration (i.e. LOOP IE).
IE-E03	When system models for initiating events frequency assessment are used, the appropriate system information is collected. (See also Table 7.2-C, General Attribute SY-C08, and Table 10.2-D, Task DF-D).	

Table 4.2-F Attributes for IE Analysis: Task IE-F 'Handling of Effects of Plant Modifications'

Task / GA	Description 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	Differences between historical plant availability over the period of event occurrences in the plant database and present plant availability, which could be different from historical values, are accounted for.		
IE-F01	Collected information on plant-specific IEs is checked for whether the causes for the IEs are applicable for the actual plant conditions.		RATIONALE: If the plant changes make the IEs that happened in the past inapplicable to the actual plant state then the analysis of the impact of the changes and assessment of the hypothetical effect on the historical data to determine to what extent the data can be used should be performed.
IE-F02	Plant modifications/changes are evaluated in order to identify whether the precursors and run-back events happened in the past may cause an IE for the actual plant conditions.		RATIONALE: See IE-F01.
IE-F03	The rationale for screening or disregarding plant-specific data is justified (e.g. plant design modifications, changes in operating practices).		RATIONALE: See IE-F01.
IE-F04	The exclusion of earlier years that are not representative of current data is justified.		RATIONALE: This attribute helps to avoid excessive conservatism. Actual experience shows that during first years of plant operation a number of IEs significantly higher than after certain period.
	Special Attribute IE-F04-S1:	*Time trend analysis is used to account for established trends, e.g. decreasing reactor trip rates in recent years.*	*RATIONALE: Time trend analysis may be important for certain applications.* *EXAMPLE: Risk evaluation of the measures implemented with the aim to eliminate specific IEs.*
IE-F05	An analysis aimed to identify whether new IEs are introduced by plant modifications/changes is performed.		EXAMPLE: Replacement of analogue by digital I&C may lead to introducing of new IEs.

Table 4.2-G Attributes for IE Analysis: Task IE-G 'IE Frequencies Quantification'

Task / GA	Description 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	Frequency of individual IE and/or IE group is assessed based on relevant generic industry and plant-specific evidence. Where feasible, generic and plant-specific evidence is integrated using acceptable methods to obtain plant-specific IE frequency estimates. IE frequency estimation is accompanied by a characterization of the uncertainty.	
IE-G01	Initiating event frequencies are calculated taking into account the fraction of time the plant is at power.	RATIONALE: Use of calendar years for frequency estimation for the PSA at power operation leads to underestimation of the IE frequencies.
IE-G02	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-G03	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 should 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-G04	For extremely rare initiating events an engineering judgment is used, augmented with applicable generic data sources and specific analysis (e.g. structural 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.
IE-G05	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 reasonable 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 should be reconsidered regarding its applicability to the initiating event under consideration.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-G06	While using system models for initiating events frequency assessment the system models are modified in such a way that (See also Table 4.2-B, General Attribute IE-B02): - IE frequencies are quantified (rather than probabilities). - 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 CCF 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.	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-G07	Each system alignment and alignments of supporting systems 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.	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.
IE-G08	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 lead to significant increase of the event with leakage due to high probability that the second check valves is in the failed state.
IE-G09	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 can be calculated by partitioning of the total IE frequency taking into account the length of the pipelines inside and outside containment.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-G10	Plant-specific information is used in the assessment and quantification of recovery actions where available for IE frequencies estimation. These recovery actions should be 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 dependent on the site-specific external grid characteristics.
IE-G11	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.	See COMMENT for IE-G05.

Table 4.2-H Attributes for IE Analysis: Task IE-H 'Documentation'

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-H	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-H01	The following is 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. - The assumptions made to identify, screen out, and group IEs. - The list of IE groups and particular IEs assigned to. **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 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.).	COMMENTS: 1) IEs frequencies mean, median, 5% and 95% percentile should be assessed and documented. 2) Aging of the plant should be investigated for time trends.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
IE-H02	All the underlying data and information sources and analyses are documented and stored.		
	Special Attribute 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.*

5. PSA ELEMENT 'AS': ACCIDENT SEQUENCE ANALYSIS

5.1. 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 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 6 of this publication.
- End states are clearly defined to be either a core damage or successful prevention with the capability to support the interface between Level-1 and Level-2 PSA.

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.

5.2. Accident sequence analysis tasks and their attributes

Table 5.2 lists the main tasks for the PSA element 'AS Analysis'. Tables 5.2-A through 5.2-E present the description of general and special attributes for these tasks.

Table 5.2 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 5.2-A Attributes for AS Analysis: Task AS-A 'Selection of a Method and Provision of Related Tools for Accident Sequences Modelling'

Task / GA	Description 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 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.

Table 5.2-B Attributes for AS Analysis: Task AS-B 'Definition of Success and Non-Success End States and Key Safety Functions'

Task / GA	Description 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 the key safety functions that are necessary to reach a success end state are identified. Success and non-success end states are clearly defined. (See also Table 6.2-A, Task SC-A).		
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.). (See also Table 6.2-A, General Attribute SC-A01). All end states are identified as success or non-success; no end-state is undetermined.		RATIONALE: Undefined end-states prevent a useful interpretation of the results.
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. (See also Sections 6 and 7).		
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. (See also Table 6.2-A, General Attribute SC-A02).		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.
	Special Attribute 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 5.2-C Attributes for AS Analysis: Task AS-C 'Accident Sequences Progression Identification and AS Models Development'

Task / GA	Description 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 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.		
AS-C01	The end states of the accident sequences are achieved when either a 'non-successful' or 'stable successful' plant conditions have been reached.		COMMENT: '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. In case stable successful plant conditions for sequences are not achieved within 24 hours, a longer mission time is to be considered and/or additional plant equipment and human interactions are modelled. EXAMPLE: The possibility to remove heat via the secondary side using limited amount of water in the demineralised water tanks for approximately 24 hours should not be considered as a successful stable end state.
AS-C02	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 systems, the operability of which may impact the accident progression are accounted for.		
	Special Attribute AS-C02-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-C03	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 should be taken to remove conservatism with appropriate justification.
	Special Attribute AS-C03-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.*

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
AS-C04	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, training simulator exercises, and existing thermal hydraulic analyses. In case of alternatives, the most restrictive accident progression is modelled. (See also Table 8.2-E, General Attributes HR-E01, HR-E02, and Table 8.2-G, General Attribute HR-G04).		
	Special Attribute AS-C04-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.*
AS-C05	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, the failure of those human interactions is assumed or additional investigations are performed to assure the possibility to perform required actions (e.g. plant - specific thermal hydraulic analysis for specific sequences, interviews with plant operators, analysis of plant experience, simulator exercises, etc.) (See also Table 8.2-E, General Attributes HR-E01, HR-E02, and Table 8.2-G, General Attribute HR-G04).		RATIONALE: Optimistic crediting the human interactions not described in the emergency procedures may mask the problems in the emergency procedures. COMMENT: Emergency procedures may be less detailed than accident sequence models in the PSA.
	Special Attribute AS-C05-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 assure the possibility to perform required actions (e.g. plant -specific thermal hydraulic analysis for specific sequences, interviews with plant operators, 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-C06	If emergency procedures permit performing an action, but the realistic t/h analyses demonstrate that the action imposes an adverse effect, the ASs nevertheless include those actions. (See also Table 8.2-E, General Attributes HR-E01, HR-E02, and Table 8.2-G, General Attribute HR-G04).		RATIONALE: Unjustified optimism should be avoided in ASs modelling.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	Special Attribute AS-C06-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.).*	*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	The accident sequences possible for each initiating event group are developed. For each initiating event group, the accident sequences model is developed to a sufficient 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 11.2-A, General Attribute MQ-A01).
AS-C08	For each key safety function its dependence on the success or failure of preceding functions and the impact on accident progression are addressed.		EXAMPLE: The success of low pressure system injection is dependent on the success of RPV depressurisation.
AS-C09	When developing accident sequences, the phenomenological conditions created by the accident progression are identified so that the effect on potential mitigating systems is properly accounted for. (See also Table 10.2-C, General Attribute DF-C01).		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 equipment).
AS-C10	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-C11	Events for which time-phased dependencies might exist are defined and are included in ASs models appropriately.		EXAMPLES 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.
AS-C12	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.)
	Special Attribute AS-C12-S1	*ATWS sequences are modelled as part of accident sequence model for each IE group. Specific analyses justify the possibility to prevent core 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.*

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
AS-C13	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 transferred sequence is used. These include functional, system, initiating event, operator, and spatial or environmental dependencies.		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 transferred to subsequent event trees.
AS-C14	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 should 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 re-close of several valves.
	Special Attribute AS-C14-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. (See also Table 8.2-E, Special Attribute HR-E01-S1).*	*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-C15	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.
	Special Attribute AS-C15-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.*

Table 5.2-D Attributes for AS Analysis: Task AS-D 'Success Criteria for Accident Sequences'

Task / GA	Description 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. (See detailed attributes in Section 6).	

Table 5.2-E Attributes for AS Analysis: Task AS-E 'Documentation'

Task / GA	Description 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 treatment of each initiator and accident sequence model is documented to support reviews and applications. The following important aspects 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; - Sufficient 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.	
AS-E02	The interfaces between Accident Sequence Analysis and the following PSA tasks are defined and documented: - 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.	

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

6.1. 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. 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 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 HRA (Human Reliability Analysis), systems analysis, and success criteria formulation.

6.2. Success criteria formulation and supporting analysis tasks and their attributes

Table 6.2 lists the main tasks for the PSA element 'Success Criteria Formulation and Supporting Analysis'. Tables 6.2-A through 6.2-C present the description of general and special attributes for these tasks.

Table 6.2 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 6.2-A Attributes for Success Criteria Formulation and Supporting Analysis: Task SC-A 'Definition of Overall and Detailed Success Criteria'

Task / GA	Description 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 is performed in a manner which is consistent with plant features, procedures and operating practices.	
SC-A01	Definition of core 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. 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.	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 damage, and (2) Unsuccessful end-states with core 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.
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 sufficient margin is specified and used to take care of limitations of the computer codes, such as limitations in the sophistication of models, and uncertainties in the results.	EXAMPLES of parameters and associated acceptance criteria that are used in PSAs include: - BWR: Collapsed liquid level less than 1/3 core height or code-predicted peak core temperature > 2500°F (1370°C) - 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.
SC-A03	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.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SC-A04	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-A05	A mission time for the accident sequences is determined. The mission time is the time during which safety related functions are required to work to achieve a stable end-state after an initiating event. It is usual practice to assume as a first approach a general mission time of 24 hours. For sequences in which stable plant conditions would not be achieved by 24 hours using the modelled plant equipment and human interactions, a longer mission time is used if needed to achieve stable plant conditions. (See also AS-02). 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 by using techniques like: 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) 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.	

Table 6.2-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	Description 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 sufficient for the quantification of CDF, and the determination of impact of success criteria on systems, structures, components and human interactions are developed by appropriate thermal hydraulic analyses and other assessment means.		
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 FSAR or other conservative analyses applicable to the plant accompanied with a justification and an assessment of associated uncertainties.		
	Special Attribute 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.		
SC-B03	When defining success criteria, thermal hydraulic, structural, or other analyses and evaluations are used which are appropriate to the 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.		

