|  |
| --- |
|  |
| ONR Technical Assessment Guide  Adequacy of probabilistic safety analysis (PSA) modelling and supporting analysis |



ONR Technical Assessment Guide (TAG)

Adequacy of probabilistic safety analysis (PSA) modelling and supporting analysis

**Head of Profession**: Fault Analysis

**Authored by**: Nuclear Safety Inspector

**Approved by**: Deputy Head of Profession - Fault Analysis

**Issue**: 8

**Published**: September 2024

**Next scheduled review**: September 2027

**Document reference**: NS-TAST-GD-030

**Record reference**: 2020/262092

Revision commentary

|  |  |
| --- | --- |
| Issue | Description of update(s) |
| 7 | The main update to the TAG is to acknowledge the TAG on – ‘Use of PSA and Probabilistic Insights’ with cross references to it where ever this is needed.  All the standards which are referred in the TAG have been updated to latest version, some superseded references have been removed.  The content, which is of the nature of guidance to inspectors, has been moved from elsewhere in the TAG to Section 5. New content has been added based on outcomes from ONR research programmes on digital C&I and multi-unit PSA. Similarly updates have been done to align with latest international guidance emerging areas of small modular reactors, evolutionary and, innovative designs.  Minor revisions to Appendix 1 and Table A-1 to clarify regulatory expectations. Minor revisions to Table B in Appendix 2 to update the cross references.  The cross references to other TAGs have been improved, and specific topics are also briefly summarised to guide the inspector where to look and what for. Guidance for collaborative opportunities with other specialist inspectors is now added where relevant. |

Contents

[1. Introduction 4](#_Toc176876510)

[2. Purpose and scope 5](#_Toc176876511)

[3. Relationship to licence and other relevant legislation 10](#_Toc176876512)

[4. Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides 12](#_Toc176876513)

[5. Advice to Inspectors 24](#_Toc176876514)

[References 62](#_Toc176876515)

[Glossary and abbreviations 67](#_Toc176876516)

[Appendix 1 - Assessment expectations for review of PSAs for NPPs 69](#_Toc176876517)

[Appendix 2 – Mapping between Issue O of the WENRA Reference Levels and this TAG 123](#_Toc176876518)

# Introduction

1. ONR has established its Safety Assessment Principles (SAPs) [1] which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other dutyholders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR’s inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide is one of these guides.

# Purpose and scope

1. The purpose of this technical assessment guide (TAG) is to provide an interpretation of those SAPs [1] related to PSA and to provide specific guidance to inspectors engaged in the assessment of the adequacy of PSAs and supporting analysis of various nuclear facilities (NF) or nuclear power plants (NPPs) from Licensees, Licence Applicants or Generic Design Assessment (GDA) Requesting Parties. All these are referred to as dutyholders in this TAG.
2. This TAG is complementary to the TAG on ‘Use of PSA and Probabilistic Insights’ [2], which provides relevant guidance as per the title, and to provide general guidance to inspectors that may interact with PSA during their duties.
3. PSA is a mathematical tool that derives numerical estimates of risk to high-risk or complex facilities. A PSA model is a logical structure that represents plant responses to a broad range of initiators and failures under different operating modes. The probabilistic evaluation of these models offers insights into the relative safety importance of initiators, response of Structures, Systems, Components (SSC’s) and of operating procedures. PSA provides an overall view of safety characteristics, including both equipment and operator's behaviour. PSA helps to assess whether the design objectives regarding reliability, protection against vulnerabilities and effectiveness of different lines of defence have been achieved satisfactorily. Further high level information on PSA can be found in a Explanatory Note from the WENRA Reactor Harmonisation Working Group [3].
4. The “SAPs addressed” section of this TAG concentrates on interpretation of the SAPs; general guidance on the assessment of PSA is given in the “Advice to inspectors” section. Detailed guidance on the assessment of PSA specific to NPPs is provided in [Appendix 1](#_Appendix_1_-).
5. This TAG is intended to provide guidance for inspectors to carry out their regulatory duties and in the exercise of their regulatory judgment. This TAG will help to demonstrate on how ONR meets the WENRA Reference Levels (RLs), IAEA Safety Standards and other international standards. This TAG is not written for dutyholders, and although it may be used as a source of guidance or good practice, it should not be taken by dutyholders as a prescriptive set of legal requirements.
6. As with all guidance, inspectors should use their judgement and discretion in the depth and scope to which they apply the guidance provided in this TAG and its [Appendix 1](#_Appendix_1_-).
7. This TAG does not claim to provide comprehensive information on how to judge the technical adequacy of the various PSA aspects discussed. Relevant sources of relevant good practice (RGP) are cross referred against specific PSA aspects which the reviewers could use in addition to their knowledge and experience to judge the technical adequacy.
8. It is not the intention of this guide to prescribe specific methods and approaches for conducting PSA. Dutyholders may choose to use alternative methods to those covered by this TAG (and in particular its [Appendix 1](#_Appendix_1_-)) as long as they lead to equally valid outcomes. In cases where the PSA, or specific areas of it, have been undertaken using alternative approaches inspectors should review them on a case-by-case basis and judge them on their own merits. External expert support may be sought if necessary.
9. PSA covers a whole range of disciplines and PSA assessment often requires collaboration with inspectors with in-depth expertise in a range of areas such as fault studies and thermal-hydraulic analysis, mechanical, electrical and C&I systems, civil engineering, human factors, software reliability, structural integrity, internal and external hazards, severe accident analysis (SAA), chemistry, radiological consequences, radwaste and radiation protection. Input from PSA and provision of PSA insights may also be of benefit to assessment conducted in the areas noted, such as the relative risk importance or faults, plant items, or other technical issues. The TAG on ‘Use of PSA and Probabilistic Insights’ [2] is to be used complementarily in this regard.
10. Inspectors must be able to form an opinion on whether risks are as low as reasonably practicable (ALARP) and it is not unreasonable to expect numerical input to the demonstration that the risk is ALARP. NS-TAST-GD-051 [4] provides further guidance on the role of PSA within safety cases and NS-TAST-GD-005 [5] provides further guidance on the role of PSA in the demonstration of ALARP.
11. PSA is typically conducted to analyse off-site risks to the public and comparison against Numerical Targets 7, 8 and 9, therefore this is the focus of this TAG. Although this TAG does not specifically cover PSA for the risk to persons on-site from nuclear accidents (‘worker risk’), it provides sufficient information to help inspectors assessing the PSA inputs for this particular aspect of the safety case provided by the dutyholders and comparison against Numerical Targets 5 and 6. The guidance for the worker risk assessment is more elaborately discussed in NS-TAST-GD-045 [6].
12. The main aspects of PSA addressed by this TAG are as follows:

* Overview of PSA
* Safety assessment principles applicable to PSA
* Guidance on assessment of PSA against the detailed methodology of PSA and supporting analysis.
* Guidance on assessment of the adequacy of PSA performed by the dutyholders against the regulatory expectations and risk targets.
* Guidance on assessment of the adequacy of PSA results and insights to form a judgement that safety case is risk ALARP.

## Terminology

1. Within this TAG, a number of terms have been used with a definition consistent with the glossary in the SAPs. Dutyholders (and also international guidance) may have slightly different definitions or terms.

* **Best estimate analysis**: An approach expected to provide the most realistic and accurate description of the fault and its consequences that could be achieved within the limitations of the analytical model employed and the knowledge of the analysts, without any deliberate bias being introduced.
* **Best estimate data**: When used to describe the data (for example, from experiment or operating experience), best-estimate refers to deriving data in such a way that it reflects the true frequency or probability of an event happening. Some conservatism may be necessary where there is a high level of uncertainty, in order to avoid unjustifiable optimism. PSA (level 1, 2 and 3) should be based on best-estimate values wherever possible.
* **Common cause failure/common mode failure**: Failure of two or more structures, systems or components due to a single specific event or cause. In PSA common cause failures are typically considered within the fault tree modelling of SSCs.
* **Containment**: Methods or physical structures designed to prevent the dispersion of radioactive material. In PSA containment performance is typically considered in the Level 2 PSA.
* **Event tree***:* A logical tree-like structure that represents the fault sequences that may occur following the postulated initiating event included at the start of the tree. Each branch point (or node) represents a test of a safety function. Conventionally success of a test is represented by a line up the page, while failure is represented by a line down the page.
* **Event tree analysis***:* An analysis technique based on event trees where all possible accident scenarios from an accidental initiating event are derived, based on whether installed safety features and other features function or not.
* **Facility***:* A part of a nuclear site identified as being a separate unit for the purposes of nuclear or radiological risk.

A facility may, for example, be a single reactor, a group of processing plants as on a nuclear fuel-cycle facility or a dock and its support systems containing a naval reactor plant. The term encompasses both the terms ‘nuclear installations’ as defined in the Nuclear Installations Act 1965 (as amended) and the term ‘plant’ as used in nuclear site licences.

* **Fault sequence***:* A combination of an initiating fault and any additional failures, faults and internal or external hazards which have the potential to lead to an accident. Fault Sequences in PSA are modelled using event trees.
* **Fault tree***:* A logical tree-like structure which is typically used to represent the failure of an SSC to perform a defined function.   
  This failure is broken down into contributing failure modes using Boolean logic gates and probability events representing specific failures.
* **Fault tree analysis***:* Systematically breaks down the initially defined failure event into the combinationsof events that cause the failure events to occur.
* **Initiating fault/event***:* The starting point of a fault sequence. This may be an internal failure or caused by an internal or external hazard or by human action, or a combination of these. In the PSA this will typically be represented at the start of an event tree.
* **Level 1 PSA***:* A PSA model representing accident sequences beginning with an initiating fault/event and ending with fuel damage (or fuel not damaged).
* **Level 2 PSA***:* A PSA model representing accident sequences beginning with fuel damage and ending with release categories. The level 2 PSA models containment performance and the phenomena that occur during severe accidents. For some reactor designs there may not be a clear dividing line between level 1 and level 2 PSA. .
* **Level 3 PSA***:* A PSA model representing accident sequences beginning with a release category/source term and ending with the effects of the radiological release on humans and the environment.
* **Quantitative risk assessment***:* A formal and systematic approach to estimating the likelihood and consequences of hazardous events. Typically carried out in a simpler way than a PSA.
* **Release category**: A release category is a collection of severe accident sequences as modelled in a Level 2 PSA which have a similar source term. The release category also depends on the inventory of radionuclides available for release to the environment and other parameters such as the height of release, chemical/physical form, heat, momentum etc.
* **Reliability**: The probability that a system or component will meet its minimum performance requirements when called upon to do so for a specified period of time and under stated operating conditions.
* **Severe accident***:* An accident with off-site consequences with the potential to exceed 100 mSv, or to a substantial unintended relocation of radioactive material within the facility that places a demand on the integrity of the remaining physical barriers. A level 2 PSA is used to model the radiological risk from severe accidents.
* **Societal risk***:* The risk of an accident with societal effects causing the deaths of a specified number of people in a single event from a single major industrial activity, i.e. an activity from which risk is assessed as a whole and is under the control of one company in one location, or within a site boundary. PSA indicates the annual risk of such an accident occurring and this can be compared against ONR’s numerical target 9.
* **Source term***:* Data on quantities of radioisotopes released in an accident and the release profile over time of the release, the location of the release and other related parameters from the facility needed as inputs to radiological consequence calculations. Representative source terms are mapped to each Release Category at the level 2/level 3 PSA interface.
* **Technical specification***:* A technical specification establishes minimum requirements for items such as safety limits, limiting safety system settings, limiting control settings, limiting conditions for operation, equipment requirements, surveillance requirements, design features, and administrative controls. These aspects are also covered by the concept of the safe operating envelope.

# Relationship to licence and other relevant legislation

1. The site licence conditions (LCs) give a legal framework which can be drawn on in assessment and are, in general, set out in the form of requiring the licensee to make adequate arrangements, in the interests of safety, to secure certain objectives. The principal LCs relevant ‘Adequacy of PSA Modelling and Supporting Analysis’ are 14, 15, 17, 20, 22, 23 (including 27), 24, and 28.

* **LC 14 - safety documentation** - requires the licensee to make and implement adequate arrangements for the production and assessment of safety cases. For complex and high hazard facilities the licensee’s safety case will need to contain PSA as well as deterministic analysis.
* **LC 15 – periodic review** - sets out the requirements for periodic review and reassessment of safety cases. The periodic reviews carried out under these arrangements include those for updating/extending the PSA (or producing one, if none previously exists, and comparison with relevant good practice) and using it to support the arguments for continuing operation during the period until the next review. It is ONR’s expectation that where licensees have established living PSA programmes all relevant files and records will be maintained for the life of the facility.
* **LC 17 – management systems** - sets out the requirement for quality assurance (QA) arrangements for all matters that affect safety. In this respect dutyholders are expected to establish an adequate QA process that is effectively applied during all phases of the PSA and its application.
* **LC 20 – modification to design of plant under construction** – where available, PSA should be used to risk inform modifications while facilities are being constructed. The earlier PSA is utilised in this process the greater the chance of any associated risks being reduced ALARP. PSA is a powerful tool for improving reliability and avoiding dependencies between SSCs.
* **LC 22 - modification or experiment on existing plant** – similarly to LC 20, use of PSA should be considered when modifications are being planned on existing plant.
* **LC 23 - operating rules** - requires the licensee to produce an adequate safety case. This should be done in line with the licensee’s safety case production arrangements required by LC 14. For complex and high hazard facilities the safety case should utilise both PSA and deterministic aspects. PSA can also be effectively used to demonstrate the risk benefits of safety mechanisms, devices and circuits, as required by LC27 where applicable.
* **LC 24 – operating instructions** - requires the licensee to ensure that all operating instructions which may affect safety are written down and complete. This expectation links with the claimed operator actions modelled in the PSA and the operating instructions. Therefore, ONR expects the PSA to be well documented with potential errors operators could make when following operating instructions modelled with high fidelity.
* **LC 28 - EIMT** – the licensee shall make and implement adequate arrangements for regular and systematic EIMT. Where available the PSA should be used to risk inform the maintenance schedules and testing regimes based on the significance of systems to safety.