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SC-B04	Analysis models and computer codes are used that have sufficient 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 sufficient resolution and 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, such as: 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 6.2-C Attributes for Success Criteria Formulation and Supporting Analysis: Task SC-C 'Documentation'

Task / GA	Description 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 of success criteria formulation and of the supporting analysis is carried out in a manner, which is fully traceable and allows changing and reproduction of the assessment if required by an application.	
SC-C01	Each of the success criteria and the supporting assessments, engineering bases, references and assumptions are documented in detail: - Conservative assumptions are described and documented including the rationale for using conservatism and an assessment of impacts. - 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. - 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.	
SC-C02	The uses, rationale and background information for expert judgment is documented in a way which is traceable and reproducible. Uncertainties and variabilities in expert judgment are stated. The impacts or effects of these uncertainties and variabilities are assessed as part of the Results Analysis and Interpretation Task. (See also Table 12.2-B, General Attribute RI-B02).	RATIONALE: Applications may require redoing expert judgments, partially or as a 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 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 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.	

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	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.	

7. PSA ELEMENT 'SY': SYSTEMS ANALYSIS

7.1 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 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.
- Intersystem dependencies and intra-system 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.

7.2. Systems analysis tasks and their attributes

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

Table 7.2 Main Tasks for Systems Analysis

Task ID	Task Content
SY-A	System Characterisation and System Boundary Definition
SY-B	Failure Cause Identification and Modelling
SY-C	Identification and Modelling of Dependencies
SY-D	Documentation

Table 7.2-A Attributes for Systems Analysis: Task SY-A 'System Characterisation and System Boundary Definition'

Task / GA	Description 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 sources are reviewed in order to: - 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 - Identify system configuration during normal and accident conditions - 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 analysed.

Table 7.2-B Attributes for Systems Analysis: Task SY-B: 'Failure Cause Identification and Modelling'

Task / GA	Description 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.	
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 7.2-A).	
SY-B02	Both normal and alternate system alignments are modelled.	COMMENT: 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.
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 Section 6. 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. EXAMPLE: (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; (c) success criteria for some systems are time-dependent.
SY-B04	The boundaries of the components required for system operation match the definitions used to establish the component failure data. This attribute complies also with General Attribute SY-C02 (Table 7.2-C).	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-B05	A systematic method is used for identification of component unavailability and failure modes.	EXAMPLE is the use of FMEA.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-B06	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-B13.		EXAMPLE of failure modes (not a comprehensive list): - active component fails to start; - active component fails to continue to run; - failure of a closed component to open; - failure of a closed component to remain closed; - failure of an open component to close; - failure of an open component 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[3].
	Special Attribute SY-B06-S1	*Leakages/ruptures of passive components are included in the model.*	*RATIONALE: Modelling of passive components failures (e.g. pipe segments) is useful for PSA applications dealing with optimization of ISI.*
SY-B07	The models include consideration to flow diversion as a result of component failures when the flow diversion is sufficient to 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 re-close. - Flow is diverted through spuriously open overpressure protection safety relief valve in the system.

[3] '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	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-B08	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: - 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. Restrictions on coincident unavailability of components/trains due to maintenance based on plant administrative practices such as Technical Specifications are addressed.		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 COMMENT: The coincident maintenance on two redundant trains, if permitted, may be an important risk contributor, and this possibility needs to be considered.
	Special Attribute SY-B08-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.*
	Special Attribute SY-B08-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.*
	Special Attribute SY-B08-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 modeled 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 modeled 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.*

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-B09	In the systems analysis, all human errors that cause the system or component to be unavailable when demanded are included (see Tasks HR-A through HR-C in Section 8).	EXAMPLE: An operator fails to restore a component to its correct state after maintenance and erroneous calibration. Task analysis is an example of a method that can be used to identify potential errors.
SY-B10	In the system model, operator errors that can occur during the operation of the system or components are included.	COMMENT: Operator errors need not be included in the system logic if they are already included in the accident sequence models where the relevant function of the system is modelled (see Tasks HR-E and HR-F in Section 8).
SY-B11	Component failures that would be beneficial to system operation are not included in the model.	EXAMPLE of a beneficial failure: A failure of an instrument in such a fashion as to generate a required actuation signal.
SY-B12	Credit is not taken for system or component operability beyond rated or design capabilities unless justified.	COMMENT: The information which could be used for justification includes: - test or operational data; - calculations; - vendor input; - expert judgment.
SY-B13	Contributors to system unavailability and unreliability (i.e., components and specific failure modes) may be excluded from the model if one of the following screening criteria is met: a) A component may be excluded from the system model if the total failure probability of the 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) One or more failure modes for a component may be excluded from the systems model if the contribution of them 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, or 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, or	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	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	d) It is shown that the omission of the contributor does not have a significant impact on the results. 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.	
	Special Attribute SY-B13-S1: *The basic event[4] screening process is revisited for certain applications.*	*RATIONALE: A checking will be needed to make sure that originally screened out events do not have an impact on application results.*
SY-B14	No credit is given to repair (recovery) of hardware faults, unless the feasibility of repair is justified.	
SY-B15	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.

[4] '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	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	Special Attribute SY-B15-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 systems.*
SY-B16	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: 1. Monitored, repairable (standby failure rate, repair time) 2. Periodically tested (standby failure rate, test interval) 3. Constant unavailability (probability) 4. Fixed mission time (operating failure rate, mission time) 5. Non repairable (standby failure rate)
	Special Attribute SY-B16-S1:	*Time-dependent failure models are used.*	*RATIONALE: Certain applications, e g test interval optimisation, require the use of time dependent models.*
SY-B17	The event naming scheme is developed in a consistent manner (see also Table 9.2-A, General Attribute DA-A02).		RATIONALE: Model manipulation and interpretation is facilitated by for example using the same designator for a component type and failure mode.

Table 7.2-C Attributes for Systems Analysis: Task SY-C 'Identification and Modelling of Dependencies'

Task / GA	Description 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 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.	
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.
	Special Attribute 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 should 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 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 (see Task SC-B in Section 6).	

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
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
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.
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.	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. COMMENT: 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.
	Special Attribute 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.*

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
SY-C08	The systems potential for causing a CCI is considered (see also Table 4.2-E, General Attribute IE-E03).	
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 with failure of containment 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	The locations of components vulnerable to environmental hazards that may impact system operation are identified.	
SY-C11	Spatial and environmental hazards 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.
SY-C12	Operator interface dependencies across systems or trains are considered where applicable. (See also Table 8.2-A, General Attribute HR-A02, Table 8.2-B, General Attribute HR-B01, Table 8.2-D, General Attribute HR-D04, and Table 8.2-G, General Attribute HR-G07).	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-C13	Intra-system common cause failures are modelled using an acceptable 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 Ref. [13] and Ref. [5].
SY-C14	Inter-system 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.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	Special Attribute SY-C14-S1:	*Inter-system common cause failures are considered.*	*RATIONALE: Consideration of inter-system 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 inter-system CCF may be the most important contributor to the function failure.*
SY-C15	Common cause component groups (CCCGs) are defined based on a logical, systematic justified process that considers similarity.		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 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 re-close after opening are treated by two CCCGs, one for each failure mode. EXAMPLE: 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.
	Special Attribute SY-C15-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.*

Table 7.2-D Attributes for Systems Analysis: Task SY-D 'Documentation'

Task / GA	Description 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 is 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 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	

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	- 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 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 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-D04	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.	

8. PSA ELEMENT 'HR': HUMAN RELIABILITY ANALYSIS

8.1. Main objectives

The objective of the human reliability analysis is to incorporate in the PSA model the impact of plant personnel actions on risk. The personnel actions considered are of two types: the first type includes those associated with the performance of surveillance testing, maintenance, and calibration, often referred to as pre-initiating event actions; the second 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 Safety Series No. 50-P-10 (Ref. [6]) are referred to as Type A and Type C human action events. When constructing models to estimate frequencies for the support system initiating events (Type B human action events), both types of actions are considered.

The important HRA topics are:

- The identification of the specific human activities whose impact should be included in the analysis;
- 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 supporting system reliability models (e.g. fault trees);
- 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 analyses on the above topics should 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. In addition, the dependency between the human failure events should be properly characterized and taken into account to ensure that the accident sequence frequency estimations are performed correctly.

8.2. Human reliability analysis tasks and their attributes

Table 8.2 lists the main tasks for the PSA element 'Human Reliability Analysis'. Tables 8.2-A through 8.2-I present the description of general and special attributes for these tasks.

Table 8.2 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
Documentation	
HR-I	Documentation

Table 8.2-A Attributes for Human Reliability Analysis: Task HR-A 'Identification of Routine Activities (Pre-initiating Event HRA)'

Task / GA	Description 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	The task includes a through identification of specific routine activities, 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 that require realignment of equipment from its normal operational or standby status are identified for those systems and components required to perform the functions required to respond to the initiating events modelled.	COMMENT: 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 should 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 contribution 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.
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 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. The procedures which allow detecting the faulty alignment or calibration are also reviewed.	EXAMPLES: incorrect calibration of steam generator level sensors; incorrect setting of torque switches.

Table 8.2-B Attributes for Human Reliability Analysis: Task HR-B 'Screening of Activities (Pre-initiating Event HRA)'

Task / GA	Description 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	The task is aimed at screening of activities that, on the basis of the plant practices, can be argued to result in a sufficiently low likelihood of failure.	COMMENT: This section refers to the screening of activities so that the potential human failures associated with them are not included in the PRA 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. Activities that result in multiple trains of a system being made unavailable during the course of the activity are analysed in more detail, since the probabilities are compared to common cause failure probabilities.	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: 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. COMMENT: Probabilities used for screening may be generated by application of simple HRA models, such as THERP (see Ref. [14]). (See also Table 8.2-D, General Attribute HR-D02).
HR-B02	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 are sufficient to 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 (see Ref. [14]). (See also Table 8.2-D, General Attribute HR-D02). EXAMPLES of defences 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-B03	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 miscalibration that is significant enough to 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 (see Ref. [14]).

Table 8.2-C Attributes for Human Reliability Analysis: Task HR-C 'Definition of Pre-initiator Human Failure Events'

Task / GA	Description 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 a human failure event 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, a human failure event is 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 should be included in the system models. 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.