1. Safety cases, including PSA, may be produced to support activities such as construction of new facilities, commissioning, modifications, and decommissioning. These activities, covered by LCs 19, 20, 21, 22 and 35, require safety documentation. Further guidance on use of PSA is contained in the TAG on 'Use of PSA and Probabilistic Insights' [2].

# Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides

## Safety Assessment Principles

1. This guide interprets ONR’s use of the PSA related SAPs, FA.1, and FA.10 to FA.14 [1]. This guide also addresses those aspects of the SAPs on ‘assurance of validity', AV.1 to AV.8, that are specifically applicable to PSA. This guide addresses the numerical targets related to PSA, namely targets 7, 8 and 9. A more detailed discussion on numerical target and their basis is contained in Annex 2 of the SAPs [1].

### Fault analysis: General – Design basis analysis, PSA and severe accident analysis – FA.1

“Fault analysis should be carried out comprising suitable and sufficient design basis analysis, PSA and severe accident analysis to demonstrate that risks are ALARP”. [1].

1. This principle outlines the inter-relationship between the three types of fault analysis, DBA, PSA and SAA and how in combination they address the range of potential initiating events (IEs) with nuclear safety significance off the site. As with DBA and SAA, the scope of PSA should be suitable and sufficient and used along with the other two fault analysis approaches to help demonstrate that risks are ALARP and to address SAPs Numerical Targets 7, 8 and 9.
2. The SAPs establish the expectation that safety cases for power reactors, or where there is significant complexity, or where the numerical targets may be challenged should include PSA. Detailed discussion on the assessment of the scope of PSA for nuclear facility’s other than power reactors is discussed in the TAG on 'Use of PSA and Probabilistic Insights' [2].

### 

### Fault analysis: PSA – Need for a PSA – FA.10

“Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis.” [1].

1. This principle sets the framework and requirements for a PSA study. PSA should assist designers in achieving a balanced and optimised design so that no particular class of accident or feature of the facility makes a disproportionate contribution to the overall risk. PSA is used by dutyholders to enable risk informed judgements on the safety of the facility, the risk profile, the risk importance of safety systems etc.
2. Further discussion on the assessment of the scope of PSA for nuclear facility’s other than power reactors is in TAG on 'Use of PSA and Probabilistic Insights' [2].
3. This TAG provides guidance on various technical aspects of PSA which will enable inspectors to judge that the expectation for a suitable and sufficient PSA has been met by the dutyholder.

### Fault analysis: PSA – Validity – FA.11

“PSA should reflect the current design and operation of the facility or site.” [1].

1. This principle establishes the need for each aspect of the PSA to be directly related to existing facility information, facility documentation or the analysts’ assumptions in the absence of such information. The PSA should be documented in such a way as to allow this principle to be met.
2. In addition, in order to meet this principle, the PSA should be kept living,   
   i.e. it should be updated periodically, as necessary to reflect the current design and operational features and to incorporate feedback from internal and external operational experience, improved understanding of physical processes or accident progression and advances in modelling techniques. Detailed discussion of assessment against the PSA elements related to FA.11 is contained in Section ‎5 of this TAG.

### Fault analysis: PSA – Scope and extent – FA.12

“PSA should cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults.” [1]

1. This principle relates to the scope of the PSA. Inspectors expectations in this area should be proportionate to the facility being assessed, taking risks, hazards, lifecycle and project status into account.
2. The scope of the PSA for new build NPPs should cover all significant sources of radioactivity at the facility (for example, fuel ponds, fuel handling facilities, waste storage tanks, radioactive sources, reactor cores, etc.), all types of IEs (for example, internal faults, internal hazards, external hazards) and all operational modes (for example, nominal full power/throughput, low power/throughput, shutdown, start-up, refuelling, maintenance outages).
3. Where a design is still undergoing development, for example, progressing through a Generic Design Assessment (GDA), the scope of the PSA should be proportionate to the stage of the project, the design information available and sufficient to enable the PSA to be used to adequately risk inform design development.
4. However, in assessing against the expectations of this principle for existing facilities, in particular the plants in operation and build to earlier standards, a proportionate approach is reasonable.
5. Where the offsite consequences are potentially significant, such as for an operating power reactor, the PSA should be at least to level 2 and include all external events (including beyond design basis events that could realistically lead to a significant offsite release (refer also to para. 618 of the SAPs [1]).
6. Detailed discussion of assessment against the PSA elements related to FA.12 is contained in Section 5 of this TAG.

### Fault analysis: PSA – Adequate representation – FA.13

“The PSA model should provide an adequate representation of the facility and/or site.” [1]

1. The aim of this principle is to ensure the technical adequacy and level of detail of the PSA is sufficient to ensure that it is realistic representation of the facility and/or site commensurate with its risk level. Inspectors should be satisfied that the PSA has a robust technical basis and thus provides a credible picture of the contributors to the risk from the facility. Best-estimate methods and data should be used as far as possible within the PSA. Detailed discussion of assessment against the PSA elements related to FA.13 is contained in Section 5 of this TAG.

### Fault analysis: PSA – Use of PSA – FA.14

“PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities”

1. The aim of this principle is to establish the expectations on what uses the dutyholder should make of the PSA to support decision-making and on how the supporting analyses should be undertaken. Some examples are provided in paragraph 661 of the SAPs [1]. Guidance and some examples to help demonstrate the various uses of PSA are provided in TAG on 'Use of PSA and Probabilistic Insights' [2].

### Fault analysis: assurance of validity of data and models – Theoretical models – AV.1

“Theoretical models should adequately represent the facility and site.” [1]

1. Theoretical models are used throughout the PSA, for example, reliability models (including CCF and human reliability models), models for the evaluation of the thermal-hydraulic or chemical behaviour, the progression of the accident and the transport of fission products, models for the analysis of structural integrity of containment and any other structures, models for the evaluation of the impact of the various isotopes on human health, etc.
2. SAP AV.1 is strongly linked to AV.2 discussed below and together aim to ensure that all the calculations that underlay the PSA are adequate to represent the facility. In this respect, these SAPs reinforce specific PSA SAPs FA.11 and FA.13 above. Relevant detailed discussion on assessment against the PSA elements related to AV.1 is part of Section 5 of this TAG.

### Fault analysis: assurance of validity of data and models – Calculation methods – AV.2

“Calculation methods used for the analyses should adequately represent the physical and chemical processes taking place.” [1]

1. Calculation methods are used in support of various tasks in PSA, for example, thermal-hydraulic analyses, analyses of chemical behaviour, accident progression analyses, analysis of structural integrity of containment and any other structures, fission product release and transport, analysis of health effects, etc. PSA software (such as Risk Spectrum, CAFTA, Sapphire etc) use a calculation algorithm to quantify the PSA models and to obtain the list of cutsets. The aim of this principle is to ensure that all the calculation methods used in the PSA adequately represent the real processes taking place in the facility and that the calculations are done as intended by the analysts. Relevant detailed discussion on assessment against the PSA elements related to AV.2 is part of Section 5 of this TAG.

### Fault analysis: assurance of validity of data and models – Use of data – AV.3

“The data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means.” [1]

1. Failure rate and probability data is the basis of the PSA; therefore, for the PSA to be an adequate representation of the facility, it should make use of data that can be demonstrated to be valid for the facility. Therefore, this SAP is viewed as a reinforcement of specific PSA SAPs FA.13 and FA.14.   
   The use of data in PSA, uncertainty in the input data, impact of data uncertainty on the overall PSA results, interpretation of this uncertainty in decision-making is part of discussion in Section 5 of this TAG. Relevant detailed discussion on assessment against the PSA elements related to AV.3 is part of Section 5 of this TAG.

### Fault analysis: assurance of validity of data and models – Computer models – AV.4

“Computer models and datasets used in support of the safety analysis should be developed, maintained and applied in accordance with quality management procedures.” [1]

1. Computer models and datasets are developed to support various tasks in PSA. The PSA model itself is typically a computer model with an associated database. Therefore, the relevance of this SAP cannot be stressed enough. The aim of this principle is to ensure that all the calculations that underpin the PSA are undertaken without error. For this, inspectors may wish to satisfy themselves that the dutyholders have put in place adequate procedures to develop, maintain and apply computer models and databases.
2. Generally, inspectors should expect that the Quality Assurance process applied to the PSA covers all items identified in SAP AV.4. Further guidance on the use of computer models in safety cases is provided in NS-TAST-GD-042 [7]. Relevant detailed discussion on assessment against the PSA elements related to AV.4 is part of Section 5 of this TAG.

### 

### Fault analysis: assurance of validity of data and models – Documentation – AV.5

“Documentation should be provided to facilitate review of the adequacy of the analytical models and data.” [1]

1. PSAs are generally large and complex safety analyses. Therefore, for them to be traceable, reproducible, verifiable, and updatable, they need to be documented in such a way as to ensure that each aspect of the PSA can be directly related to existing facility information, facility documentation or the analysts’ assumptions in the absence of such information. In this respect this SAP reinforces PSA-specific SAP FA.11 (Validity) addressed above. Relevant detailed discussion on assessment against the PSA elements related to AV.5 is part of Section 5 of this TAG.

### Fault analysis: assurance of validity of data and models – Sensitivity analyses – AV.6

“Studies should be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation.” [1]

1. Sensitivity analyses are a key aspect of the PSA because they are needed to provide confidence that the conclusions obtained from the PSA are valid despite the uncertainties associated with the supporting analysis and assumptions used in the development of the PSA. If the sensitivity analyses performed do not provide sufficient confidence in the validity of the conclusions of the PSA, reasonably practicable steps need to be taken to reduce the uncertainties associated with the model and data – this may include use of independent methods and computer codes, where appropriate, as indicated in the text accompanying SAP AV.6.   
   Relevant detailed discussion on assessment against the PSA elements related to AV.6 is part of Section 5 of this TAG.

### Fault analysis: assurance of validity of data and models – Data collection – AV.7

“Data should be collected throughout the operating life of the facility to check or update the safety analysis.” [1]

1. The validity and applicability of the IE frequencies, component failure probabilities, unavailability’s, etc., used in the PSA can only be assured if these are reviewed periodically using facility specific information.
2. Therefore, it is reasonable to expect dutyholders to put systems in place for collecting relevant data throughout the life of the facility and to use this data every time the PSA is updated as required, for example, by PSA SAP FA.11 and Assurance of Validity SAP AV.8. Relevant detailed discussion on assessment against the PSA elements related to AV.7 is part of Section 5 of this TAG.

### Fault analysis: assurance of validity of data and models – Update and review – AV.8

1. LC 15 requires the licensees to conduct periodic reviews of the safety cases for their facilities. These periodic safety reviews (PSRs) are normally carried out every ten years. However, a licensee's arrangements under LC 15 should also require interim reviews on a shorter-term basis taking into account the number and safety significance of modifications to the facility and/or changes to the safety case since the previous review as discussed in NS-TAST-GD-050 [8].
2. AV.8 should also be interpreted as highlighting the principle of Living PSA, in that ONR expects PSAs to be living analyses that constantly reflect the best estimate of the dutyholder on the reliability of components, plant availability, technical specification limits and conditions, testing and maintenance schedule, allowed outage limits, and current knowledge on plant behaviour analysed using modern analysis methods. In this regard, this principle reinforces the specific PSA principle FA.11 discussed above.

### Numerical Targets

#### Target 7: Individual risk to people off the site from accidents

1. The targets for the individual risk of death to a person off the site, from accidents at the site resulting in exposure to ionising radiation, are:

* BSL: 1 x 10-4 pa
* BSO: 1 x 10-6 pa

1. Target 7 address accident risks to the public, summed for all facilities on a site. ALARP considerations by dutyholders below the BSO should, however, not be ruled out.

### 

#### Target 8: Frequency dose targets for accidents on an individual facility – any person off the site

1. The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site are presented in Table 1.

Table 1 - Total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site.

|  |  |  |
| --- | --- | --- |
| Effective dose, mSv per annum | Total predicted frequency (/yr) | |
| **BSO** | **BSL** |
| 0.1-1 | 1 | 1 x 10-2 |
| 1-10 | 1 x 10-1 | 1 x 10-3 |
| 10-100 | 1 x 10-2 | 1 x 10-4 |
| 100-1000 | 1 x 10-3 | 1 x 10-5 |
| >1000 | 1 x 10-4 | 1 x 10-6 |

1. Target 8 sets expectations on levels of the frequencies of classes of accidents at individual facilities that could give rise to doses off the site within the specified bands. ALARP considerations by dutyholders below the BSO should, however, not be ruled out.

#### Target 9: Total risk of 100 or more fatalities

1. The targets for the total risk of 100 or more fatalities, either immediate or eventual, from accidents at the site in exposure to ionising radiation, are:

* BSL: 1 x 10-5 pa
* BSO: 1 x 10-7 pa”

1. Target 9 is intended to be used as a guide to assist in judging whether more detailed analysis is warranted. As with other numerical targets, Target 9 is a pragmatic approach to enable targeted and proportionate use of resources. ALARP considerations by dutyholders below the BSO should, however, not be ruled out. Further guidance to inspectors on Numerical Targets is provided in Section ‎5.16 and in the TAG on 'Use of PSA and Probabilistic Insights' [2].

## 

## Relationship with the WENRA Reference Levels

1. The Reactor Harmonization Working Group (RHWG) of the Western European Nuclear Regulators Association (WENRA) published Reactor Safety Reference Levels (RLs) in most recent version February 2021 [9].   
   They reflect expected practices to be implemented in the WENRA countries. As the WENRA members have different responsibilities, the emphasis of the RLs has been on nuclear safety, primarily focusing on the main safety functions for ensuring the integrity of the reactor core and spent fuel.   
   Issue O of these reference levels refers to Probabilistic Safety Analysis (PSA). This TAG is consistent with Issue O of the RLs. [Appendix 2](#_Appendix_2_-) presents the mapping between Issue O of the RLs and this TAG.

## Relationship with the IAEA Safety Standards

1. There is a significant amount of guidance through IAEA safety standards applicable to the regulatory assessment of PSA. As per the hierarchy of safety publications of the IAEA the Safety Fundamentals (SF) is the highest tier, followed by Safety requirements (SR) and then by the Safety Guides (SG). The guidance in this TAG is consistent with the expectations of the SF, SR and SGs. The IAEA publications available in the lower tiers such as safety reports, technical reports and TECDOCs contain more detailed guidance or case studies, however they have been subject to a lower level of governance within IAEA, and not routinely reviewed or updated. Such lower tier sources may still be relevant and useful when assessing PSAs, however care should be taken to confirm the applicability, relevance and provenance of the information.
2. The key IAEA documents which are useful for regulatory assessment of PSA are listed here:

* Safety Fundamentals, No SF-1 [10]
* Safety of Nuclear Power Plants: Design, SSR-2/1 (Rev1) [11]
* Safety Assessment for Facilities and Activities, IAEA Safety Standard Series GSR Part 4 (Rev 1) [12]
* Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants – IAEA Safety Standards Series No SSG-3 Rev 1 [13]
* Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants – IAEA Safety Standards Series No SSG-4 [14]
* 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, IAEA Safety Series 50-P-12 [15]

1. The IAEA publications which belong to the category of ‘practice/procedure’ series have historically enabled the performance of PSAs of existing/extant facilities. However, these have now been categorized as superseded publications due to updated safety guide publications. Some of these publications are listed below because the information contained could be of interest.

* Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1) – IAEA Safety Series No 50-P-4 [16]
* 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 – IAEA Safety Series No 50-P-8 [17]
* Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice – IAEA Safety Series No 50-P-7 [18]

1. Some lower tier sources from IAEA documents which may still be relevant and useful when assessing PSAs, are as follows:

* Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA- TECDOC-1804 [19]
* Regulatory Review of Probabilistic Safety Assessment (PSA) – Level 1, IAEA-TECDOC 1135 [20]
* Regulatory Review of Probabilistic Safety Assessment (PSA) Level 2 – IAEA – TECDOC - 1229 [21]
* Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Units, Safety Report Series No 96 [22]
* Risk Aggregation for Nuclear Installations, IAEA TECDOC -1983 [23]
* IAEA, “Safety Report on Applicability of Safety Standards on Non Water Cooled Reactors and Small Modular Reactors. https://preprint.iaea.org/search.aspx?orig\_q=reportnumber:IAEA-PC--8839,” 2022. [24]
* Case Study on Assessment of Radiological Environmental Impact from Potential Exposure, IAEA TECDOC-1914 [25]

## 

## Other relevant sources for good practice

1. ONR assessments have recognised some of these standards as a source of relevant good practice for nuclear reactor facility PSA. ONR has not conducted a comprehensive review of the standards, and not all have been used to support PSAs assessed by ONR, however they are used by a wide range of vendors, designers and operators worldwide. Therefore they are likely to be a good source of relevant good practice and help inspectors understand the standards common applied to develop PSAs internationally.
2. Some documents by ASME, EPRI, USNRC and NEA which may be considered sources of relevant good practice and are referenced within this TAG are as follows:

* ASME, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-S-1.1, 2022 [26]
* ASME, Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), ASME RA-S-1-2, 2014 [27]
* ASME, Standard for Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to support Nuclear Installation Applications, ASME RA-S-1-3, 2017 [28]
* USNRC, Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, NUREG/CR-6268 Rev 1, 2007 [29]
* USNRC, Industry-average performance for components and initiating events at U.S. commercial nuclear power plants, NUREG/CR-6928, 2007 [30]
* EPRI/NRC-RES, Fire PRA Methodology for Nuclear Power Facilities, NUREG/CR-6850, 2005 [31]
* IEC, Functional Safety of Electrical/Electronic/Programmable Electronic Safety related systems - Part 3 Software Requirement, IEC 61508-3, 2010 [32]
* EPRI, Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment, TR-1019194, 2009 [33]
* EPRI, Seismic Probabilistic Risk Assessment Implementation Guide, EPRI Report - 3002000709, 2013 [34]
* EPRI, Screening, Prioritization and Implementation Details (SPID) -Seismic, Report 1025287 [35]
* OECD/NEA, “https://www.oecd-nea.org/jcms/pl\_58495/status-of-site-level-including-multi-unit-probabilistic-safety-assessment-developments,” [Online] [36]
* NEA/CSNI, “A Joint Report on PSA for New and Advanced Reactors, NEA/CSNI/R(2012)/17,” 2012. [37]

# Advice to Inspectors

## Introduction

1. This section of the TAG aims to provide guidance on the assessment of a PSA which generally is associated with SAPs FA.10 to FA.13. The guidance in this section is presented in the order in which a typical PSA is developed.
2. This section is split up into several parts dealing with the different elements of a PSA. The sections are generally aligned with those used within IAEA Safety Guides on PSA [13] [14]. Each part contains a general overview of the topic followed specific points of guidance to ONR inspectors to consider in their assessment. It should be noted that all these points need not be met fully in each instance. It is left to the judgement of the individual inspector to identify both the scope and depth of assessment. Inspectors should judge the adequacy of the submission taking into account the context of the facility being analysed.
3. PSAs are often large and complex, therefore any assessment may lead to observations of shortfalls against the guidance within this TAG. This TAG takes in consideration the intelligence gathered by ONR through the assessment of different PSAs, such as, the one’s performed after the start of plant operations (as in the case of AGRs), that in the construction stage (as in the case of SZB), or those in design stage (as in the case of generic design assessments (GDAs) such as performed for EPR, AP1000, ABWR, and HPR1000). Inspectors should be aware of the need for a graded approach to compliance with the regulatory expectations contained in this TAG. It may be proportionate and reasonable in different situations to look at the wider context of the safety case, relative risk, remaining life, and other justifications in forming regulatory judgements for the facility.
4. The guidance provided in this section is generally applicable to the assessment of PSAs for all types of nuclear facilities. More specific, and detailed assessment expectations for review of PSAs for NPPs are given in [Appendix 1](#_Appendix_1_-) to this TAG. However, much of the guidance provided in [Appendix 1](#_Appendix_1_-)can also be applied to other types of facilities, inspectors may wish to use [Appendix 1](#_Appendix_1_-)at their discretion for the assessment of PSAs for facilities other than NPPs.
5. The guidance in this TAG should be used along with other widely accepted standards/guidance published by IAEA, USNRC, EPRI and ASME if applicable. The relevant standards/guidance often represent RGP in the context of performance of PSA. These have been listed in sections ‎4.20 and ‎4.21**.** of this TAG and also specifically cross referred where relevant.
6. The following topics are covered within this section:

* PSA Scope
* PSA Methodology
* Derivation of Initiating Events including Internal and External Hazards
* PSA model
* Protection and Mitigation Systems Modelling
* Accident Sequence Analysis
* PSA Input Data
* Digital Control Instrumentation in PSA
* Human Reliability Analysis
* Analysis of internal and external hazards
* Non Reactor PSA (such of Fuel Route)
* Analysis of other operating modes
* Quantification of the analysis
* Level 2 PSA
* Level 3 PSA
* Sensitivity and Uncertainty studies
* Presentation of the results of the PSA
* Multi-unit and site-level considerations
* PSA of Novel Designs of Nuclear Power Plants

## PSA Scope

1. Safety assessment principle FA.10. sets expectations and provides guidance on the need for a PSA for a nuclear facility and the scope of such an analysis. Adequate scope of PSA is important to support and inform the uses/applications of the PSA.
2. The scope of the PSA should be broad enough so that the results allow a meaningful comparison of risk from different aspects of the facility. If the scope is incomplete there is a risk that the insights from PSA will be skewed towards addressing aspects that have been modelled, at the expense of aspects which have not.
3. Complex new build facilities should aim to develop a full scope PSA. The level of detail may be lower for existing facilities if they can argue that the effort to provide more detail would be disproportionate to the benefits obtained. Inspectors should satisfy themselves that any limitations in scope are soundly based upon the hazard and complexity of the facility and the balance between the benefits of performing additional analysis and the cost of doing so.
4. The TAG on 'Use of PSA and Probabilistic Insights' [2] provides wider guidance on scope, including aspects which inspectors should consider when assessing scope and applicability to non-nuclear power plant type of facilities and potential risk informed applications.
5. Specific assessment expectations for review of the scope of the PSA for NPPs can be found in Table A1-1.2 (PSA Scope) of [Appendix 1](#_Appendix_1_-).

## General aspects of PSA

1. The starting point for assessing a PSA is to develop a familiarity with detailed description of the design and operation of the facility and its associated protection systems, and their behaviour in fault conditions.   
   This would typically include facility descriptions, fault schedules, drawings, operating instructions, safety reports and transient, radiological and any other deterministic analyses that support the PSA.
2. The inspector may consider whether:

* the detailed design of the facility and its equipment to which the PSA refers is identified;
* sufficient information is provided on the design and operation of the facility and on its behaviour in fault conditions to support the PSA. (The inspector should consider carrying out a site visit(s) to confirm a selection of design and operating assumptions used in the PSA. If the facility is in design/construction phase a deep dive workshop to understand the supporting analysis and assumptions in response to fault conditions, could be considered);
* the methods of analysis used in the PSA are defined and are suitable to meet the objectives of the analysis;
* the PSA has been fully documented. The objectives and content of PSA documentation is well discussed in the IAEA references [13] [14];
* the PSA has been carried out in accordance with written QA procedures. One example for the expectations of quality assurance is explained in the ASME standards for Level 1/2 PSA [26] [27];
* the PSA has undergone an independent assessment/peer review and the findings are acceptable. One example for independent peer review expectations are well discussed in the ASME standards for PSA [26] [27].

1. PSA modelling is expected to be based on best-estimate methods and data for the transient analyses, accident progression analyses, source term analyses, radiological analysis and any other deterministic analyses that support the PSA. Where no credible best estimate is possible, reasonable assumptions should be made and the sensitivity of the risk to these assumptions should be established. The term “best-estimate” is defined in section ‎2.1 of this TAG.
2. PSA studies should identify the relative contribution to risk from the features of the facility and allow a judgement on the balance of the design. This is ideally achieved if each component of the study is treated in a best estimate manner. If one element of the study contains a large measure of conservatism and dominates the resulting risk calculation, evaluating the benefit from improving the reliability of that element, or indeed other elements, is more difficult. Therefore, while the use of conservative design basis analysis within the PSA can be justified to show either that the risks are low, or to act as a screening mechanism for future best estimate analysis, risk-informed decision making could be severely compromised using when conservative assumptions.
3. Specific assessment expectations for review of the adequacy of the documentation provided in support of each technical task of the PSAs for NPPs can be found in the various Tables of [Appendix 1](#_Appendix_1_-).
4. An important stage in developing a PSA is developing the PSA methodologies. PSA methodologies should detail how each individual aspect of the PSA is going to be developed and the end states which will be analysed.