Table 8.2-D Attributes for Human Reliability Analysis: Task HR-D 'Assessment of Probabilities of Pre-initiator Human Failure Events'

Task / GA	Description 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 reasonableness 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: An acceptable model for estimating HEPs is THERP (see Ref. [14]).
HR-D02	Screening values of the probabilities of the HFEs, based on a simple model of the general procedures for restoration, 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.
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-initiating event activities. The detailed assessment considers the specific aspects of the procedures and the man-machine interface.	RATIONALE: When the unavailability to reconfigure evaluated using a simple model is comparable with the probabilities of other modes of unavailability, a detailed assessment should be performed.
HR-D04	The degree of dependence between HFEs is assessed taking into consideration whether there are common elements in their cause.	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

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
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.
HR-D06	The reasonableness 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.
	Special Attribute 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 reasonableness of the estimates.*	*RATIONALE: A more complete investigation of the plant history can be obtained by looking through the plant maintenance records.*

Table 8.2-E Attributes for Human Reliability Analysis: Task HR-E 'Identification of Post-initiator Operator Responses'

Task / GA	Description 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 required for each of the accident sequences modelled is performed in a systematic way using appropriate information sources.		
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 as a function of the plant status represented in the development of the accident sequences. (See also Table 5.2-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 damage). - Actions required to change the status of components in order to fulfil a function required to prevent or mitigate core damage.		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.
	Special Attribute HR-E01-S1:	*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. 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 8.2-H, Task HR-H).* *EXAMPLE: Manual starts of a standby pump following failure of auto-start.*

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	Special Attribute HR-E01-S2:	*Significant errors of commission, i.e. actions that lead to additional functional unavailabilities, or inappropriately initiate system are identified.*	*RATIONALE: Errors of commission can lead to the creation of additional accident 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, Ref. [15]) 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 (Ref. [15]).* *EXAMPLE: An error of commission might be securing an injection system inappropriately.*
HR-E02	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. For the more challenging sequences, a detailed talk-through of the development of the sequences is performed (see also Table 5.2-A, General Attribute AS-C04).		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-E03	Simulator exercises are observed to gain a general understanding of crew dynamics, and the use of the procedures. For the more challenging accident sequences, simulator exercises are observed. Such exercises 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.		RATIONALE: An understanding of the performance shaping factors is important for the evaluation of the HEPs (see Table 8.2-F, Task HR-F, and Table 8.2-G, Task HR-G).

Table 8.2-F Attributes for Human Reliability Analysis: Task HR-F 'Definition of Post-initiator Human Failure Events'

Task / GA	Description 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	The task consists of the definition of human failure events that represent the failure to 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 function are identified and included in the plant logic model. Failures to perform more than one response are grouped into a single HFE, 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: - availability of cues and/or other indications for alerting the operators to the need for action; - the scenario specific procedural guidance; - time available for successful completion of response; - timing of cues relative to accident progression; - availability of systems, or components identified in the procedures; - the tasks comprising the required response.	COMMENTS: 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 8.2-G) can be satisfied.

Table 8.2-G Attributes for Human Reliability Analysis: Task HR-G 'Assessment of Probabilities of Post-initiator Human Failure Events'

Task / GA	Description 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 are performed using appropriate methodologies and data.	
HR-G01	Detailed assessment of the HEPs is performed for the significant HFEs (see Note). Screening values are used for the non-significant HFEs.	COMMENTS: 1) The identification of the significant HFEs is an iterative process requiring several quantifications of the PSA model. 2) 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 (FV) 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.
	Special Attribute 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-G07).
	Special Attribute 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 optimise EOPs and AMPs.*
HR-G03	The model used to assess the HEPs addresses the following performance shaping factors on a scenario and plant-specific basis: - the type (classroom or simulator) and frequency of training on the response; - the quality of the written procedures and administrative controls; - availability of necessary instrumentation; - degree of clarity of the cues/indications; - timing issues - time at which cues are received, time required to perform the response, and the time available to complete the response; - complexity of the tasks to be performed; - nature of the human-machine interface.	COMMENT: Many HRA models do not deal with each of these factors explicitly. However, they should be taken into account when comparing the relative values of HEPs (see HR-G6). 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	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	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: - environmental factors (e.g. heat, radiation, humidity); - accessibility of equipment to be manipulated; - need for special tools; - time to reach physically the place if not permanently occupied; - communication issues between MCR and local personnel.	
HR-G04	The timeline for occurrence of cues and the evaluation of the time available to complete the action is based on applicable generic studies (e.g. thermal-hydraulic analyses).	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 Special Attribute applies.
	Special Attribute HR-G04-S1: *The time line is based on plant-specific thermal-hydraulic analyses.*	
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, talk-throughs 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.
HR-G06	After estimation of the HEPs, the relative values are assessed to check that they are reflective of the impact of the various performance-shaping factors identified in HR-G03 above.	RATIONALE: This is a crucial attribute. Because of the lack of actuarial data, HEPs will always be uncertain. This must be taken into account when interpreting the results of the PSA. However, it is essential that the relative values of the HEPs be recognized as they can affect the relative risk significance of accident sequences, functions, systems, and components, which are important for many applications.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
HR-G07	The degree of dependence between HFEs appearing in the same accident sequence or cut set is assessed. Factors affecting the degree of dependence include: - use of common cues; - responses called for in the same procedure; - closeness in time of cues or required actions; - increased stress caused by failure of the first response. A conditional probability of the second, third, etc. event, given failure of the first, second, etc. is evaluated. The assumption of independence between HFEs is justified.	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.
HR-G08	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.

Table 8.2-H Attributes for Human Reliability Analysis: Task HR-H 'Recovery Actions'

Task / GA	Description 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	The task includes identification of additional recovery actions after the initial solution of the PSA model.	
HR-H01	Recovery actions that can restore the functions of systems or components are included on an as-needed basis to eliminate unnecessarily conservative contributions to 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 is available and operator training has been provided for the action OR it is considered to be a skill-of-the-craft 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, 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 – feasibility of the action is confirmed.	
HR-H03	The potential for dependency between recovery actions and any other HFEs in the accident sequence cutset 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.

Table 8.2-I Attributes for Human Reliability Analysis: Task HR-I 'Documentation'

Task / GA	Description 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 adequately performed.	
HR-I01	The HRA analysis is documented in enough detail to reproduce results and permit the reviewers to understand limitations imposed by the models, assumptions, and data. The specific aspects of the HRA to be documented include the following: – HRA methodology: • Approach used to identify HFEs • Methods used to estimate HEPs • Approach to the assessment of dependency – Basis for each HEP: • Screening values • Detailed HEP evaluations: - Factors used in the quantification of the HEPs - How they were characterized - How they were incorporated in the quantification	

9. PSA ELEMENT 'DA': DATA ANALYSIS

9.1. 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, or
- 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 mixed up with the parameters of probability distributions used to describe the uncertainty of reliability parameters.

9.2. Data analysis tasks and their attributes

Table 9.2 lists the main tasks for the PSA element 'Data Analysis'. Tables 9.2-A through 9.2-H present the description of general attributes and special attributes for these tasks.

Table 9.2 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	Handling of Reliability Parameters Affected by Plant Changes, Handling of New Equipment
DA-H	Documentation

Table 9.2-A Attributes for Data Analysis: Task DA-A 'Reliability Model Parameter Identification'

Task / GA	Description 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 in Section 7, Table 7.2-B (Failure Cause Identification and Modelling).	
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 offsite-power), (f) Failure to repair a component, system, or function in a defined time period.
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.	

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-A03	The parameters to be estimated and the data required are identified. The parameters identified and their characteristics are included in the database established under DA-A02.	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 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 9.2-B Attributes for Data Analysis: Task DA-B 'Component Grouping for Parameter Estimation'

Task / GA	Description 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 (e.g. motor operated pump, air-operated valve) and according to the detailed characteristics of their usage: 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 created under Task DA-A (Table 9.2-A).		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: A too narrow population in a group may lead to a sample of plant-specific data that is not statistically significant.
	Special Attribute 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 9.2-C Attributes for Data Analysis: Task DA-C 'Collecting and Evaluating Generic Information'

Task / GA	Description 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 in accordance with the parameter definitions of Task DA-A (9.2-A) and the grouping rationale of Task DA-B (Table 9.2-B) and evaluated regarding its applicability. Appropriate generic parameters are selected or parameters are composed for the plant from applicable generic sources.	
DA-C01	Generic information on failures and unavailabilities 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 those determined in response to Tasks DA-A and DA-B (Tables 9.2-A and 9.2-B respectively). 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. Generic information is traced to the primary source to avoid inadvertent double counting of information and to assure that no information from the plant itself is contained in the generic information in the case that the generic and the plant specific are combined under Task DA-E (Table 9.2-E). 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 understanding and 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	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
	Special Attribute 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.*

Table 9.2-D Attributes for Data Analysis: Task DA-D 'Plant-Specific Data Collection and Evaluation'

Task / GA	Description 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 of Task DA-A (Table 9.2-A) and the grouping rationale of Task DA-B (Table 9.2-B).	
DA-D01	Plant-specific data for the basic event/parameter population corresponding to that defined in Tasks DA-A (Table 9.2-A) and DA-B (Table 9.2-B) is collected. The following databases are created: (1) 'Failure database' containing failures, planned and unplanned maintenance and test events. (2) 'Success database' containing exposure to demands and, depending on the type of equipment, the exposure to standby and operation. These databases are linked to the equipment/basic event database.	
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 (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) All events that would have resulted in a failure to perform the mission as defined in the PSA are included as failures.	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.
DA-D04	The 'success database' 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.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
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.
	Special Attribute 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 database' 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.
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.
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 are counted which occurred during the particular plant status for which maintenance unavailability data is collected. Special attention is paid to the case of a multi-plant 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.		
DA-D10	Coincident outage times for redundant equipment (both intra- and inter-system) are identified and evaluated based on actual plant experience.		

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
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 offsite 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 offsite 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 Ref. [16]).

Table 9.2-E Attributes for Data Analysis: Task DA-E 'Derivation of Plant-Specific Parameters, Integration of Generic and Plant-Specific Information'

Task / GA	Description 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 acceptable 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 'child disease' effects.
	Special Attribute 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. Alternatively, 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.
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 reasonable 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 should be reconsidered regarding its applicability to the component and failure mode under consideration.

Table 9.2-F Attributes for Data Analysis: Task DA-F 'Derivation of Plant-Specific Parameters for Common Cause Failure Events'

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*		Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DA-F	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.		COMMENT: 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.
DA-F01	The Beta-factor approach or an equivalent method is used for CCF models and regarding the estimation of CCF parameters.		
	Special Attribute DA-F01-S1:	*The Beta-factor approach or an equivalent method is only used for an initial screening step with screening values for the parameters. For the finalized model, a model is used which allows a refined representation of failure combinations for higher order redundancies.*	*RATIONALE: Use of the Beta-factor model may masks-out intermediate failure combinations for equipment with more than two redundancies. For such equipment, the Beta-factor model does not provide a realistic description of CCF events.* *EXAMPLE of more detailed modelling:* *(a) Alpha Factor Model* *(b) Basic Parameter Model* *(c) Multiple Greek Letter Model* *(d) Binomial Failure Rate Model*
DA-F02	Generic common cause failure probabilities are used.		RATIONALE: Since CCF events are rare, uncertainties in estimates of CCF probabilities are relatively large. For many applications, the use of generic parameter values is acceptable, although the conclusions from the PSA need to be assessed for their robustness with respect to the uncertainty in the CCF probabilities.
	Special Attribute DA-F02-S1:	*Realistic common cause failure probabilities consistent with plant-specific design and operational practices, supported by plant-specific screening and mapping of industry-wide data is 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 (see Ref. [13]). Alternatively, an approach like the Partial Beta-factor is used which is, however, limited to the Beta-factor CCF model.*

Table 9.2-G Attributes for Data Analysis: Task DA-G 'Handling of Reliability Parameters Affected by Plant Changes, Handling of New Equipment'

Task / GA	Description 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	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 [see Tasks DA-B (Table 9.2-B), DA-C (Table 9.2-AC), and DA-D (Table 9.2-A)]. 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.	
DA-G01	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 (see also Table 9.2-E, General Attribute DA-E02).	