## Derivation of Initiating Events Including Internal and External Hazards

1. A list should be included providing identification of all the potential IEs within the scope of the PSA which could lead directly or in combination with other failures to a release of radioactive material. A sample methodology for internal and external hazards based initiating events for LWRs and BWRs is given in IAEA SSG-3 [13]. It also provides a list of various sources to be considered to derive a comprehensive list of initiating events, including internal and external hazards for which the PSA is being developed.
2. For internal and external hazards, suitable screening of the exhaustive list of hazards is expected with appropriated screening criteria (based on risk significance of the hazard to the site and design of facility). The result of this screening should be a list of hazards to be considered in the PSA.   
   Hazards screening in important to determining the scope of the PSA and has a large impact on resourcing and cost of development of the PSA
3. The inspector may consider whether:

* the list of IEs covers all the sources of radioactive material in the facility;
* the quantity, form and location of all radioactive material in the facility is identified;
* if any sources of radioactive material are not included in the PSA, justification is given that this would not lead to a significant contribution to the risk;
* the list of IEs covers all the operating modes of the facility;
* if any operating mode is not covered in the list of IEs, justification is given that the contribution to the risk is small during this operating mode;
* the IE identification process is shown to be comprehensive so that all possible IEs are identified;
* the list of IEs includes partial failures as well as total failures;
* all relevant internal hazards are listed;
* all relevant external hazards are listed;
* derivation of a screened-in list of hazards through systematic screening of internal and external hazards
* each IE is defined clearly and the causes of each IE are identified;
* features such as administrative systems, control systems, interlocks etc. which limit the frequency of an IE are identified;
* failures of protection system equipment which can occur as a consequence of an IE are identified;
* a list is prepared of IEs which are screened-out from the list of IEs because of very low frequency or "incredibility", with reference to the justification;
* full records of the IE identification process are available and are of suitable quality;
* any IE screening criteria adopted are clearly described and justified

1. Specific assessment expectations for review of the adequacy and completeness of the list of IEs considered in the PSAs for NPPs can be found in Tables A1-2.1 (identification and grouping of initiating events), A1-2.7 (analysis of hazards) and A1-2.8 (low power and shutdown modes) of [Appendix 1](#_Appendix_1_-).

## 

## PSA Model

1. The PSA model, often represented as event trees with linked system fault trees, is expected to be of the level of detail that is sufficient to ensure that it is a realistic representation of the plant. It is expected that the logic is correct, that the dependencies are captured, and that the data used is applicable to the boundary selected for each (basic) event in the PSA.   
   Model simplifications (for example, modelling of bounding sequences, use of super-components) and their justification should be clearly described; particular attention should be paid to ensuring that dependencies are not missed due to such simplifications. As noted in SAPs para., 652 [1], the PSA should model events until a safe stable state is reached and justify the mission time accordingly.
2. PSA should identify systematically and comprehensively the complete range of sequences leading to the “undesired” consequences that may occur.   
   This makes no distinction regarding the frequency at which each sequence is estimated to arise, rather it seeks to ensure that all conceivable routes to a release are systematically identified. To address the relevant numerical targets of the SAPs, the PSA should model accidents with high consequences as well as those that have a higher frequency but lower radiological consequence.
3. The PSA model is expected to account for all contributions to the risk, including, but not necessarily restricted to: random component individual failures, components which are failed by the IE, common cause failures (CCFs) (and, as necessary, other dependent and consequential failures), unavailability’s due to testing and maintenance, pre-initiating event human errors (for example, misalignments and mis-calibrations), human errors that lead to IEs and human errors during the course of the accident sequences (including misdiagnosis, decision errors, omission errors and commission errors). The potential dependencies between separate human activities (either by the same or by different operators) should be analysed and reflected in the models and probabilities used.
4. Computer models are developed to support various tasks in PSA, for example, for derivation of success criteria (applied to system success definition), accident progression analyses (applied to event tree modelling and operator action timings), fission product release and transport, analysis of structural integrity of containment and any other structures, etc. The PSA itself comprises a computer model and an associated database.   
   Therefore, the relevance of SAP AV.4 on assurance of validity of data and model applies here. The aim of this principle is to ensure that all the calculations that underlay the PSA are undertaken without error. For this, inspectors may wish to satisfy themselves that the dutyholders have put in place adequate procedures to develop, maintain, and apply computer models and databases.
5. These procedures should cover verification, validation, or qualification of computer codes, as appropriate, for the specific design of the facility.   
   The procedures should also require the dutyholder to identify the degree of accuracy and uncertainties associated with the selected computer codes and to ensure that the codes are only used within their limit of applicability and by adequately trained users. In addition, the procedures should require the dutyholder to ensure that the modelling of the plant inputted as underlying basis for the calculations and the input data files are auditable and are verified. Inspectors may choose to review or audit these procedures and/or seek evidence of their correct application by the dutyholder.

## Protection and Mitigation Systems Modelling

1. The PSA should identify the safety/protection/mitigation systems which are required to operate in response to the IEs (shown in the event trees) and identify the success criteria for each of the safety/protective/mitigative functions of such systems.
2. The accident sequence analysis identifies combinations of IEs and failures of safety systems and then considers the failures of these systems down to a lower level to identify the combinations of basic events within the various safety systems or support systems which could lead to the failure. The basic events modelled are expected to include component failure, CCF, component unavailability during maintenance or test and operator error.
3. The inspector should assess whether in response for each IE (shown in the event trees) the following is considered:

* the safety functions have been identified;
* the minimum safety systems requirements to achieve the safety functions have been identified;
* the minimum protection system requirements are consistent with any deterministic / transient analysis presented;
* for automatic protection actions, the parameters and systems used to initiate the action have been identified;
* for manually initiated protection actions, the alarms and indications which would alert the operator to the need for the action are identified

1. The usually followed method of safety/mitigative system analysis is fault tree analysis; other techniques are acceptable but may need additional scrutiny.
2. In assessing the safety/mitigative system analysis, the inspector may consider whether:

* the systems failure analysis covers all the failure states identified by the accident sequence analysis;
* the analysis has been carried out to a low enough level of detail (for example, individual component level) so that the design and operation of the system is adequately modelled;
* all the relevant failure modes of protection system equipment have been included;
* where components have been grouped together in the analysis (for example, in “super-components”), failure of each of the components in the mode specified has the same effect on the system and justification is clearly documented;
* the systems failure analysis models all the support systems required and that all interdependencies due to common services have been represented;
* the systems failure analysis takes account of consequential failures which could occur due to the IE or hazard;
* CCFs are included in the models at an appropriate level and that the probability given to each CCF has been derived on a best-estimate basis;
* all operator errors which can contribute to the failure of a system credited in the PSA have been identified and modelled in the analysis, with due consideration of dependencies;
* the unavailability of components, trains of systems or the entirety of systems during periods of maintenance or testing has been addressed in the analysis.

1. Specific assessment expectations for review of the adequacy of the credited safety/protective/mitigative systems in PSAs for NPPs can be found in Table A1-2.2 and A1-2.4 (Accident sequence development: determination of success criteria, and System analysis) of [Appendix 1](#_Appendix_1_-).

## Accident Sequence Analysis

1. The next stage of the PSA is the accident sequence analysis which models the behaviour of the facility for the IEs. The analysis should cover all possible combinations of success or failure of the protection/mitigative systems to perform the safety functions and should identify the accident sequences which involve failure to maintain the facility within safe limits.
2. The events or functions that are identified in the accident sequences will relate to the success or failure of the safety systems and human actions taken in carrying out the safety functions required for the groups of initiating events. The end points of the accident sequence models will correspond either to a safe stable state where all required safety functions have been performed successfully or to core damage (for the reactor) or to fuel damage (for the fuel pond). The inspector may check that, for each IE (and the developed event tree):

* the accident sequence analysis covers all the safety functions required and all the combinations of protection/mitigative system equipment which can operate to perform the safety functions;
* the accident sequence analysis takes account of all the functional dependencies between safety functions and protection/mitigative systems;
* the accident sequence analysis covers all the mechanisms which could lead to failure of the physical barriers such as a reactor pressure vessel or the containment;
* the accident sequence analysis covers the factors which affect the release and transport of radioactive materials to the environment and their effects on humans;
* sufficient radiological analysis is available to justify the categorisation of the end-points of the accident sequence analysis or that best-estimate assumptions have been made;
* the transient, radiological and other deterministic analyses used to support the PSA models do not contain undue pessimisms (these should preferably be best estimate);
* where IEs are grouped, the frequency is the sum of the individual IEs grouped, and the consequential impact on safety systems is represented by the most onerous one. Such simplifications are often conservative. Care needs to be taken to avoid gross conservatism, since it could affect the conclusions drawn from the analysis and thereby limit the usefulness of the PSA to support decision-making.

1. The frequency of occurrence and consequences of each of the fault sequences identified should be estimated. For quantification of the Level 1 PSA accident sequences, cut-offs will need to be specified to manage the time taken for the analysis. The usual approach is to set cut-offs in such a way so as to justify that a cut-off is set at a sufficiently low level that the overall result from the Level 1 PSA converges and does not lead to any under estimate of the core/fuel damage frequency.
2. Specific assessment expectations for review of the adequacy of the grouping of IEs in PSAs for NPPs can be found in Table A1-2.1 of [Appendix 1](#_Appendix_1_-). Specific assessment expectations for review of the accident sequence analysis in PSAs for NPPs can be found in Table A1-2.3 of [Appendix 1](#_Appendix_1_-)

## PSA Input Data

1. The PSA model, requires data to arrive at the meaningful quantitative results. This data pertains to frequencies of initiating events, component failure probabilities/frequencies, component outage frequencies and durations, maintenance – periodic, preventative and repair information, and common cause failure parameters.
2. There are multiple sources for component failure, data initiating event frequency data, common cause failure data, and other data used for PSA input. There is a hierarchy of data sources, in descending order of preference:

* Site specific data.
* Data from the same fleet of stations, for example, AGRs, French PWRs.
* Generic Nuclear Industry Data – Typically from NUREGs [38] [30], T-Book (Swedish PSA database), ZEDB (German PSA database) etc.
* Generic non-nuclear Industry Data – Oil and Gas, Process industry etc.
* Manufacturers Data.

1. Relevant good practice for PSA data is for site specific data to be informed by fleet or generic data using a justified mathematical technique, such as Bayesian update of generic data with facility-specific data as described, for example, in [38].
2. Data used in PSA should be best estimate where possible. When data used in PSA is linked only to classification of the system, it would not be best estimate. There are many sources of uncertainty in PSA, accuracy and applicability of data is one of them
3. Where facility/site specific data is not available, use of generic data may be acceptable providing it is shown to be appropriate to the design and operating conditions of the facility and it relates to a relevant and sufficiently large population. The source of the data, the sample size and the uncertainty in the data should be specified. If changes to the source data are made to take account of differences between the available data and the plant conditions, these should be justified.
4. Where no relevant statistical data are available, judgements should be made, and their bases stated. Particular attention should be paid to determining the sensitivity of the results of the PSA to such judgements.   
   Ad-hoc judgements not following a robust and systematic process should generally attract inspector’s scrutiny.
5. When models are used for the calculations of probabilities in the PSA, the methodologies used should be justified and should account for all the key influencing factors. In particular:

* The methodology used for the calculation of probabilities of structural failures should be justified and the details of the analysis should be transparent. If use is made of data from available structural (for example, pipework) failure databases, the sources of data and the way in which the data has been used should be clear and the applicability of the data should be justified. If use is made of probabilistic fracture mechanics codes, advice from the Structural integrity specialist inspector (also refer NS-TAST-GD-016 (metallic structures) [39]) may be sought on the adequacy of the codes and validation against operational experience and/or experiments. The range of loads and combinations of loads that could lead to the structural failures of concern should be adequate to represent the conditions which are possible for the facility under evaluation.
* Guidance for control & instrumentation system modelling accounting for both hardware and software failures has been discussed in Section ‎5.9.6
* Analyses to estimate the probability of occurrence of phenomena (for example in the severe accident portion as applied to Level 2 PSA) should be performed in a systematic and transparent manner taking account of up-to-date information from an appropriate range of sources about the phenomena. NS-TAST-GD-007 on Severe Accident Analysis provides guidance on the identification of the relevant severe accident phenomena and expectations on the analyses [40]. Similarly appropriate guidance for support to Level 2 PSA on ‘Radiological Source Terms and Accident Chemistry’ is available in NS-TAST-GD-089 on Chemistry Assessment [41].