Table 9.2-H Attributes for Data Analysis: Task DA-H 'Documentation'

Task / GA	Description 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 is 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 sources of data; f) The time periods for which plant-specific data were gathered; g) Key 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; h) Justification for exclusion of any data; i) The basis for the estimates of common cause failure probabilities, including justification for screening or mapping of generic and plant-specific data; j) The rationale for any distributions used as priors for Bayesian updates, where applicable; k) Parameter estimates including the characterization of uncertainty as appropriate.		
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.		
	Special Attribute 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.*

10. PSA ELEMENT 'DF': DEPENDENT FAILURES ANALYSIS

10.1. 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
- Residual dependencies (common cause failures)

It should 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 10.1. 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 10.1 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	Initiating events analysis Accident sequence analysis Systems analysis Human reliability analysis

Dependence Type	Dependence Category	Analysis Procedure or Method	PSA Elements
Physical	Common environmental effects	Development of accident sequences Development of system models	Accident sequence analysis Systems analysis
	Dynamic effects	Physical analyses	Initiating events analysis (pipe breaks)
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

10.2. Dependent failure analysis tasks and their attributes

Table 10.2 lists the main tasks for the PSA element 'Dependent Failure Analysis'. Tables 10.2-A through 10.2-G present the description of general and special attributes for these tasks.

Table 10.2 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 10.2-A Attributes for Dependent Failure Analysis: Task DF-A 'Design Related Dependency Analysis'

Task / GA	Description 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).	

Table 10.2-B Attributes for Dependent Failure Analysis: Task DF-B 'Operations Related Dependency Analysis'

Task / GA	Description 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-initiating event 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. (See also Tasks HR-A through HR-C [Tables 8.2-A through 8.2-C]).	
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 (see HR-E and HR-F).	
DF-B04	The values of the HEPs used for the HFEs are appropriate for the plant-specific and scenario- specific conditions. (See also Tasks HR-D (Table 8.2-D) and HR-G (Table 8.2-G)).	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 dependence between HEPs appearing in the same cutset is assessed and the values changed as appropriate. (See also Table 8.2-D, General Attribute HR-D04, and Table 8.2-G, General Attribute HR-G07).	

Table 10.2-C Attributes for Dependent Failure Analysis: Task DF-C: 'Physical Dependency Analysis'

Task / GA	Description 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 (see also Table 5.2-C, General Attribute AS-C09, and Table 7.2-C, General Attributes SY-C09, SY-C10, SY-C11): 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 isolation wool material and blocking of the recirculation flow (post –LOCA).	RATIONALE: Physical effects can substantially reduce the mitigation possibilities.

Table 10.2-D Attributes for Dependent Failure Analysis: Task DF-D 'Common Cause Initiating Event Analysis'

Task / GA	Description 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. (See also Table 4.2-A, General Attributes IE-A04, IE-A06, and Table 4.2-E, General Attribute IE-E03).	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 10.2-E Attributes for Dependent Failure Analysis: Task DF-E 'Common Cause Failure Analysis'

Task / GA	Description 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 (see Tasks SY-C in Table 7.2-C and DA-F in Table 9.2-F).	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'.

Table 10.2-F Attributes for Dependent Failure Analysis: Task DF-F 'Subtle Interactions'

Task / GA	Description 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.		
	Special Attribute DF-F01-S1:	*Historical events that involve unusual dependent effects are reviewed to determine whether such occurrences can occur at the plant being analysed.*	*RATIONALE: A structured identification and consideration of subtle interactions may be needed for completeness purposes.* *COMMENT: So called subtle dependencies[5] 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.* *EXAMPLES: A list of subtle interactions can be found in NUREG-1150 (see Ref. [17]).*

[5] Subtle dependencies are also called 'system interactions' or 'subtle interactions'.

Table 10.2-G Attributes for Dependent Failure Analysis: Task DF-G 'Documentation'

Task / GA	Description 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.
	Special Attribute 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 analysed 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	For the CCI analysis, the following 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 the initiator frequency.		
DF-G04	For the physical dependency analysis, the following is documented: - Extensions to LOCA and transient categories - Refinements to accident sequence models of LOCAs and transients - Evaluation of containment sump operability.		

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
DF-G05	For the CCF analysis, the following is documented: - Identification and definition of CCCGs - All CCCGs and components included - Treatment of intra-system and intersystem CCFs - Models used - Special CCF events - CCF data - A description of how CCF is implemented in the overall PSA model.	

11. PSA ELEMENT 'MQ': MODEL INTEGRATION AND CDF QUANTIFICATION

11.1. 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 core damage frequency and to develop an understanding of the contributors to core damage model (see also Section 12). The following principles should 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.

11.2. Model integration and CDF quantification tasks and their attributes

Table 11.2 lists the main tasks for the PSA element 'Model Integration and CDF Quantification'. Tables 11.2-A through 11.2-D provide the description of general and special attributes for these tasks.

Table 11.2 Main Tasks for Model Integration and CDF 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 11.2-A Attributes for Model Integration and CDF Quantification: Task MQ-A 'Integrated Model'

Task / GA	Description 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 10 is performed.	
MQ-A01	All system models and accident sequences models are integrated to provide the logic structure of the PSA model. 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. In both cases, the conditions include the impact of the success or failure of functions or systems required prior to the function or system of concern, which has an impact on the success criteria, both in terms of the number of trains required and the timing for required functions or systems, which in turn affects the human reliability analysis appropriate to the event.	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. For these models, the use of a consistent naming scheme for the events and gates in the fault trees is essential. 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. COMMENT: Initiating events for which accident sequence are not developed, but that are assumed to lead directly to core damage should also be included in the integrated model. Examples that are sometimes undeveloped include ISLOCA, and reactor vessel rupture.
MQ-A02	For the fault tree linking approach, logic loops are cut in a manner that minimizes loss of information and does not produce ungrounded 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 (Ref. [18]) 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.

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
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 - 10.

Table 11.2-B Attributes for Model Integration and CDF Quantification: Task MQ-B 'Requirements on the Quantification'

Task / GA	Description 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 core damage (e.g. minimal cutsets) and the quantification of the core damage frequency 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 damage frequency.		
MQ-B03	For the fault tree linking approach, the final truncation value is justified by a sensitivity analysis demonstrating that the core damage frequency does not significantly change, if the truncation value is reduced.		COMMENT: A rule of thumb says that the truncation value should be 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.
	Special Attribute MQ-B03-S1:	*For the derivation of some importance lists (especially RAW) the truncation value is re-evaluated and justified. (See also Table 12.2-A, General Attribute RI-A03).*	*RATIONALE: If this is not done, several low-probability events might be excluded from the importance list whenever RAW is significant for the application.*
	Special Attribute MQ-B03-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 CDF rather than the total CDF.*	*COMMENT: Sensitivity tests should be conducted for the set of results of interest.*

Task / GA	Description of Task/General Attributes *Identifier and Description of Special Attributes (in Italics)*	Rationale/Comments/Examples for: General Attributes and *Special Attributes (in Italics)*
MQ-B04	Core damage frequency is evaluated as a mean value and the uncertainty distribution characteristics are provided, for the total CDF 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. 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-B05	When using logic flags (also designated as house events), the logic flag events should 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.

Table 11.2-C Attributes for Model Integration and CDF Quantification: Task MQ-C 'Review and Modification of the Results'

Task / GA	Description 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 as discussed below. 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.		
	Special Attribute 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. (See also Table 7.2-B, General Attributes SY-B02 and SY-B08).*	*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 and the degree of dependency assessed (see Table 8.2-D, General Attribute HR-D04, and Table 8.2-G, General Attribute HR-G07).		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	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 have reasonable likelihood of success assuming that trained and qualified personnel are performing the recovery action(s). (See also Task HR-H in Table 8.2-H).		

Table 11.2-D Attributes for Model Integration and CDF Quantification: Task MQ-D 'Documentation'

Task / GA	Description 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 is performed in a manner that facilitates peer review and future upgrades.		
MQ-D01	The following aspects of the model integration and CDF 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 CDF, each class of initiating events, and of significant core damage sequences; - the accident sequences and their contributing cut sets.		
	Special Attribute MQ-D01-S1:	*When only a fraction of the CDF is required to be analysed for an application, the documentation supports this analysis.*	

12. PSA ELEMENT 'RI': RESULTS ANALYSIS AND INTERPRETATION

12.1. 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 events, 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.

12.2. Results analysis and interpretation tasks and their attributes

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

Table 12.2 Results Analysis and Interpretation Tasks

Task ID	Task Content
RI-A	Identification of Significant Contributors
RI-B	Assessment of Assumptions
RI-C	Documentation

Table 12.2-A Attributes for Results Analysis and Interpretation: Task RI-A 'Identification of Significant Contributors'

Task / GA	Description 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 CDF are identified. The contributors are, in increasing level of resolution: - Initiating events - Accident sequences - Key safety function failures - System failures - Basic events The basic events include: - Equipment failures or unavailabilities - Common cause failures - Human failure events	
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.
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 PSA model rather than re-quantifying a pre-solved cutset list.	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 truncation value.

Table 12.2-B Attributes for Results Analysis and Interpretation: Task RI-B 'Assessment of Assumptions'

Task / GA	Description 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 key assumptions and model uncertainties is performed.	
RI-B01	Significant 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 significant 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 significant 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.
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. 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 12.2-C Attributes for Results Analysis and Interpretation: Task RI-C 'Documentation'

Task / GA	Description 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 of results is performed in a way that facilitates understanding of the technical basis for the significance of contributors.	
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.	

13. 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 elevated capabilities within particular PSA elements to meet special needs of PSA applications.

In order to indicate what specific features of PSA are needed for particular PSA applications, Tables 13.1 through 13.6 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 *essential special attribute* emphasises 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 special attribute may preclude meaningful use of the study for an intended application.

Supplemental special attributes 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 attribute 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 should 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 13.7 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.

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 13.7 for the set of identifiers of essential and supplemental special attributes relevant for the application.[6] If several applications are planned, the corresponding attributes have to be selected and considered jointly.

[6] In Table 13.7, the identifiers of essential special attributes are provided in bold underlined font. The identifiers of supplemental special attributes are provided in regular font.

STEP (3) Consult relevant information presented in Tables 13.1-13.6 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.[7]

STEP (5) Consult corresponding Sections 4-12 of the publication to get information on the content of the special attributes and the features of PSA elements needed to meet them.

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

Table 13.1 Safety Assessment

SA Identifier	Relevance to Specific Applications in the Category
Essential Attributes	
IE-F04-S1	The time trend analysis in relation to IEs provides important information for insights regarding the plant behaviour if changes in the number of specific events are observed at the plant (Application 1.2).
DA-E01-S1	A time trend analysis is important for the assessment of aging effects of the equipment and allows for gaining a realistic risk estimate for operating plant (Application 1.2).
Supplemental Attributes	
IE-H02-S1	The availability of information on IEs in the form of an electronic database is useful for periodic PSA updating, which is often part of the periodic safety review (Application 1.2).
IE-A06-S1	Explicit consideration of IEs caused by operator errors, especially those with severe consequences, helps to gain additional insights regarding the plant protection against malevolent acts (Application 1.3).
IE-B01-S1	Reconsideration of the events (especially those with severe consequences), which were screened out based on low frequency in the 'base case PSA', helps to gain additional insights regarding the protection of the plant against malevolent acts (Application 1.3).
AS-C02-S1	Plant-specific realistic thermal hydraulic analyses are useful to assure a realistic representation of the specific plant features influencing the accident progression (Application 1.2).
AS-C04-S1	Analysis of the defence against malevolent acts may be enhanced by a thorough consideration of possible mitigation strategies taking into account the impact of malevolent acts for Application 1.3.
AS-C12-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-C15-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 and 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 the differences or effects of changes (Application 1.2).
HR-G04-S1	The time windows for operator actions that are based on plant-specific thermal-hydraulic analyses provide a more realistic input in the HRA and thus promote getting plant-specific insights dealing with operator performance (Application 1.2).
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).

Table 13.2 Design Evaluation

SA Identifier	Relevance to Specific Applications in the Category
Essential Attributes	
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 (Application 2.1) or provides a better understanding of the deviations between an existing plant design and revised design-related rules (Application 2.2).
SY-C14-S1 SY-C15-S1	Consideration of inter-system common cause failures and more detailed modelling of CCF are important for realistic estimation of the plant risk for newly designed NPPs (Application 2.1); it provides also a better understanding of the deviations between an existing plant design and revised design-related rules (Application 2.2).
DA-F01-S1	Decisions on the number of redundancies and diversities to be included in the design require a detailed modelling of CCFs (Applications 2.1 and 2.2).
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).
Supplemental Attributes	
IE-A06-S1	Explicit consideration of IEs caused by operator errors helps to get additional insights regarding deficiencies in the control room design, plant procedures, and operator training. This additional consideration may be used for improvement of the design (Application 2.1).
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).
AS-B03-S1 AS-C02-S1 AS-C03-S1 AS-C14-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 (Application 2.1).
AS-C12-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-C15-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).
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 2.2).
SY-B13-S1	Revisiting the components screening process promotes a more realistic estimation of the risk for newly designed NPPs at different stages of the design (Application 2.1) and a better understanding of the deviations between an existing plant design and revised design-related rules (Application 2.2).
SY-B15-S1	A detailed modelling of the components promotes a better appreciation of the risk impact of constituting parts of components for newly designed NPPs (Application 2.1) and provides a better understanding of the deviations between an existing plant design and revised design-related rules (Application 2.2).
HR-E01-S2	A search for plant states that could lead to conditions conducive to errors of commission can lead to the identification of defences to prevent such occurrences (Application 2.1).
DF-F01-S1	A structured identification and consideration of subtle interactions is helpful for modelling dependencies for newly designed NPPs (Application 2.1) and assessing the safety importance of deviations between an existing plant design and updated/revised design-related rules (Application 2.2).

SA Identifier	Relevance to Specific Applications in the Category
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 2.2).
MQ-B03-S1 MQ-B03-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 2.2).

Table 13.3 NPP Operation

SA Identifier	Relevance to Specific Applications in the Category
Essential Attributes	
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).
IE-F04-S1	Time trend analysis is essential to assess the impact of components aging, which may be the cause for the changes in the number of IEs (Application 3.1.3).
AS-B03-S1 AS-C02-S1 AS-C03-S1 AS-C14-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-C04-S1 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 Applications 3.2.1, 3.3.1, and 3.4.2.
SY-B08-S1	The possibility to effectively handle maintenance basic events allows assessment of the impact of maintenance program optimization (Application 3.1.1), impact of improvements in maintenance personnel training program (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-B08-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 program optimization (Application 3.1.1 and Application Group 3.4).
SY-B08-S3	Symmetric models are needed for Risk Monitor type applications in order to avoid overestimation or underestimation of specific plant configurations (Application Group 3.4).
SY-B13-S1 SY-B15-S1	Maintenance program 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 program optimization (Applications 3.1.1 and 3.1.3).
SY-B16-S1	Time-dependent modelling is needed for application dealing with changes to test activities (Application 3.4.1).
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 is essential for the development and improvement of emergency operating procedures and improvement of operator training programs (Applications 3.2.1 and 3.3.1).
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 program 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 program (Application 3.1.3).
MQ-C02-S1	A more detailed modelling of specific system configurations (e.g. maintenance on specific trains) is important for maintenance program optimization (Application 3.1.1) and all Risk Monitor type applications (Application Group 3.4).

SA Identifier	Relevance to Specific Applications in the Category
Supplemental Attributes	
IE-A06-S1	1) Changes in the maintenance program may impact the probability of operator errors leading to IEs. It is worthwhile to assess the influence of this particular aspect (Application 3.1.1). 2) It is useful to consider the IEs caused by operator errors to avoid adverse impact of changes in maintenance, tests, and training activities (Applications 3.3.1, 3.3.2, and 3.4.1), as well as to identify and assess the events caused by operator errors that may initiate an accident sequence with severe consequences (Applications 3.2.2 and 3.2.3). 3) It is useful to consider IEs caused by human errors while developing management training program (Application 3.3.3).
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 program (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-F04-S1	The time trend analysis is useful in assessing the impact of changes in the maintenance, test, and training activities on the occurrence of IEs (Applications 3.3.1, 3.3.2, 3.3.3, and 3.4.1).
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).
AS-B03-S1 AS-C02-S1 AS-C03-S1 AS-C14-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 programs based on plant-specific PSA insights (Application 3.3.3).
AS-C04-S1 AS-C05-S1 AS-C06-S1	A more complete modelling of accident progression dealing with requirements of plant emergency procedures is useful for the improvement of management training programs (Application 3.3.3).
AS-C15-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.
SY-B08-S1 SY-B08-S2	The possibility to effectively handle test and maintenance basic events may be useful for the improvement of operator training programs (Application 3.3.1).
SY-B13-S1 SY-B15-S1	Improvement of operator training programs may ask for inclusion of more components than those already modelled in the system models (Application 3.3.1).
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-E01-S1	Modelling of the actions to recover from the equipment failure to automatically initiate or change state may be useful for assessing specific impacts of changes in emergency operating procedures (Application 3.2.1).
HR-E01-S2	Identification of the conditions and plant status conducive to errors of commission could reduce the potential for such errors (Application 3.3.1).
HR-G04-S1	Improvement of the management training program would benefit from a more realistic HRA that use the time windows for operator actions which are based on plant-specific thermal-hydraulic analyses (Application 3.3.3).
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 programs (Applications 3.3.1 and 3.3.3).
DA-F01-S1	Detailed modelling of CCFs reflecting the combinations of redundancies/diversities would lead to a more accurate analysis to support plant configuration control (Application Group 3.4).

SA Identifier	Relevance to Specific Applications in the Category
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 program optimization (Application 3.1.1), support for plant ageing management program (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).
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 programs (Applications 3.3.1 and 3.3.3).

Table 13.4 Permanent Changes to the Operating Plant

SA Identifier	Relevance to Specific Applications in the Category
Essential Attributes	
IE-A06-S1	It is important to verify that the changes to TS (e.g. transfer of equipment maintenance from shutdown to power operation) do not impose additional unacceptable risk caused by introducing a potential for new IEs due to operator errors (Applications 4.2.1 and 4.2.2). In addition, 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 (Application 4.2.3).
IE-F04-S1 IE-H02-S1	The time trend analysis in relation to IEs and the incidence database are essential for the decisions on NPP upgrades, back-fitting activities, plant modifications, and life-time extension (Application Group 4.1).
AS-B03-S1 AS-C02-S1 AS-C03-S1 AS-C14-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).
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-B08-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-B08-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-B08-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, 4.3.2).
SY-B16-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 require adequate modelling of the impact of pipe ruptures if the latter are included in the model (Application 4.2.5).
DA-C02-S1	Use of generic sources of data for reliability parameters for new equipment should be justified (Application 4.1.1).
DA-E01-S1	A time trend analysis to explore the existing trends in the reliability parameters is important for Application 4.1.2.
MQ-C02-S1	A more detailed modelling of specific system configurations is important for applications dealing with changes in TS (Application Group 4.2).
Supplemental Attributes	
IE-A06-S1	Analysis of the IEs caused by operator errors is useful to estimate the impact of changes in the in-service testing or plant modifications (Application 4.1.1 and 4.2.4).
IE-B01-S1	NPP upgrades and changes in in-service testing may increase the frequency of 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-F04-S1	The time trend analysis in relation to IEs provides helpful information for decision making about equipment risk significance (Applications 4.1.2, 4.3.1, and 4.3.2).
IE-H02-S1	An electronic IE database is useful for Applications 4.1.1, 4.1.2, 4.3.1, and 4.3.2.
AS-C04-S1	Incomplete modelling of accident progression dealing with requirements of plant emergency

SA Identifier	Relevance to Specific Applications in the Category
AS-C05-S1 AS-C06-S1	procedures may cause incomplete or inadequate coverage of accident scenarios for Application 4.1.1.
AS-C15-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.
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).
SY-B08-S1 SY-B08-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-B13-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-B15-S1 SY-C15-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-B16-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).
HR-E01-S2	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 to reduce the potential for introducing changes that could increase the likelihood of, or create conditions conducive to, errors of commission (all Applications in Category 4).
HR-G01-S1	Performing a detailed assessment of all HEPs may be useful in prioritising the NPP upgrades, back-fitting activities and plant modifications (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 and Application Group 4.2).
DA-F01-S1 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-F01-S1 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).
MQ-B03-S2 MQ-D01-S1	Use of reduced truncation values 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).

Table 13.5 Oversight Activities

SA Identifier	Relevance to Specific Applications in the Category
Essential Attributes	
IE-A06-S1 IE-B01-S1 IE-C02-S1	The lists of IEs and IE groups should be detailed enough to allow the evaluation of inspection findings and operational events (Applications 5.2.1 and 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 Attributes	
IE-F04-S1	The time trend analysis in relation to IEs provides useful information for decision making (Application Group 5.1).
IE-H02-S1	An electronic IE database is useful for Application Group 5.1.
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).
SY-B13-S1 SY-B15-S1 SY-C15-S1	More components may need to be included into the model for Application Group 5.2.
DA-B01-S1 DA-F01-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).
DA-E01-S1	The time trend analysis is useful for the assessment of long term performance indicators (Application 5.1.2).
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.
MQ-B03-S1 MQ-B03-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).