1. In assessing the PSA data used in initiating event frequencies, failure probabilities and other parameters in PSA, the inspector may sample to consider whether:

* data is provided for all the basic events and IE frequencies included in the PSA;
* the data provided is preferably best estimate and appropriate for the use made of it in the PSA;
* where use is made of operating experience data in calculating IE frequencies and component failure rates, and the event is a potentially important contributor to the risk, there is an adequate discussion of the relevance of the data and the statistical uncertainty;
* where insufficient directly relevant data are available, the source of any quoted generic data and the basis of any judgements are stated;
* for IE frequencies:
  + the data covers all the causes of the IEs which have been identified;
  + where the IE frequency has been calculated from failure data for the causes of the fault, the data is applicable for this use and has been combined correctly to derive the frequency;
  + where no relevant operating data is available and judgement has been used to assign the IE frequency, the basis for this judgement has been stated and shown to be valid, as far as possible;
* for component failure rates (or probabilities)
  + the boundaries of the component for which the data is specified are defined;
  + the data covers all relevant failure modes of the component;
  + the data used corresponds to the component in terms of type, manufacture, operating environment, usage and maintenance regime;
  + the form of the data is suitable - that is, a failure rate per unit time or a failure probability per demand is given as appropriate for running or standby components;
  + where a test interval is used to change a failure rate per unit time to a failure probability per demand, there should be a reference to the relevant testing schedule and procedures;
  + where a component is required to operate continuously after a fault, the required period of operation is defined and justified by reference to the supporting deterministic analysis;
* for component unavailability’s:
  + the data covers all causes of component unavailability including tests (scheduled and unscheduled), maintenance (scheduled and unscheduled) and repair;
  + justification is given that the frequency and duration of the component unavailability’s adequately represents typical facility operation;
* For Common Cause Failures (CCFs):
  + The approach selected for the CCF modelling and for CCF parameter estimation should be justified and should be adequate to represent any level of redundancy present in the specific design of the facility. The consideration of coupling mechanisms and facility specific defences against CCF should be traceable. The applicability of the CCF data sources used should be demonstrated. Relevant international standards for CCF modelling are NUREG/CR-6268 [29] and NUREG/CR-5497 [42].
  + where numerical values are derived through engineering judgement, adequate justification is given that this reflects the potential for common cause failures to occur. The engineering judgement should take account of layout, segregation and any other measures adopted to reduce the likelihood of a common cause failure.
  + SAP EDR.3 addresses deterministic consideration of CCFs and discusses the deterministic expectation for modelling of CCFs. The requirement of additional regulatory scrutiny where the claim for CCF is below 1E-5 applies to deterministic principles for design of systems with redundancy. Probabilistic modelling of CCFs using appropriate parametric models such as alpha, beta or multiple Greek letter, is expected to be on a best-estimate basis aligned international standard guidance and data sources, such as NUREG/CR-6268 [29] and NUREG/CR-5497 [42] .
* the measures proposed to ensure that the reliabilities claimed for components and systems will be achieved and/or maintained, are stated and evidence is available to demonstrate the adequacy of any such measures;
* the possibility of component failure rates or unavailability’s increasing with time, for example, through ageing, is considered.

### Passive Safety features

1. Passive safety features (i.e., those that take advantage of natural forces or phenomena such as gravity, pressure differences or natural heat convection) have been in use in nuclear power plants to accomplish safety functions without requiring an active power source for many decades.
2. Systems based on gravity and pressure differences (for example, reactor scram or accumulator injection) are generally able to be tested during commissioning and operation and their reliability can be established from data (for example, from a fleet of similar plants). These types of systems have been modelled in PSAs for many years and are not typically novel.
3. Systems based on natural convection have historically been backups for frontline active systems. Historically passive convection systems have been assumed to be highly reliable and have not been modelled in PSA. The optimism associated with this was typically small due to the large number of active systems also claimed prior to the passive ones (for example, active feed water systems to promote natural circulation in the primary circuit).
4. These types of systems are becoming more common in the latest designs of reactors and are being claimed as highly classified SSCs to carry out post-trip cooling of the reactor or post-accident cooling of the containment without reliance on active systems. These passive convection systems have smaller driving forces than an equivalent active system. This means that there is the potential for these systems to fail due to blockages, leakage, hazards, non-condensable gases or aging related changes in materials amongst others.
5. Modelling of passive systems in PSA should be considered in the same way as modelling of active systems. However, it is recognised that quantification of reliability and understanding of failure modes may be more challenging. Inspectors should focus attention on modelling of passive systems where significant claims are being placed upon them or where they are significant contributors to the risk profile.
6. Passive systems can be analysed via physical test rigs or by numerical analysis using thermal-hydraulic codes. Some passive systems may not be able to tested during commissioning as easily as those based on gravity and pressure differences which can lead to dutyholders using numerical analysis to support their claims. Where evidence from test rigs or numerical analysis is used inspectors should confirm that the systems are substantiated by suitable analysis covering the full range of accident conditions for which they are required.
7. IAEA TECDOC 1624 [43] provides an overview of the types of passive systems that can be used for core decay heat removal and containment cooling and pressure suppression. The TECDOC provides an overview of the types of phenomena that can lead to failure of passive systems. IAEA TECDOC-1752 [44] provides an overview of methods for analysing the reliability of passive systems. Research on passive systems safety is currently being progressed by the IAEA and other international organisations.
8. EPRI study on passive safety systems [45] presents a formal, comprehensive analysis approach for such systems that are characterized as possessing high risk significance and high phenomenological complexity. The approach uses a structured search of failure scenarios using existing techniques such as FMEA and HAZOP for the passive systems. It also utilizes limited expert judgment as an integral part of the search process, and draws upon existing expert elicitation techniques common in fields such as seismic PRA and second-generation human reliability analysis. Ultimately, the goal of the comprehensive analysis approach is to estimate the failure probability for the passive system.
9. When assessing the modelling of passive systems in the PSA, close collaboration with Fault Studies inspectors is encouraged.
10. Specific assessment expectations for review of the PSA input data in PSAs for NPPs can be found in Table A1-2.6 (Data Analysis) of [Appendix 1](#_Appendix_1_-).

## Digital Control Instrumentation in PSA

### Introduction

1. Nuclear facilities in the UK have traditionally included control and instrumentation (C&I) systems that were analogue in nature, often based upon relays and other similar components. These systems were simple and with failure modes well understood enough to be modelled comprehensively in PSA, for example the Post-Trip Sequencing Equipment at the AGR power stations composed of hundreds of relays is modelled explicitly in the AGR PSA models.
2. Safety-related control and instrumentation (C&I) systems in new nuclear facilities often incorporate digital C&I (DCI) technology. DCI is increasingly being adopted in legacy plants and facilities in the UK as existing analogue equipment becomes obsolete. General experience in conducting PSA for nuclear facilities shows that DCI is often a significant risk contributor, similar to that of analogue C&I systems or higher risk due to conservatisms.
3. Modelling of DCI in PSA is complex due to the contributions of both software and hardware reliability. Hardware reliability is affected by random failures which is numerically quantifiable[[1]](#footnote-2) based on equipment and component testing, operational use and experience, etc. Software reliability is predominantly affected by systematic failures, which are caused by inherent flaws in software, either in its requirement specification, design/ implementation or aspects of the software development lifecycle. Numerically quantifying software reliability is discussed in detail in Sections ‎5.9.6 to ‎5.9.10.
4. SAP FA.13 [1] states that ‘The PSA model should provide an adequate representation of the facility and/or site’. As noted in Section ‎5.5 the level of detail of PSA should be sufficient to ensure that it is realistic, that the logic is correct, that the dependencies are captured, and that the data used is applicable to the boundary selected for each (basic) event in the PSA.
5. ONR have carried out research project to review the international state of the art in C&I modelling and quantification of software reliability [46]. Based on this research project output, workshop with industry practitioners, and internal workshop with C&I inspectors the guidance as available internationally is summarised below. Additionally, the experience gained through ONR assessments is also summarised.

### International Guidance – IAEA

1. The latest revision of Specific Safety Guide 3 on Level 1 PSA [13] provides guidance on software-based systems:

* The PSA should consider reliability assessment of software-based systems where these are claimed as SSCs or where they can cause initiating events;
* A graded approach should be used to determine the scope and method used for reliability assessment based on the risk importance of the SSCs;
* The reliability assessment of operator interface systems should take account of other C&I system failure dependencies through normal PSA fault and event tree modelling;
* The reliability assessment of software based systems should cover both hardware and software components as well as configuration data for the programmable logic devices of those systems. Modelling the reliability of software based systems is a challenge because the standard statistical approaches have limited applicability for the software modules;
* The scope of the DCI system and its PSA related tasks should be identified. Spurious actuation should be considered. Interactions between different DCI systems should be considered;
* The analysis of a software based system should be detailed enough to capture the functionally relevant failure modes of the system and to capture the dependencies between systems;
* In the analysis of programmable components (for example, processors, communication modules, sensors, actuators), the starting point should be to consider both the hardware and software parts of the components (for example, modules, subcomponents), and then to decompose this hardware and software further if necessary and feasible, and if applicable data are available;
* The reliability of the hardware modules should be assessed using standard techniques, as long as these techniques can model the system behaviour, failure modes and dependencies identified;
* The reliability assessment of software modules should include an assessment of existing operating experience (including from other nuclear power plants or from other industrial applications) and an assessment of the development processes (including the validation and verification process) to gain as much confidence as possible in the reliability estimates provided. The reliability assessment of software modules still poses a challenge, with recognised industrial practice still to be established;
* The reliability assessment of programmable systems, including communications networks, should include an assessment of intersystem common cause failures. Attention should be paid to computer systems carrying out similar or the same functions. If credible dependencies in the hardware and software of the two computer systems are identified, they should be taken into account in the Level 1 PSA;
* IAEA Safety Standards Series No. SSG-39 [47], Design of Instrumentation and Control Systems for Nuclear Power Plants states that insights gained from probabilistic safety assessment should be considered in the design of C&I systems. The derivation of instrumentation and control system reliability should be substantiated and based on internationally recognised approaches. Assumptions should be documented and justified.

### US NRC Research

1. The US NRC have a long running research program into software reliability using a variety of methodologies, including dynamic fault trees, dynamic event trees, Markov models, Bayesian methods and petri-net methods.   
   This research programme is ongoing and is summarised on the NRC website [48]. The goal of the research programme is to develop additional technical methods and tools to better quantify risks and integrate risk insights into technical reviews and inspections of digital systems. At present the tools and techniques under development by the NRC are not required to be used by U.S. industry.

### Modelling of C&I systems in PSA

1. Existing PSA models can represent DCI in varying levels of detail, ranging from simple ‘super-component’ events to more complex fault trees separating hardware and software elements. The level of detail of the PSA modelling should be proportionate based on the risk significance of the systems being modelled and how the PSA is going to be used. For example, a conservative assessment of software reliability may be acceptable to demonstrate that numerical targets have been met, but if a PSA is being used to risk inform design or as a risk monitor then a more refined approach will be required.
2. The level of detail expected in a PSA will depend on the evidence available at different project stages, the related uncertainty, and the importance of recording and validating assumptions. For example, during GDA a requesting party is unlikely to have evidence to fully substantiate a best estimate claim, but could have confidence that one will be made in future. This could be supported by sensitivity studies to show the impact if the claim was not substantiated in the future.
3. The following guidance is applicable to development of C&I modelling in PSA:

* Dutyholders should aim to use their PSA to understand where there may be vulnerabilities in their design due to software and hardware failures. To do this the PSA needs to be developed to a suitable level of detail to be able to show where vulnerabilities may lie;
* The PSA modelling should be sufficiently detailed to reveal dependencies between failures of C&I systems and other systems. Previous failures in the accident sequence should be carried forwards to affect SSCs claimed later in a sequence;
* Where C&I failures would affect the ability of the operators to diagnose or respond to faults this should be represented in the PSA model;
* Spurious initiation of C&I systems and any faults this could lead to should be modelled in the PSA. Dependencies between spuriously initiated C&I and C&I systems claimed to respond to the spurious initiation should be modelled;
* Dutyholders should seek to understand which C&I failures would be detected and which would be undetected. They should also seek to understand which failures are dangerous and not dangerous.

1. The approach laid out in EPRI 1021077 [49] provides an example of a useful modelling approach. The document lays out the structure of modelling instrumentation units (sensors and actuators), computing units (signal processing and voting logic) and communication units as separate aspects of the model. This type of treatment is appropriate for reactor protection systems and similarly complex systems. Where a dutyholder has installed simpler smart devices, this approach is likely to be disproportionate.
2. During the assessment of C&I PSA modelling inspectors are likely to see reliability values stated to multiple significant figures. This is different to the approach typically seen in deterministic C&I assessments which will assign reliability values on an order of magnitude basis. Inspectors should be wary of implied accuracy when assessing C&I reliability values. However, the use of multiple significant figures to represent reliability may be the output of a particular method for calculation of reliability. These figures should not be dismissed based on the precision of the value. Values used in PSA should not be artificially rounded if doing so affects the PSA results or insights. Relative differences between values at greater precision than typical high confidence values for the DCI often provide useful risk insights. The user should remain aware that the error in the estimated value is dominated by the C&I input value and typically exceeds this precision.
3. Once a suitably detailed PSA model has been developed the PSA can be analysed to show which aspects of the C&I system are risk significant. It is expected that a graded approach may be used, where more risk significant aspects of the C&I system have more effort put into quantifying a best-estimate reliability.

### Modelling approaches for C&I Hardware

1. Typical PSA models in the UK model the hardware aspects of C&I systems in varying levels of detail. The approach to modelling C&I hardware should be similar to modelling of electrical or mechanical equipment, with failure rates based on OPEX and other data sources, taking the testing and maintenance regime into account.
2. The level of detail expected for C&I hardware modelling should be linked to risk significance and the availability of design information. It is expected that more risk significant systems should be modelled in greater detail. As facility designs increase in maturity from design to commissioning to operation it is expected that the level of detail of C&I in the associated PSA will also be improved.
3. Similarly to the modelling of electrical or mechanical systems, the use of super-components should be justified, and where super-components are used to represent C&I systems the contents included within the boundary should be clearly identified and dependencies with other systems should be captured.

### Modelling approaches for C&I Software

1. Modelling of software failures in PSA has traditionally been optimistically ignored, or conservatively assessed using reliability values linked to Safety Integrity Levels derived from IEC 61508 [32] or equivalent standards. These high-confidence values have then typically been assigned directly to basic events in PSA models. These high-confidence values are not intended to be best-estimate. As most other reliability data in a PSA is best estimate, this approach can skew results and risk insights. Once the PSA model has been quantified the high-confidence software reliabilities will cause the associated systems and faults to have a greater risk significance than they would if best estimate data were used. This can cause the insights from the PSA to also be skewed towards highlighting these aspects while neglecting others which may in fact be more risk significant. For risk-insignificant systems a reliability value based on high-confidence reliability values may be appropriate, if this can be shown to not skew the PSA results or risk insights.
2. Software should be modelled differently to hardware in PSA. Unlike hardware, software does not wear out and random failures are not expected to dominate reliability, instead faults that can cause software to fail are likely to be inherent or designed into the system. The modelling of software in PSA can be compared with common cause failures or human reliability analysis. In all three of these areas there is typically insufficient data or operating experience to empirically derive a failure rate and so specific models or techniques are required to quantify reliability. These models often include consideration of external factors (for example, time pressure or supply chain diversity) that affect reliability but are difficult to quantify and therefore often rely on expert judgement. Due to the high uncertainty of these aspects of PSA modelling it is important that sensitivity studies are produced to understand their risk significance.
3. Once a detailed PSA model has been created with relevant failure modes included the PSA model can be used to establish which failure modes lead to risk significant consequences. A range of reliabilities can be used at this stage to test the sensitivity of the PSA model.
4. It is important to recognise that whilst PSA should strive to be best estimate, outputs from PSA may be used in establishing design rules or system requirements which should be set on a conservative basis. PSA models containing DCI should be set up in a way that allows both best estimate and conservative data to be used if PSA forms an input to a process where conservative data is required.
5. The inspector should consider asking for the following sensitivity studies:

* Software failures assigned best-estimate reliabilities – this should form the base-case and is likely to be of most interest to PSA inspectors. Best Estimate software reliability is particularly important where a PSA is being used as the basis for a risk monitor;
* Software failures assigned high confidence reliabilities – this can be useful for deriving reliability requirements and is likely to be of interest for C&I inspectors;
* Software failures switched off – this requires a PSA model with hardware and software failures modelled separately, this can allow other disciplines (for example, mechanical, electrical, C&I) to form a view on the hardware reliability of a system based on its architecture;
* Software assigned a range of other values to demonstrate the sensitivity of different aspects of the design to the software reliability.

1. Inspectors should keep in mind that software reliability is a complex topic, with no established methods to quantify purely best estimate reliabilities. Best estimate claims on software reliability are likely to be focused on applying other factors to amend high confidence reliabilities. However, research in this area is ongoing and methods may become available in the future which enable best-estimate reliabilities to be calculated. Inspectors should keep an open mind and discuss with C&I colleagues if new quantification approaches are submitted.
2. Pragmatism should be applied, and inspectors should focus on claims with the potential to significantly impact the risk insights from PSA or where numerical targets are challenged. Input from C&I specialists should be sought for complex claims or assessments.
3. It is likely that some elements of expert judgment will be required to assign reliability values to the various failure modes identified during the modelling of C&I systems. For risk-significant failures an expert panel may be required to ensure a complete understanding of the C&I systems and the consequences of their failures are understood. The process used to assign reliability values should be transparent and documented. Such processes may consider and combine a range of factors to establish an overall holistic reliability for a digital C&I system. During the process to consider relevant factors, due consideration must also be given to reduce risks ALARP (this is because combining a number of factors to establish a best-estimate reliability value could mask the importance of certain factors in the PSA results). Additionally, where such reliabilities are assigned to the PSA, suitable sensitivity studies should be conducted to establish the sensitivity of the assigned reliability.
4. There have been previous examples of dutyholders successfully making arguments that individual system reliabilities and CCF parameters are more reliable than the high-confidence values assigned from the SIL process. Typically these arguments have led to a single order of magnitude reduction in failure probability. Whilst this goes some way towards reducing potential conservatisms in software reliability, dutyholders should aim where possible to use fully best-estimate reliabilities for the PSA.
5. Successful arguments have often relied on operating experience gathered from the software in question operating at different facilities around the world. Although operating experience cannot rule out future software failures due to their systematic nature, for the purposes of PSA operating experience can help to support arguments that software reliability is higher than the high-confidence values based on design requirements.
6. To make best use of operating experience dutyholders should be encouraged to capture operating experience from their C&I systems and where failures are observed the root cause of these should be established.
7. Inspectors and dutyholders should be aware that, where a best-estimate claim on software reliability is being made on a C&I system, the level of evidence required to demonstrate it is lower than the equivalent submissions required to demonstrate a high-confidence claim. This is because a best-estimate claim is generally equivalent to a less reliable high-confidence claim. The important aspect from a PSA perspective is for software to be modelled in a way that captures the consequences of it failing, and with a reliability in line with operating experience of similar software in similar settings.
8. The computer-based safety systems TAG (TAG-46) [50] notes that high-confidence values can range from the order of 1E-01 to 1E-04 per demand or frequency of dangerous failure per year (ff). In the case of high-confidence values, 1E-04 is a limit on the maximum reliability that can be claimed on a computer-based system important to safety (CBSIS). TAG-46 also noted that it may be acceptable for duty-holders to claim a best estimate reliability of lower than 1E-04 for the purposes of a PSA. ONR’s inspectors should look at the adequacy of the duty-holder’s arguments and evidence to support this claim in the PSA model. Discussion with C&I inspectors is advised if reliability claims better than 1E-04 for risk significant systems are submitted in a PSA.

### Systematic Software Failures and CCFs

1. The nature of software-based systems means they are more vulnerable to systematic failure. A systematic software failure is a type of common cause failure where the conditions that cause software to fail are present in all iterations of the software or across the software platform. In comparison to hardware-based systems, increasing redundancy is unlikely to have a significant impact on the chance of CCF due to the expected dominance of systematic failures. For software-based systems, resilience to CCF is gained by increased diversity rather than redundancy.
2. Annex 2 of IAEA’s Safe Use of Smart Devices in Systems Important to Safety in NPPs [51] provides detailed discussion of common cause failure analysis for software based systems. It is expected that the deterministic analysis of C&I reliability and associated CCFs will consider the elements outlined in the guidance. When the relevant C&I systems are modelled in the PSA, information from the deterministic analysis can be used to inform the PSA.
3. CCF analysis should account for the consequences of a given CCF. For example, particular attention needs to be given to spurious actuation, where failure of a smart device model can both initiate an accident scenario and simultaneously defeat multiple defences. The likelihood of a CCF should also be considered. There is generally significant uncertainty on the estimation of the correlation factor among smart devices, as well as difficulty in estimating software reliability so assigning a likelihood value for a CCF is difficult but necessary to support PSA.
4. As discussed above, assigning reliability values to software failures in a single redundancy system is likely to rely on a combination of operating experience, review of the pedigree of the software and expert judgement. When there are multiple iterations of the same software or multiple software iterations running on the same platform, an additional CCF factor should be considered within the PSA representing the possibility of a common cause or platform failure.
5. The PSA should separately model the probability of each function being delivered where this is justified. CCF factors should be linked to the level of functional diversity within the architecture of systems. Inspectors should expect to see the use of CCF factors lower than one (i.e. less than complete dependence) in a PSA model where this can be justified based on the architecture and characteristics of the system. Guidance on software diversity for high reliability systems is provided in Appendix 5 of the computer-based safety systems TAG (TAG-46) [50].
6. Typically the most straightforward approach is to assume a CCF factor of one, meaning that all software failures are CCFs or platform failures. This may be acceptable for low-risk systems or where design details are not available, however it should be avoided within a best estimate PSA where justifiable. Conducting sensitivity studies using a range of values for different CCF factors is likely to reveal which CCFs are most risk significant. This information can be used to help target assessment. A sensitivity study with the CCF factor set to one is likely to be required by C&I inspectors to support high confidence deterministic analysis.
7. For hardware components of a DCI system the usual approaches for assigning CCF values can be used, for example the Alpha Factor method or Multiple Greek Letter method can be used based on failure data gathered from the wider population of equipment used worldwide.

### Use of Statistical Testing

1. As the computer-based safety systems TAG [50] notes:

“Where statistical testing is required as part of the equipment substantiation, this should be to a high statistical confidence level (for example, 99%). This requires, for example, of the order of 46,000 tests with no failure for a 1E-4 pfd. Where statistical testing is being used to determine a reliability estimate for modelling purposes (for example, PSA), best estimate confidence may be appropriate (for example, 50%). This requires, for example, of the order of 7,000 tests with no failure for the same pfd of 1E-4.

Where 95-99% confidence testing is used, the PSA can use a corresponding lower reliability figure when modelling the performance of CBSIS.”

1. Where significant numbers of tests have already been produced to support a deterministic case, these test results may be used to support a higher reliability claim in the PSA. However, it should be recognised that statistical testing is just one type of independent confidence building measure (ICBM) that can provide evidence on top of production excellence assessment to support a reliability claim and that statistical testing alone should not be used to support best estimate data. The use of such ICBMs to support PSA claims is discussed in the section below.

### ICBMs to support PSA

1. The ONR SAPs outline, under ESS. 27, the expectation of a two-legged approach to substantiate CBSIS, i.e. production excellence (PE) assessment supported by independent confidence building measures (ICBMs). The philosophy of this multi-legged approach is that substantiation of the system centres on both a demonstration of high-quality production and an independent searching examination of the system’s fitness for purpose that reveals no significant faults or errors that compromise the system’s required safety performance. A wide range of ICBM activity is often completed and recorded to complement the production excellence assessment and overall qualitative substantiation of CBSIS. These activities include but are not limited to:

* Device type tests
* Commissioning tests
* Examination, inspection, maintenance and testing (EIMT) records
* Data on prior use from reputable sources
* Evidence of manufacturer pedigree
* Device hardware failure modes and effects analysis
* Dynamic analysis of source code
* Static analysis of source code
* Independent desk top review of source code
* Statistical testing
* Certification by an independent body (supported by evidence)
* Independent Functional Safety Assessment (FSA)
* Independent tool review

1. ICBMs make an important contribution to providing evidence that a high-confidence reliability has been achieved. If a licensee makes additional arguments that a best-estimate reliability can be demonstrated based on production excellence or ICBMs this should be discussed with C&I assessors. It is not expected that additional PE/ICBM work would be carried out solely to support a best-estimate reliability claim.

### Treatment of software reliability in other industries

1. The ONR research project [46] to review the international state of the art in DCI modelling and quantification of software reliability in PSA. One of the goals of the research was to find out how other industries model software reliability, if software reliability was being analysed on a best estimate basis and what methods others were being used.
2. The research identified that software reliability in PSA is treated in different ways by different industries. Many industries use the Safety Integrity Level (SIL) process outlined in IEC61508, or industry specific versions of that standard.
3. Some parts of the aviation industry consider software reliability during system development, in order to specify that the software reliability should be commensurate with the hardware reliability. The system reliability including hardware and software systematic failures is assessed using Design Assurance Levels which is similar to a SIL based process. However, when final reliability values are produced for the platform the software failure contributions are switched off;
4. Other industries such as process, rail, automotive, oil and gas and defence were reviewed. These industries use approaches similar to the SIL based process in IEC61508 or similar derived standards. The research project did not find evidence of these industries attempting to produce best-estimate software reliability values;
5. NASA develop PSA models for their space vehicles and have developed dynamic fault tree methods to include software failures in these. These approaches are more best estimate than those used in other industries. Best-estimate reliability values are derived based on a Bayesian process combining previous OPEX for similar software combined with specific test data.
6. The conclusions of the research indicate that currently there are no established methods for quantifying the reliability of software in a best-estimate way that could be considered relevant good practice.
7. However, in line with the expectations of SAP FA.13, within PSAs conducted for UK nuclear facilities software failures should not be ignored and should be quantified according to the requirements of the PSA model. Dutyholders are expected to use their PSA models to understand their vulnerability to software failures and model this appropriately.

## Human Reliability Analysis

1. The safety of nuclear installations often requires claims on human action. Where safety important human actions and administrative controls are required and their need is justified, the feasibility and reliability of the actions should be demonstrated qualitatively using task analysis. This qualitative modelling should be used to substantiate any human-based safety claims and the quantitative modelling of the probability of the associated human errors.
2. The general expectations on human reliability analysis are targeted towards assessing the demonstration through the PSA modelling of operator errors showing adequate consideration of:

* The plant context as it is in reality;
* The process of task analysis underlying the human error quantification.