Table 13.6 Evaluation of Safety Issues

SA Identifier	Relevance to Specific Applications in the Category
Essential Attributes	
All SAs	For Application Category 6 any of the special attributes may be required on a case-by-case basis depending on the issue to be analyzed. For these applications, the PSA model should be upgraded in a manner that would allow evaluating the impact associated with the considered measure or issue by the PSA model.
Supplemental Attributes	
None	

Table 13.7 Mapping the Special Attributes of PSA Elements to PSA Applications[8]

PSA Application Category	PSA Application Group/ PSA Application	PSA Elements								
		IE	AS	SC	SY	HR	DA	DF	MQ	RI
1. SAFETY ASSESSMENT	1.1 Assessment of the overall plant safety	-	-	-	-	-	-	-	-	-
	1.2 Periodic safety review	**IE-F04-S1** IE-H02-S1	AS-C02-S1 AS-C12-S1 AS-C15-S1	SC-B01-S1	-	HR-G04-S1	**DA-E01-S1** DA-H02-S1	DF-F01-S1 DF-G01-S1	-	-
	1.3 Analysis of the degree of defence against assumed terrorist attack scenarios	IE-A06-S1 IE-B01-S1	AS-C04-S1 AS-C15-S1	-	-	-	-	-	-	-
2. DESIGN EVALUATION	2.1 Application of PSA to support decisions made during the NPP design (plant under design)	IE-A06-S1 IE-C02-S1 IE-C02-S2	AS-B03-S1 AS-C02-S1 AS-C03-S1 AS-C12-S1 AS-C14-S1 AS-C15-S1	-	**SY-C07-S1 SY-C14-S1 SY-C15-S1** SY-B13-S1 SY-B15-S1	HR-E01-S2	**DA-F01-S1 DA-C02-S1**	DF-F01-S1	-	-
	2.2 Assessment of the safety importance of deviations between an existing plant design and updated/revised deterministic design rules	-	-	SC-B01-S1	**SY-C07-S1 SY-C14-S1 SY-C15-S1** SY-B13-S1 SY-B15-S1	-	**DA-F01-S1**	DF-F01-S1 DF-G01-S1	MQ-B03-S1 MQ-B03-S2 MQ-D01-S1	-
3. NPP OPERATION	**3.1 NPP maintenance**									
	3.1.1 Maintenance program optimization	IE-A06-S1 IE-B01-S1	-	-	**SY-B08-S1 SY-B08-S2 SY-B13-S1 SY-B15-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	-	-	-	-	-		-	-	-
	3.1.3 Risk-informed support for plant ageing management program	**IE-F04-S1** IE-H02-S1	-	-	**SY-B13-S1 SY-B15-S1**	-	**DA-E01-S1**	DF-F01-S1 DF-G01-S1	-	-

[8] The general attributes described in Sections 4-12 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 13), are provided in **bold underlined 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 13), are provided in regular font.

PSA Application Category	PSA Application Group/ PSA Application	PSA Elements								
		IE	AS	SC	SY	HR	DA	DF	MQ	RI
	3.2 Accident mitigation and emergency planning									
	3.2.1 Development and improvement of the emergency operating procedures	-	**AS-B03-S1** **AS-C02-S1** **AS-C03-S1** **AS-C14-S1** **AS-C04-S1** **AS-C05-S1** **AS-C06-S1**	-	-	**HR-G02-S1** **HR-G04-S1** HR-E01-S1	-	DF-F01-S1 DF-G01-S1	-	-
	3.2.2 Support for NPP accident management (severe accident prevention, severe accident mitigation)	IE-A06-S1 IE-B01-S1	-	-	-	**HR-G02-S1**	-	DF-F01-S1 DF-G01-S1	-	-
	3.2.3 Support for NPP emergency planning	IE-A06-S1 IE-B01-S1	-	-	-	-	-	-	-	-
	3.3 Personnel training									
	3.3.1 Improvement of operator training program	IE-A06-S1 IE-F04-S1	**AS-B03-S1** **AS-C02-S1** **AS-C03-S1** **AS-C14-S1** **AS-C04-S1** **AS-C05-S1** **AS-C06-S1** AS-C15-S1	-	SY-B08-S1 SY-B08-S2 SY-B13-S1 SY-B15-S1	**HR-G04-S1** HR-E01-S2	DA-D05-S1	-	MQ-C02-S1	-
	3.3.2 Improvement of maintenance personnel training program	IE-A06-S1 IE-F04-S1	AS-C15-S1	-	**SY-B08-S1**	HR-D06-S1	-	-	-	-
	3.3.3 Improvement of plant management training program	IE-A06-S1 IE-F04-S1	AS-C02-S1 AS-C03-S1 AS-C14-S1 AS-C04-S1 AS-C05-S1 AS-C06-S1 AS-C15-S1	-	-	HR-G04-S1	DA-D05-S1	-	MQ-C02-S1	-

PSA Application Category	PSA Application Group/ PSA Application	PSA Elements								
		IE	AS	SC	SY	HR	DA	DF	MQ	RI
	3.4 Risk-based configuration control/ Risk Monitors									
	3.4.1 Configuration planning (e.g. support for plant maintenance and test activities)	IE-A06-S1 IE-F04-S1	-	-	**SY-B08-S1** **SY-B08-S2** **SY-B08-S3** **SY-B16-S1**	-	**DA-B01-S1** **DA-D05-S1** DA-F01-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-C02-S1** **AS-C03-S1** **AS-C14-S1** **AS-C04-S1** **AS-C05-S1** **AS-C06-S1** AS-C15-S1	-	**SY-B08-S1** **SY-B08-S2** **SY-B08-S3**	-	**DA-B01-S1** **DA-D05-S1** DA-F01-S1 DA-F02-S1	DF-F01-S1 DF-G01-S1	**MQ-C02-S1**	-
	3.4.3 Exemptions to TS and justification for continued operation	**IE-B01-S1**	-	-	**SY-B08-S1** **SY-B08-S2** **SY-B08-S3**	-	**DA-B01-S1** **DA-D05-S1** DA-F01-S1 DA-F02-S1	DF-F01-S1 DF-G01-S1	**MQ-C02-S1**	-
	3.4.4 Dynamic risk-informed TS	-	-	-	**SY-B08-S1** **SY-B08-S2** **SY-B08-S3**	-	**DA-B01-S1** **DA-D05-S1** DA-F01-S1 DA-F02-S1	DF-F01-S1 DF-G01-S1	**MQ-C02-S1**	-
4. PERMANENT CHANGES TO THE OPERATING PLANT	**4.1 Plant changes**									
	4.1.1 NPP upgrades, back-fitting activities and plant modifications	**IE-F04-S1** **IE-H02-S1** IE-A06-S1 IE-B01-S1 IE-C02-S1 IE-C02-S2 IE-H02-S1	**AS-B03-S1** **AS-C02-S1** **AS-C03-S1** **AS-C14-S1** AS-C04-S1 AS-C05-S1 AS-C06-S1 AS-C15-S1	**SC-B01-S1**	**SY-B16-S1** SY-B13-S1 SY-B15-S1 SY-C15-S1	HR-E01-S2 HR-G01-S1	**DA-C02-S1** DA-D05-S1	DF-F01-S1 DF-G01-S1	MQ-B03-S2 MQ-D01-S1	-
	4.1.2 Lifetime extension	**IE-F04-S1** **IE-H02-S1** IE-B01-S1 IE-F04-S1 IE-H02-S1	-	-	-	HR-E01-S2	**DA-E01-S1**	DF-F01-S1 DF-G01-S1	-	-

PSA Application Category	PSA Application Group/ PSA Application	PSA Elements								
		IE	AS	SC	SY	HR	DA	DF	MQ	RI
	4.2 Technical specification changes									
	4.2.1 Determination and evaluation of changes to allowed outage time and changes to required TS actions	**IE-A06-S1**	-	-	**SY-B08-S1** **SY-B08-S2** **SY-B08-S3** **SY-B16-S1** SY-B13-S1 SY-B15-S1 SY-C15-S1	HR-E01-S2	DA-B01-S1 DA-D05-S1 DA-F01-S1 DA-F02-S1	-	**MQ-C02-S1**	-
	4.2.2 Risk-informed optimisation of TS	**IE-A06-S1**	-	-	**SY-B08-S3** **SY-B16-S1** SY-B13-S1	HR-E01-S2	DA-B01-S1 DA-D05-S1 DA-F01-S1 DA-F02-S1	-	**MQ-C02-S1**	-
	4.2.3 Determination and evaluation of changes to surveillance test intervals	**IE-A06-S1**	-	-	**SY-B08-S3** **SY-B16-S1** SY-B13-S1 SY-B15-S1 SY-C15-S1	HR-E01-S2	DA-B01-S1 DA-D05-S1 DA-F01-S1 DA-F02-S1	-	**MQ-C02-S1**	-
	4.2.4 Risk-informed in-service testing (IST)	IE-A06-S1 IE-C02-S1 IE-C02-S2	-	-	**SY-B16-S1** SY-B08-S1 SY-B08-S2 SY-B15-S1 SY-C15-S1	HR-E01-S2	DA-B01-S1 DA-D05-S1 DA-F01-S1 DA-F02-S1	-	**MQ-C02-S1**	-
	4.2.5 Risk-informed in-service inspections (ISI)	IE-C02-S1 IE-C02-S2	-	-	**SY-C01-S1** SY-B13-S1 SY-B15-S1 SY-C15-S1 SY-B06-S1	HR-E01-S2	DA-B01-S1 DA-D05-S1 DA-F01-S1 DA-F02-S1	-	**MQ-C02-S1**	-

PSA Application Category	PSA Application Group/ PSA Application	PSA Elements								
		IE	AS	SC	SY	HR	DA	DF	MQ	RI
	4.3 Establishment of graded QA program for SSC									
	4.3.1 Equipment risk significance evaluation	IE-F04-S1 IE-H02-S1	-	-	**SY-B08-S3** SY-B13-S1 SY-B15-S1 SY-C15-S1 SY-B16-S1	HR-E01-S2	-	-	-	-
	4.3.2 Evaluation of risk impact of changes to QA requirements	IE-F04-S1 IE-H02-S1	-	-	**SY-B08-S3** SY-B13-S1 SY-B15-S1 SY-C15-S1 SY-B16-S1	HR-E01-S2	-	-	-	-
5. OVERSIGHT ACTIVITIES	**5.1 Performance monitoring**									
	5.1.1 Planning and prioritization of inspection activities (regulatory and industry)	IE-F04-S1 IE-H02-S1	-	-	-	-	-	DF-F01-S1 DF-G01-S1	MQ-B03-S1 MQ-B03-S2 MQ-C02-S1 MQ-D01-S1	-
	5.1.2 Long term risk-based performance indicators	IE-F04-S1 IE-H02-S1	-	-	-	-	DA-B01-S1 DA-F01-S1 DA-F02-S1 DA-H02-S1 DA-E01-S1	DF-F01-S1 DF-G01-S1	MQ-B03-S1 MQ-B03-S2 MQ-C02-S1 MQ-D01-S1	-
	5.1.3 Short term risk-based performance indicators	IE-F04-S1 IE-H02-S1	-	-	-	-	DA-B01-S1 DA-F01-S1 DA-F02-S1 DA-H02-S1	DF-F01-S1 DF-G01-S1	MQ-B03-S1 MQ-B03-S2 MQ-C02-S1 MQ-D01-S1	-
	5.2 Performance assessment									
	5.2.1 Assessment of inspection findings	**IE-A06-S1** **IE-B01-S1** **IE-C02-S1**	All SAs for AS	**SC-B01-S1**	SY-B13-S1 SY-B15-S1 SY-C15-S1	-	DA-B01-S1 DA-F01-S1 DA-F02-S1 DA-H02-S1	DF-F01-S1 DF-G01-S1	MQ-B03-S1 MQ-B03-S2 MQ-D01-S1	-
	5.2.2 Evaluation and rating of operational events	**IE-A06-S1** **IE-B01-S1** **IE-C02-S1**	All SAs for AS	**SC-B01-S1**	SY-B13-S1 SY-B15-S1 SY-C15-S1	-	DA-B01-S1 DA-F01-S1 DA-F02-S1 DA-H02-S1	DF-F01-S1 DF-G01-S1	MQ-B03-S1 MQ-B03-S2 MQ-D01-S1	-

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

14. CONCLUSIONS

The matter of PSA 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 support reliably 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.