1. Human performance can make a significant contribution towards overall plant risk, hence it must be assessed within the safety case as accurately and effectively as possible.
2. Human error probability (HEP) should take account of the specific task demands, psychological influences (for example, stress), degree of supervision, level of training, working practices, time available, physical environment, etc, and the potential dependencies between separate activities (either by the same or by different operators). Any equipment or procedural requirements to promote reliable human performance should be identified. The best estimate approach to risk analysis requires that the beneficial and potentially detrimental performance of personnel be represented within the PSA. The factors that can influence the ability of personnel to carry out activities need to be carefully considered before any quantification can take place.
3. The topic of human error quantification is discussed in the TAG for human reliability analysis [52] where guidance on the regulatory expectations on the PSA modelling considerations cover the following:

* Identifying and modelling human tasks and errors
* Identifying and modelling performance influencing factors
* Identifying and modelling dependence amongst human actions
* Quantification and analysis
* Sensitivity and importance analysis
* Relevant human actions are risk ALARP

1. Specific assessment expectations for review of the HRA in PSAs for NPPs can be found in Table A1-2.5 (Human Reliability Analysis) of Appendix 1.

## Analysis of internal and external hazards

1. Development of internal and external hazard PSA generally follows a similar method to the Level 1 internal events PSA method, i.e.: selection of IE (in this case a particular internal or external hazard); screening and bounding of the IE; accident sequence analysis and systems analysis. As such, the recommendations listed above are generally applicable for both hazards PSA and internal-events PSA.
2. The task of hazard identification should aim to generate a comprehensive list of potential internal and external hazards. The external hazard identification would be site specific, while internal hazards are often design and site specific. The comprehensive list of internal and external hazards is expected to be assessed through a systematic screening process which is well defined in international guidelines such as EPRI [53] and IAEA [13] and [54].
3. Adequate consideration is expected for a risk based graded approach for the analysis of hazard initiator PSA studies. Proportionate and appropriate probabilistic treatment of multiple hazard combinations such as correlated hazards (for example, highest wind speed and highest surge height), consequential hazards (for example, seismic with fires) and coincidental hazards (for example, flood levels greater than a certain height for multiple days, extended periods of extreme heat or cold) is expected. It is expected that this topic would require collaborative working with the internal and external hazards specialist inspectors. ONR guidance on deterministic safety expectation on this topic is available through TAG-13 [55] for external hazards and TAG-14 [56] for internal hazards.
4. Specific assessment expectations for review of the Analysis of Internal and External Hazards in PSAs for NPPs can be found in Table A1-2.7 of Appendix 1.

## Non-reactor PSA (such as Fuel Route)

1. It is generally noted that the highest radiological risk arises from the reactor core. However the risk form other plant areas where radioactive material is either stored of handled may not be non-negligible. These are areas such as the Fuel route, Radiological waste storage and processing, spent fuel ponds, and new fuel stores etc.
2. Most PSAs for complex facilities would often include a proportionate approach to modelling of these facilities. The assessment of these PSAs would also require the consideration of the all the aspects discussed in the sections above in a proportionate manner.

## Analysis of other Plant Operational States

1. As stated above, the scope of a PSA is expected to address all plant operational states (POS) wherein the nuclear facility is expected to operate. PSAs are typically developed for ‘at-power’ operational state initially, then further develop to model other POS. The recommendations listed above are applicable for PSA models of all POS.
2. When assessing PSAs for POS other than ‘at power’ or for facilities where it is not ‘at power’ equivalent (for example, a fuel cycle or fuel route facility) inspectors should consider other POS such as:

* Reduced or Low power or partial POS
* Shutdown POS (Annual outage POS)
* Refuelling POS
* Startup or restart POS

1. Specific assessment expectations for review of the Analysis of Low Power and Shutdown Modes in PSAs for NPPs can be found in Table A1-2.8 of [Appendix 1](#_Appendix_1_-).

## Quantification of the Analysis

1. The PSA should determine the combinations of basic events such as component failure, CCF, operator error and plant unavailability which lead to the undesirable event (or initiating event) and determine its frequency of occurrence. The methods used to do this should be identified and shown to be adequate. Due to the complexity of the analysis, the quantification of the PSA normally requires a computer program. This code should be quality assured (see AV.4) and the evidence of this should be provided by the dutyholder (AV.5).
2. The inspector may consider whether:

* where computer programs are used, they and their results are verified, manual calculations should have been independently checked by the dutyholder;
* the combinations of basic events (minimal cutsets) which lead to failure of the protection or support systems are identified and listed for each of the IEs analysed;
* that single order minimal cutsets are identified and brought to the attention of the assessors dealing with compliance with the single failure criteria;
* the combinations of basic events which lead to the protection system failure (for this, inspectors should review a sample of the cutsets including those which make the highest contributions to the frequency/probability calculated);
* if the quantification of the analysis has required a restriction to be applied on the probability of the combinations of basic events included, this has not affected the accuracy of the analysis significantly;
* in the calculation, all dependencies are taken into account. This includes the dependency between redundant components, between nominally diverse systems and between individual operator errors. Dependencies due to common support systems should be modelled explicitly in the analysis;
* the importance of IEs, components, systems, operator errors and dependencies in the calculation of the risk have been identified.

## 

## Level 2 PSA

1. For NPPs Level 1 PSA is the part of the overall PSA that deals with the frequency of core damage and characterises the state of the core into plant damage states. Level 2 PSA starts with plant damage states and models the containment and the phenomena that occur following fuel damage. Level 2 PSA ends with a set of release categories/source terms. Effectively, Level 2 PSA widens the Level 1 PSA to consider the containment systems which are designed to act as barriers to release outside the containment. Hence the level 2 PSA is often used to compute the large early release frequency (LERF) and the large release frequency (LRF) metrics considered for many light water reactors.
2. All the aspects of Level 1 PSA in terms of modelling and data would also apply to Level 2 PSA. In addition the underpinning analysis for Level 2 PSA is part of the severe accident analysis. It is expected that the PSA inspector works collaboratively with the SAA inspector to assess the supporting calculations for the Level 2 PSA. ONR TAG-7 [40] provides the guidance for assessment of severe accident analysis. Similarly the topic of containment fragility and source terms need to be collaboratively assessed with specialist inspectors of Civil engineering and Chemistry respectively.
3. Specific assessment expectations for review of the Level 2 PSA for NPPs can be found in Table A1-3 of Appendix 1.

## Level 3 PSA

1. The output of level 2 PSA is the estimation of magnitude and frequency of releases to the environment, often grouped into groups of release categories. The Level 3 PSA then uses these release categories as input to dispersion analysis codes (for example, PACE or PC-COSYMA) to calculate the impact to the public.
2. The Level 3 PSA often provides the basis for the off-site risks assessed through Targets 7, 8 and 9. This area of assessment may need collaborative effort with specialist inspector from Radiological Consequences. TAG 45 [6] provides information on assessment of radiological consequences that may support assessment of the Level 3 PSA. The TAG notes that there are large sources of uncertainty related to the calculation of radiological releases. Where the calculation is being used to support PSA the assumptions made should be best-estimate rather than conservative. Another source of guidance on Level 3 PSA is the ASME standard on Level 3 PSA [28], issued for trial use and pilot application.
3. Specific assessment expectations for review of the Level 3 PSA for NPPs can be found in Table A1-4 of Appendix 1 and the Radiological consequences TAG [6]

## Sensitivity and Uncertainty Studies

1. The results of the probabilistic analysis may be sensitive to the assumptions made and the data used. Since these contain some uncertainty, studies should be conducted to determine the degree of sensitivity to ensure that the conclusions drawn from the analysis are still valid in the light of these uncertainties (AV.6). These sensitivity studies should cover a sufficiently wide range of conditions to give confidence in the accuracy of the results of the analysis and the conclusions drawn from it. Importance measures such as Fussell-Vesely importance, risk increase factor, risk decrease factor, Birnbaum importance etc. may be used to identify the critical basic events to be covered by the sensitivity studies, as well as providing how the impact to the risk can be interpreted.
2. The inspector may check that:

* appropriate studies have been carried out to determine the sensitivity of the results of the PSA to any significant uncertainties in the models, assumptions and data;
* the error factors in the basic event data parameters are justified, systematically assigned and are a reasonable representation of the uncertainty.

1. The topic of sensitivity studies is good example of applications of PSA. This is also discussed with appropriate examples in the TAG on 'Use of PSA and Probabilistic Insights' [2] and as it relates to C&I modelling in sections ‎5.9.4, ‎5.9.5, and ‎5.9.6 of this TAG
2. Specific assessment expectations for review of the Sensitivity and Uncertainty Analyses in PSAs for NPPs can be found in Table A1-2.9.1 of Appendix 1.

## Presentation of the Results of the PSA

1. The results of the PSA should be presented in a form which allows comparison with the numerical targets of the SAPs and the dutyholder's own criteria. The use of the PSA results would also be the expectation in the presentation of results. Inspectors are advised to refer the TAG on 'Use of PSA and Probabilistic Insights' which has discussed several aspects on use of best estimate calculations [2].
2. The inspector may consider:

* whether sufficient information is provided to allow ONR to make a comparison with the SAPs;
* whether suitable judgements have been made, where possible, of the magnitude of ‘excluded’ contributions to the risk in relation to those calculated in the PSA;
* whether the results of the PSA have been reviewed systematically to determine if changes could be made to the design or operation of the facility to make the risks as low as reasonably practicable – see ONR’s ALARP guidance, NS-TAST-GD-005 [5].
* whether, in cases where changes to the design or operation of the facility are proposed, the corresponding reduction in the risk has been calculated.
* the extent to which the results of the PSA meet the numerical target in the SAPs;

1. Specific assessment expectations for review of the Results of the PSAs for NPPs can be found in Tables A1-2.9 (Level 1 PSA), A1-3.6 (Level 2 PSA), A1-4.2 (Level 3 PSA) and A1-5 (Overall conclusions from the PSA) of Appendix 1.

## Multi-unit and site-level considerations

### Expectations from SAPs

1. SAP FA. 11 sets out the expectation that the PSA should cover all significant sources of radioactivity. The supporting text to FA. 11 also specifically identifies that at multi-facility sites, the analysis should also consider the potential for specific initiating faults giving rise to simultaneous impacts on several facilities or for faults in one facility to impact another facility.
2. Numerical Targets 7 and 9 consider ‘accidents at the site’, often requiring some form of aggregation of the risk from multiple facilities.

### Background

1. PSAs have traditionally been developed on a single-unit basis. However, most nuclear sites, in the UK and internationally, contain multiple facilities. This fact brings about the need to consider the following aspects when assessing the adequacy of the PSA:

* How faults or initiating events which affect multiple facilities or cascade from one facility to another are considered within the PSA.
* How PSA results across various facilities, hazards and operational states aggregated to consider site-level risk.

1. This section of the TAG aims to provide inspectors with a high-level background on both topics along with some guidance on the technical areas most likely to be relevant when assessing the adequacy of a PSA from a site-level or multi-unit perspective.
2. As the existing and proposed nuclear sites in the UK often contain multiple reactor units or other facilities, dutyholders are expected to consider the impact of multiple reactor units and other facilities within the PSA. However, the extent, depth and detail of the analysis is likely to vary.
3. For existing sites with limited dependencies between individual facilities this may be limited to a single unit PSA for a representative reactor unit or facility. For a new build site, or a site with significant or complex interactions between facilities, more detailed analysis or a specific multi-unit PSA models may be required.
4. Development of multi-unit PSA models is a difficult area of analysis and has been a focus of research by the international PSA community for several years.

### Sources of guidance and relevant good practice for site-level PSA

1. The Working Group on Risk Assessment (WGRISK) of the OECD/NEA have recently published a report on the Status of Site-Level (Including Multi-Unit) PSA Developments that collects information on how member countries are addressing challenges and developments of site-level PSA and actual or intended uses and applications of site-level PSA [36]. Inspectors may find the content of the report useful to understand international RGP and how the various technical challenges are being considered around the world.
2. IAEA safety guides for Level 2 PSA [14] and ASME procedure guide for Level 3 PSA [28] include consideration of coincidental and consequential multi-unit faults into single unit PSA models. For risk aggregation guidance the IAEA Tecdoc 1983 [23] is a good resource which contains discussion on approach taken by various member states to aggregation of risk across various facilities, hazards and operational states.
3. Development of Multi-Unit PSAs to consider multiple units within the same integrated PSA model has been a focus of IAEA since Fukushima with several reports published or due to published:

* IAEA Safety Report 96 - Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Units [57] provides a roadmap and methodology for performing a multi-unit PSA, proposes a set of site level risk metrics, and presents examples of approaches to resolve specific issues
* IAEA Safety Report 110 – Multi-Unit Probabilistic Safety Assessment [58] provides a methodology for conducting a multi-unit PSA, tested by a case study and supported by annexes of experiences in member states.
* IAEA is currently revising and SSG-4. SSG-3 Rev 1 includes a section on development of Level 1 multi-unit PSA [59]. The revised version of SSG-4 is not currently publicly available, however ONR has been involved in the review process for SSG-4 and it is expected to have similar content on multi-unit PSA.

1. In 2018 EDF NGL commissioned research on Multi-Unit PSA which identifies the main technical issues of developing a multi-unit PSA, focusing on application to the EDF NGL fleet of reactors.
2. ONR has conducted research on “Consequence Assessment for Multi-Unit PSA” (see further information below) which included a summary of current practice and ongoing research [60].