This publication covers a Level-1 internal events at-power PSA. Nine 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 relation to each PSA application, the special attributes were further distinguished as essential and supplemental. An essential special attribute emphasises 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.

This 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 be also 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. Refs [19], [20].

Appendix I
RISK METRIC DEFINITIONS

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 (FV)*

  For a specific basic event, the FV 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 damage frequency, annual average (CDF_{AVE})

This is the frequency of core damage 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.

Change in core damage frequency, annual average (ΔCDF_{AVE})

This is the change in the annual average CDF 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 damage frequency, time-dependent (CDF{t})

This is the frequency of core damage as a function of time. It is often referred to as the 'instantaneous core damage frequency.' Only some of the parameters that the *CDF* 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 damage event over a specified time interval.

Conditional core samage probability (CCDP)

This is the conditional core 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 damage for the condition that the initiating event has occurred.

Incremental conditional core damage probability (ICCDP)

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

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 ($\Delta LERF_{AVE}$)

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.

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.

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 for use in decision making[9]	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_{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 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.	ΔCDF_{AVE}, $\Delta LERF_{AVE}$, CDF_{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 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 2.2.

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

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
1.3 Analysis of the degree of defence against assumed terrorist attack scenarios Assessment may include identification of vital plant areas, which may pose significant risk to the plant in case of malevolent acts, and of exploratory design options aimed to reduce the risk.	CCDP, CLERP, risk importance measures of plant of all SSCs, HEs, and plant areas	Vital areas identification would in principle require a full scope Level 1 through 3 PSA covering all operating and shutdown modes and both internal and external plant hazards. However, meaningful results for vital area identification can be obtained from Level-1 internal and external hazards PSA. After September 11, 2001, this application was introduced to analyse the quantitative degree of defence of NPPs against attack scenarios similar to the observed. Other types of terrorist attack scenarios, i.e. external explosions can be considered within the scope of this application. This application requires the development of special analysis models derived from the baseline model by adding event trees or additional fault trees to the existing model including the required data. It requires a reassessment of the HRA for post-accident human actions, accident management actions and SAMG-actions, with special regard to hardware dependencies. Special deterministic analysis in support of the model extensions as a part of the events sequence analysis is required, i.e. for the structural dynamics of buildings, impact of fires and explosions, etc. Event sequence analysis may require additional experimental analysis.
2. DESIGN EVALUATION		
2.1 Application of PSA to support decisions made during the NPP design (plant under design) The application focuses on identification of design weaknesses and effective areas for improvement in view of plant risk. 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_{AVE}, $LERF_{AVE}$, CDP, LERP, QHOs, ΔCDF_{AVE}, $\Delta LERF_{AVE}$, 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. Particular effort should be made to identify unique initiating events, failure modes, event sequences and dependencies that may be introduced by new design features. Detailed dependency matrices should be developed to identify and document all physical and functional dependencies among support systems and front-line systems. All normally operating systems should 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. 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, and to develop SSC reliability and availability targets.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
2.2 Assessment of the safety importance of deviations between an existing plant design and updated/revised deterministic design rules Assessment may include investigation of risk-significance of deviations from revised design rules; often performed in the framework of a periodic safety review.	CDF_{AVE}, $LERF_{AVE}$, QHOs, ΔCDF_{AVE}, $\Delta LERF_{AVE}$, Risk importance measures of affected SSCs and HEs (e.g. F-V, RAW)	The key issue in this application is the possible impact of changes in the design rules on risk associated with plant operation. Special model adjustments, model extensions and revisiting key 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, 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.
3. NPP OPERATION		
3.1 NPP maintenance		
3.1.1 Maintenance program optimization The application includes assessment, optimization and establishment of maintenance plans and 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.	Risk importance measures of affected SSCs (e.g. F-V, RAW), ΔCDF_{AVE}, $\Delta LERF_{AVE}$	Risk importance measures from the base PSA are used to help prioritize candidate maintenance changes: changes in CDF and LERF are used to justify acceptable risk impacts and to determine risk significance. Explicit model of maintenance unavailabilities and capability to predict or bound the impact of program 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 program 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 events (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), ΔCDF_{AVE}, $\Delta LERF_{AVE}$	The results of an external event and internal hazard PSA are used to assess the relative risk contributions of rooms and areas and identify backfitting measures. For example, the results of an internal fire PSA may be taken into account for adjusting transient combustible control.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
3.1.3 Risk-informed support for plant ageing management program The aim of this application is to optimise the scope of the plant specific ageing program 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), ΔCDF_{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.
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_{AVE}, $\Delta LERF_{AVE}$	Importance measures from base PSA used to help prioritize candidate procedural changes, change in CDF 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 for use in decision making[9]	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_{AVE}, $\Delta LERF_{AVE}$	Importance measures from 'base case PSA' are used to help prioritize candidate accident management procedure changes; changes in CDF 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 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 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.	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. An example is to support the determination of EPZ distance, emergency action levels, and planning and training for evacuation and sheltering activities.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
3.3. Personnel training		
3.3.1 Improvement of operator training program PSA is used to improve operator training program 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 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 to make operators understand severe accident scenarios.	Description of dominant ASs for CDF_{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_{AVE}, $\Delta LERF_{AVE}$	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 program Training of maintenance staff is enhanced based on insights and information from the PSA. Focus is on potential risk significant impacts of 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 program as well as opportunities to optimize maintenance tasks that are not significant to risk management.	Risk importance measures (e.g. F-V, RAW) of affected SSCs, pre-accident HEs, and basic events dealing with maintenance and CCFs, ΔCDF_{AVE}, $\Delta LERF_{AVE}$	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 program 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 maintenance program 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.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
3.3.3 Improvement of plant management training program 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_{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 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.	CDF{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 and LERF results dependent on specific plant configurations 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 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 should be capable of predicting the temporal changes in initiating event frequencies, component unavailabilities due maintenance and other configuration changes on CDF 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 operating 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.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
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{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 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.	ΔCDF_{AVE}, $\Delta LERF_{AVE}$, 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 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 an 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 relaxes 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 plant configurations including safety and non-safety related SSCs.	CDF{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 for use in decision making[9]	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, back-fitting 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_{AVE}, $\Delta LERF_{AVE}$	Importance measures from 'base case PSA' are used to help prioritize candidate design changes; change in CDF 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 should 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 Lifetime 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_{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 should 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.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
4.2 Technical specification changes		
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 whether on-line maintenance is appropriate.	Risk importance measures of affected SSCs, ΔCDF_{AVE}, $\Delta LERF_{AVE}$, 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 whose 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 for use in decision making[9]	Comments on how PSA models can be used to support application and examples
4.2.2 Risk-informed optimisation 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 optimise TS provisions. Beside risk insights, other not risk-based parameters may have to be used as constraints in the optimisation process.	Risk importance measures of affected SSCs, ΔCDF_{AVE}, $\Delta LERF_{AVE}$, 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_{AVE}, $\Delta LERF_{AVE}$	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 the STI on each affected component unavailability due to a random failure. 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 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.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
4.2.4 Risk-informed in-service testing Use of PSA to support the IST 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 IST program. 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 program.	Risk importance measures (e.g. F-V, RAW) of affected SSCs, ΔCDF_{AVE}, $\Delta LERF_{AVE}$	Risk importance measures from the base PSA used to help prioritize candidate changes to IST program for selected pumps and valves, change in CDF 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 program 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, 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.	Component failure rates for different inspection strategies (e.g. obtained using PFM or Markov model), CCDP, CLERP, ΔCDF_{AVE}, $\Delta LERF_{AVE}$	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) program. These passive components are normally not explicitly modelled in a 'base case PSA'. Hence, special analyses must be performed to estimate component (e.g. weld) level failure rates as a function of level and type of inspection, and consequences of pipe failure in terms of the CCDP 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 program for selected weld locations, change in CDF 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 and CLERP of any assumed failure mode within the scope of the piping systems selected for the RI-ISI program. 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 programs.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
4.3 Establishment of graded QA program for SSC		
4.3.1 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_{AVE}, $\Delta LERF_{AVE}$	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. An example is evaluating the change in risk associated with relaxation of QA requirements.
5. OVERSIGHT ACTIVITIES		
5.1 Performance monitoring		
5.1.1 Planning and prioritization of inspection activities (regulatory and industry) PSA based ranking of design and operational features is used to focus resources for regulatory and industry inspections on important issues and equipment.	CDF_{AVE}, $LERF_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk, ΔCDF_{AVE}, $\Delta LERF_{AVE}$, CCDP, CLERP	The insights from baseline PSA results are used to support setting the agenda and 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.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
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. Long term use includes analysis of past plant behaviour integrating the events occurred, failures and unavailabilities. This information (including CDF trends, comparison between expected and calculated CDF, 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 for the next period.	CDF_{AVE}, $LERF_{AVE}$, CDF{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 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 estimates derived by integration of instantaneous CDF for the observed plant configurations. An example is the trending of the number of failures or unavailable hours of a highly risk significant SSCs.
5.1.3 Short term risk based performance indicators Risk based indicators for short term use require instantaneous evaluation of risk. This type of application provides information on changes in CDF due to plant events and risk associated with planned activities.	CDF_{AVE}, $LERF_{AVE}$, CDF{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 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. An example is the identification of the abnormal conditions for equipment operation leading to increase in their failure probabilities.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
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_{AVE}, $LERF_{AVE}$, ΔCDF_{AVE}, $\Delta LERF_{AVE}$	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 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 damage due to such event.	CCDP, CLERP, CDF_{AVE}, $LERF_{AVE}$	If the event in question is an initiating event, the PSA model is used to estimate the CCDP 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 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. Example: Evaluating the conditional probability of core 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_{AVE}, $\Delta LERF_{AVE}$	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.

Brief description of PSA application	PSA results and metrics for use in decision making[9]	Comments on how PSA models can be used to support application and examples
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_{AVE}, $LERF_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk, key 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.
6.2 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_{AVE}, $LERF_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk, ΔCDF_{AVE}, $\Delta LERF_{AVE}$, CCDP, CLERP	PSA results are used to develop risk insights, and strategies to maintain or reduce risk levels are devised. 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_{AVE}, $LERF_{AVE}$, QHOs, risk importance measures of all SSCs and HEs, primary contributors to risk, ΔCDF_{AVE}, $\Delta LERF_{AVE}$, CCDP, 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.

Appendix III

MAPPING THE PSA ELEMENTS TO THE PSA TASKS ADDRESSED IN THE IAEA PSA GUIDELINES

The table below shows the relation between the PSA elements defined in this publication and PSA technical tasks from the IAEA PSA Procedure Guide 'Procedures for Conducting PSA of NPPs (Level 1)', Safety Series No. 50-P-4, 1992. The table helps to realize what tasks from the Procedure Guide are correspondent to the PSA elements.

ID	PSA ELEMENT IN TECDOC	TASKS FROM SAFETY SERIES No. 50-P-4
IE	Initiating Events Analysis	Task 13: Selection of initiating events
		Task 17: Grouping of the initiating events
		Task 24: Assessment of the frequency of initiating events
AS	Accident Sequence Analysis	Task 12: Definition of core damage states or other consequences
		Task 14: Determination of safety functions
		Task 15: Assessment of function/system relationships
		Task 18: Event sequence modelling
		Task 22: Impact of physical processes on development of logic models
		Task 23: Classification of accident sequences into plant damage states
		Task 27: Determination of accident sequence Boolean equations
SC	Success Criteria and Supporting Analysis	Task 16: Assessment of plant system requirements (success criteria)
SY	Systems Analysis	Task 19: System modelling
		Task 22: Impact of physical processes on development of logic models
HR	Human Reliability Analysis	Task 20: Human performance analysis
		Task 26: Assessment of human error probabilities
DA	Data Analysis	Task 25a: Assessment of component reliability
		Task 25b: Assessment of common cause failure probabilities
DF	Dependent Failures Analysis	Task 21: Qualitative dependence analysis
MQ	Model Integration and CDF Quantification	Task 28: Initial quantification of the accident sequences
		Task 29: Final quantification of the accident sequences
		Task 30: Uncertainty analysis
RI	Results Analysis and Interpretation	Task 31: Importance and sensitivity analysis
		Task 34: Preparation of documentation

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Guide, IAEA Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2002).

[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).

[3] 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: A Safety Practice, Safety Series No. 50-P-8, IAEA, Vienna (1995).

[4] 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).

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

[6] 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).

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

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

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

[10] 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).

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

[12] THE AMERICAN NUCLEAR SOCIETY, External Events in PRA Methodology, American Nuclear Society Standard ANSI/ANS-58.21-2003, ANS (2003).

[13] 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, DC (1998).

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

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

[16] 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).

[17] 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).
[18] US NUCLEAR REGULATORY COMMISSION, Interim Reliability Evaluation Program Procedures Guide, NUREG/CR-2728, USNRC, Washington, DC (1983).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Review of Probabilistic Safety Assessments by Regulatory Bodies, Safety Report Series No. 25, IAEA, Vienna (2002).
[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Review of Probabilistic Safety Assessment (PSA) – Level 1, IAEA-TECDOC-1135, IAEA, Vienna (2000).

ABBREVIATIONS

AC	alternating current
AMP	accident management procedure
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
CDF	core damage frequency
CLERP	conditional large early release probability
DBA	design basis accident
DC	direct current
DG	diesel generator
ECCS	emergency core cooling system
EDG	emergency diesel generator
EOP	emergency operating procedure
EPZ	emergency planning zone
ESF	engineered safety feature
ET	event tree
FMEA	failure mode effect analysis
FT	fault tree

F-V	Fussell-Vesely (importance measure)
GA	general attribute
HE	human error
HEP	human error probability
HFE	human failure event
HPCI	high pressure coolant injection
HPECC	high pressure emergency core cooling
HRA	human reliability analysis
I&C	instrumentation and control
ICCDP	incremental conditional core damage probability
ICLERP	incremental conditional large early release probability
IE	initiating event
IPSART	international probabilistic safety assessment review team
ISI	in-service inspection
ISLOCA	interfacing system LOCA
IST	in-service testing
LERF	large early release frequency
LOCA	loss of coolant accident
LOOP	loss of offsite power
LWR	light water reactor
MCP	main coolant pump
MMI	man-machine interface
MSIV	main steam isolation valve
NDE	non-destructive examination
NPP	nuclear power plant
P&IDs	piping and instrumentation diagram
PFM	probabilistic fractural mechanics
PORV	pressurizer power operated relief valve
PRA	probabilistic risk assessment

PSA	probabilistic safety assessment
PSF	performance shaping factor
PWR	pressurized water reactor
QA	quality assurance
QHO	quantitative health objective
RAW	risk achievement worth
RHR	residual heat removal
RI-ISI	risk-informed in-service inspection
RPS	reactor protection system
RPV	reactor pressure vessel
SA	special attribute
SAMG	severe accident management guideline
SAR	safety analysis report
SG	steam generator
SGSV	steam generator safety valve
SLOCA	small LOCA
SSC	systems, structures, and components
STI	surveillance test interval
TECDOC	technical document
THERP	technique for human error rate prediction
TS	technical specification

CONTRIBUTORS TO DRAFTING AND REVIEW

Alsop, C.J.	British Energy/ NNC International Consulting (BENIC), United Kingdom
Alzbutas, R.	Lithuanian Energy Institute, Lithuania
Angaloor, V.K.	Safety Directorate NPCIL, India
Bagdonas, A.	Ignalina NPP, Lithuania
Bennemo, L.J.G.	Swedish Nuclear Power Inspectorate, Sweden
Berg, H.P.	Bundesamt für Strahlenschutz, Germany
Bertucio, R.	SCIENTECH, United States of America
Bradley, R.E.	Nuclear Energy Institute, United States of America
Chakraborty, S.	Swiss Federal Nuclear Safety Inspectorate, Switzerland
Comanescu, L.	Atomic Energy of Canada Limited, Canada
De Gelder, P.	AVN, Belgium
Dinnie, K.S.	Nuclear Safety Solutions Ltd, Canada
Drouin, M.	U. S. Nuclear Regulatory Commission, United States of America
El-Shanawany, M.	International Atomic Energy Agency
Elter, J.	Paks NPP, Hungary
Eriksson, P. S.	RINGHALS, Sweden
Evans, M. G. K.	Jacobsen Engineering Ltd, United Kingdom
Fleming, K.	Karl N. Fleming Consulting Services, United States of America
Gabco, P.	Bohunice NPP, Slovakia
Ghelbereu, S.	Cernavoda NPP, Romania
Gheorghe, R.	Canadian Nuclear Safety Commission (CNSC), Canada
Godinez, V.	Comisión Nacional De Seguridad Nuclear Y Salvaguardias, Mexico
Gomez-Cobo, A.	Nuclear Installations Inspectorate Health and Safety Executive, United Kingdom

Grantom, C.R.	South Texas Project Nuclear Operating Company, United States of America
Grint, G.	Nuclear Installations Inspectorate, United Kingdom
Gubler, R.	Ingburo Dr. Reinhard Gubler, Switzerland
Habib, A.	Pakistan Nuclear Regulatory Authority, Pakistan
Hahn, L.	GRS, Germany
Hamar, K.	Hungarian Nuclear Safety Directorate, Hungary
Hellstrom, P.	RELCON AB, Sweden
Hellstrom, P. E.	RELCON AB, Sweden
Hendrickx,I.	Tractebel Engineering, Belgium
Hörtner, H.	GRS, Germany
Husarcek, J.	Slovak Nuclear Regulatory Authority, Slovakia
Hustak, S.	Nuclear Research Institute Rez, Czech Republic
Ilieva, M.	Risk Engineering Ltd, Bulgaria
Ishaq, S.	Karachi Nuclear Power Complex, Pakistan
Islamov, R.	International Nuclear Safety Center, Ministry for Atomic Energy of the Russian Federation, Russian Federation
Jakes, M.	Nuclear Safety State Office for Nuclear Safety, Czech Republic
Jang, S.C.	Korean Atomic Energy Research Institute, Republic of Korea
Jonsson, O.B.V.	OKG, Sweden
Kajimoto, M.	Japan Nuclear Energy Safety Organization (JNES), Japan
Kaufer, B.	OECD/NEA
Kichev, E.	CENS
Kirchsteiger, C.	European Commission, JRC, Netherlands
Klevtsov, S.	ETD, Ukraine
Klügel, J.U.	Goesgen NPP, Switzerland
Kobilicova, M.	CENS

Koeberlein, K.	GRS, Germany
Kolesov, S.	National Nuclear Energy Generating Co. 'EnergoAtom', Ministry of Fuel and Energy, Ukraine
Kompella, J.D.	Safety Directorate NPCIL, India
Kouzmina, I.	International Atomic Energy Agency
Krasnukha, S.	South-Ukrainian NPP, Ukraine
Kubanyi, J.	European Commission Joint Research Centre
Kulig, M.J.	ENCONET, Austria
Lanore, J.M.	IRSN, France
Lehner, J.	Brookhaven National Laboratory, United States of America
Lopez, R.M.	National Commission of Nuclear Safety and Safeguards, Mexico
Lyubarskiy, A.	SEC NRS Gosatomnadzor RF, Russian Federation
Macsuga, G.	Nuclear Safety Directorate Hungarian Atomic Energy Authority, Hungary
Marinova, B.	Risk Engineering Ltd, Bulgaria
May, R.	European Commission, JRC, Netherlands
Mlady, O.	Temelin NPP, Czech Republic
Moir, G. R.	British Energy, United Kingdom
Morozov, V.	Atomenergoproject, Russian Federation
Niehaus, F.	International Atomic Energy Agency
Novakova, H.	Relko Ltd, Slovakia
Papazov, V.	Kozloduy NPP, Bulgaria
Parry, G.	US NRC, United States of America
Patrik, M.	Nuclear Research Institute Rez, Czech Republic
Petri, M.C.	Argonne National Laboratory, United States of America
Prochaska, J.	VUJE Trnava Inc. Engineering, Slovakia
Ranguelova, V.	International Atomic Energy Agency

Reinhart, F.M.	US NRC, United States of America
Rybar, J.	Nuclear Regulatory Authority, Slovakia
Schoen, G.	HSK, Switzerland
Schultz, R.	HSK, Switzerland
Serbanesku, D.	Pebble Bed Module Reactor (PBMR) Ltd, South Africa
Shapiro, H. S.	Atomic Energy of Canada Limited, Canada
Sheronov, Y.	Rovno NPP, Ukraine
Shiversky, E.	RDIPE, Russian Federation
Sholly, S.	Institute of Risk Research University of Vienna, Austria
Sloane, B.	Westinghouse Electric Co. LLC, United States of America
Suransky, L.	Mochovce NPP, Slovakia
Svirmickas, S.	State Nuclear Power Safety Inspectorate (VATESI), Lithuania
Tokmachev, G.	Atomenergoproject, Russian Federation
Tong, J.	Institute Of Nuclear Energy Technology, Tsinghua University, People's Republic of China
Tudor, C.	Cernavoda NPP, Romania
Utenkov, S.	ROSENERGOATOM, Russian Federation
Van Graan, H.	Pebble Bed Module Reactor (PBMR) Ltd, South Africa
Varde, P.V.	Bhabha Atomic Research Centre, India
Vazquez, T.	CSN, Spain
Versteeg, M.F.	Ministry of Housing, Spatial Planning and the Environment, Netherlands
Vojnovic, D.	Slovenian Nuclear Safety Administration, Ministry of the Environment, Slovenia
Yang, J.E.	Korean Atomic Energy Research Institute, Republic of Korea
Yllera, J.	International Atomic Energy Agency