### Guidance on PSA elements for site-level PSA

1. The following provides some general advice to inspectors on the different technical aspects of PSA relevant to multi-unit considerations.

#### PSA Scope for site-level /multi-unit PSA

1. The scope of the PSA is expected to cover all significant sources of radioactivity on site. The presence of multiple reactor units and other facilities on a site should be considered when developing and justifying the scope of the PSA.
2. Whilst inspectors should usually start with the expectation for the PSA to be full scope (including multi-unit and site-level considerations), there should be a high level of pragmatism when considering the need to develop a detailed multi-unit PSA model. In particular:

* There is likely to be limited value in a site with limited operating life remaining expending significant resources to develop a detailed multi-unit PSA.
* Technical challenges and uncertainties in single unit PSA (for example, quantification of CCFs, seismic fragilities, long timescale SSC reliability and success criteria etc.) are likely to be increased in multi-unit PSAs, therefore inspectors should also consider the benefit of conducting a PSA when uncertainties and assumptions would dominate the insights and negate the benefits of developing the PSA.

1. To date in the UK, all multi-unit sites have focused on producing PSAs for representative single units, for example:

* PSAs for the AGRs are all for single representative units. However faults affecting multiple units (for example, loss of grid) are identified and support systems are modelled accordingly (for example, feed water supplies, ability to cross connect shared trains).
* The PSA for HPC is for a single unit. Additional scoping analysis is conducted to analyse and report the site level risk [61].

#### PSA Methodologies for site-level/multi-unit PSA

1. There are several options available to dutyholders when considering multiple reactor units or facilities within the PSA. This may extend from justification that a single unit model adequately represents the site, all the way to a fully integrated multi-unit PSA covering all sources of radioactivity on site, and various steps in-between. There are advantages and disadvantages to the different approaches, depending upon the complexity of the site, the dependencies between the facilities, and the level of risk for the site. The approach taken should be suitable to understand the risk and develop a suitable and sufficient PSA to support the expected PSA applications.

#### Initiating events for site-level/multi-unit PSA

1. Initiating events which affect multiple units or facilities should be considered and analysed. Initiating events which propagate between units or facilities should also be considered and analysed, for example, external hazards like coastal floods, seismic, and extreme weather.

#### Accident sequence analysis for site-level/multi-unit PSA

1. Dependencies and the potential for propagation between units and facilities should be identified and suitably considered in the PSA. This may include safety systems, support systems, control systems, operator actions, CCFs, phenomenology, and radiological consequences. The potential for a radiological release at one facility to impact the operator response on an adjacent facility should be considered

#### Input data for site-level/multi-unit PSA

1. Data used in the PSA model, or any multi-unit sensitivity studies may be impacted by the scope of the PSA, including CCFs, operator actions and initiating event frequencies. Therefore, data used in any multi-unit PSA models or studies should be documented and justified.

#### Internal and external hazards for site-level/multi-unit PSA

1. The potential for propagation of internal hazards between units and facilities should be considered. This may include tasks such as extending the fire PSA multi-compartment analysis to consider adjacent facilities.
2. Many external hazards have the potential to impact multiple facilities on the same site. External hazard prioritisation and external hazards PSA models or sensitivity analysis should include consideration of all facilities which may be affected by the external hazard. Additional analysis for seismic PSA may be required to consider the potential for correlation between SSCs in different facilities.

#### Evaluation of off-site consequences for site-level/multi-unit PSA

1. Additional consequence analysis may be required to evaluate the consequences of a multi-unit accident. For example, a seismic event may be considered to lead to a release on multiple similar facilities, with a similar or higher frequency than a single unit release, and therefore additional consequence analysis should be performed.
2. ONR has conducted research on the impact on off-site consequences due to releases from multiple facilities in the same location [60]. The research identified sources of international experience and conducted additional analysis using the PACE dispersion modelling code. The research concluded that an additive combination (for individual risk) or linear combination (for societal risk) of single unit results provided a good approximation for simultaneous multi-unit releases. However, there were more complex effects seen for time off-set releases and some areas of potential non-conservatism for deterministic consequences. Inspectors assessing PSAs or other analysis including multi-unit releases should review the report recommendations for any relevant to the specific assessment.

#### Quantification and presentation of results for site-level/multi-unit PSA

1. PSA results should be quantified, aggregated, and presented in a suitable way to allow for comparison against SAPs numerical targets, understanding of sensitivity and uncertainty, demonstration of risks being reduced to ALARP and use of PSA results to support the PSA applications. Consideration of site-level or multi-unit risk may require different risk metrics to those used within single unit PSAs. Level 3 PSA may be required to aggregate risks from different sources.
2. Care should be taken to ensure that dutyholders are not splitting a site into many smaller facilities to achieve a favourable comparison against Numerical Target.8, however inspectors should also avoid detailed assessment if a different approach would not impact comparison against the numerical targets or the risk insights gained.
3. Inspectors should reassure themselves that the risk aggregation is conducted in a suitable way to meet the overall intent of the numerical targets to understand risks and to allow for meaningful risk insights. For example, if a specific aspect of the PSA has a significantly higher uncertainty than the other aspects, this high level of uncertainty should be considered in the risk aggregation.

## 

## PSA for Novel Designs of Nuclear Power Plants

1. Over the last couple of decades there has been a lot of interest in small modular designs for water cooled reactors and also for other novel and evolutionary designs which are liquid metal or high temperature gas cooled reactors. Commensurate to the interest, research, and development work carried out in these designs, IAEA, USNRC and NEA have published review of guidance (regulatory and also performance) on the topic of safety analysis supporting these novel designs. The following references reflect this effort:

* IAEA safety series report on the assessment of the applicability of the current safety standards to new and novel reactor designs is captured in [24],
* USNRC has published a Non-Light Water Review Strategy white paper [62], and
* NEA has published guidance on PSA for new and advanced reactors [37].

1. ONR had hosted an International symposium on PSA for Reactors of Singular Designs as part of WGRisk of NEA and supported by IAEA in 2022. Forty three experts from across the world participated and shared their experience through technical papers and discussion forums. Several topics were identified as areas which may pose technical challenges and need consideration in developing the PSA Strategy such as:

* Risk metric definitions may be more complex and may require Level 3 PSA.
* Initiating event identification and quantification is likely to be more resource intensive.
* Passive system reliability, including identification and evaluation of failure modes, is an ongoing area of research that may impact reactors which have a reliance on passive safety features.
* Code qualification and validation (for example, thermal hydraulics or severe accident codes), especially for novel or innovative designs, may be limited. This will likely be challenging to the design process as well as the development of the PSA and require substantial effort to address.
* Human Reliability Analysis based upon existing methodologies may not be completely applicable to reactors with singular designs, especially where digital or remote control rooms are used or when long time windows are claimed.

1. Based on the above, it could be concluded that while most of the regulatory expectations and standards for PSA as applied to the water cooled reactors would apply to the non-water cooled reactors with some exceptions. The dutyholder, or requesting party in case of GDA, would need to, in all cases, identify the exceptions and provide justification. The justification would need to be assessed by the inspector in the light of overarching guidance in the UK context of reducing risk ALARP.
2. Other than PSA it is acknowledged that novel and evolutionary reactor designs have some features not covered by the safety standards including the use of alternative operating models, such as factory commissioning of nuclear steam supply assemblies prior to transport to the operating site, autonomous operation, refuelling (possibly at the factory), remote monitoring, remote intervention, also providing heat/steam/electricity to industrial processes and the hazards posed by these facilities. The guidance in these areas is still under development internationally.

# References

|  |  |
| --- | --- |
| [1] | ONR, “Safety Assessment Principles (SAPs) for Nuclear Facilities - 2014 Edition (Revision 1),” 2020. |
| [2] | ONR, “NS-TAST-GD-116 - Use of PSA and Probabilistic Insights”. |
| [3] | WENRA, “Explanatory Note on PSA,” March 2007. [Online]. Available: https://www.wenra.eu/sites/default/files/ publications/rhwg\_psa\_explanatory\_note\_march07.pdf. |
| [4] | ONR, “NS-TAST-GD-051 - The purpose, scope and content of safety cases”. |
| [5] | ONR, “NS-TAST-GD-005 - Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)”. |
| [6] | ONR, “NS-TAST-GD-045 - Radiological Analysis for Fault Conditions”. |
| [7] | ONR, “NS-TAST-GD-042 - Validation of computer codes and calculation methods”. |
| [8] | ONR, “NS-TAST-GD-050 - Periodic Safety Reviews (PSRs)”. |
| [9] | WENRA, “WENRA Safety Reference Levels for Existing Reactors Revision 2020,” February 2021. [Online]. Available: https://www.wenra.eu/sites/default/files/publications/wenra\_safety\_reference\_level\_for\_existing\_reactors\_2020.pdf. |
| [10] | IAEA, “Fundamental Safety Principles, SF-1,” 2006. |
| [11] | IAEA, “Safety of Nuclear Power Plants: Design, SSR-2/1 (Rev1),” 2016. |
| [12] | IAEA, “Safety Assessment and Verification, NS-G-1.2,” 2001. |
| [13] | IAEA, “Development and application of Level 1 PSA for Nuclear Power Plants, SSG-3 Rev-1,” 2024. |
| [14] | IAEA, “Development of Level 2 PSA, SSG-4,” 2010. |
| [15] | IAEA, “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, IAEA Safety Series 50-P-12,” 1996. |
| [16] | IAEA, “Procedure for conducting Level 1 PSA, 50-P-4,” 1992. |
| [17] | IAEA, “Procedure for conducting Level 2 PSA, 50-P-8,” 1995. |
| [18] | IAEA, “Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice, 50-P-7,” 1995. |
| [19] | IAEA, “Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, TECDOC-1804,” 2016. |
| [20] | IAEA, “Regulatory Review of Probabilistic Safety Assessment (PSA) – Level 1, TECDOC-1135,” 2000. |
| [21] | IAEA, “Regulatory Review of Probabilistic Safety Assessment (PSA) Level 2 – IAEA – TECDOC - 1229,” 2001. |
| [22] | IAEA, “Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Units, Safety Report Series No 96,” 2019. |
| [23] | IAEA, “Risk Aggregation for Nuclear Installations, Tecdoc-1983,” 2021. |
| [24] | IAEA, “Safety Report on Applicability of Safety Standards on Non Water Cooled Reactors and Small Modular Reactors. https://preprint.iaea.org/search.aspx?orig\_q=reportnumber:IAEA-PC--8839,” 2022. |
| [25] | IAEA, “Case Study on Aasessment of Radiological Environment Impact from Potential Exposure,” 2020. |
| [26] | ASME, “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-S-1.1-2022,” 2022. |
| [27] | ASME, “Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), ASME RA-S-1-2,” 2014. |
| [28] | ASME, “Standard for Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to support Nuclear Installation Applications, ASME RA-S-1-3,” 2017. |
| [29] | USNRC, “Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, NUREG/CR-6268 Rev 1,” 2007. |
| [30] | USNRC, “Industry-average performance for components and initiating events at U.S. commercial nuclear power plants, NUREG/CR-6928,” 2007. |
| [31] | USNRC, “EPRI/NRC-RES, Fire PRA Methodology for Nuclear Power Facilities, NUREG/CR-6850,” 2005. |
| [32] | IEC, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety related systems - Part 3 Software Requirement, IEC 61508-3,” 2010. |
| [33] | EPRI, “Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment, TR-1019194,” 2009. |
| [34] | EPRI, “Seismic Probabilistic Risk Assessment Implementation Guide, EPRI Report 3002000709,” 2013. |
| [35] | EPRI, “Screening, Prioritization and Implementation Details (SPID) -Seismic, Report 1025287,” 2012. |
| [36] | OECD/NEA, “https://www.oecd-nea.org/jcms/pl\_58495/status-of-site-level-including-multi-unit-probabilistic-safety-assessment-developments,” [Online]. |
| [37] | NEA/CSNI, “A Joint Report on PSA for New and Advanced Reactors, NEA/CSNI/R(2012)/17,” 2012. |
| [38] | USNRC, “Handbook of Parameter Estimation for Probabilistic Risk Assessment, NUREG/CR-6823,” 2003. |
| [39] | ONR, “NS-TAST-GD-016 - Integrity of Metal Components and Structures,” 2022. |
| [40] | ONR, “NS-TAST-GD-007, Severe Accident Analysis,” 2022. |
| [41] | ONR, “NS-TAST-GC-089, Chemistry Assessment,” 2022. |
| [42] | USNRC, “Common-Cause Failure Parameter Estimations, NUREG/CR-5497,” 1998. |
| [43] | IAEA, “Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants, TECDOC-1624,” 2009. |
| [44] | IAEA, “Progress in Methodologies for the Assessment of Passive Safety System Reliabilty in Advanced Reactors, TECDOC - 1752,” 2014. |
| [45] | EPRI, Program on Technology Innovation: Comprehensive Risk Assessment Requirements for Passive Safety Systems, Report No 1016747, 2008. |
| [46] | ONR, “ONR-RRR-112 PSA Best estimate C&I software modelling and realiabilty, https://www.onr.org.uk/documents/2023/onr-rrr-112.pdf,” 2023. |
| [47] | IAEA, “IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants,” 2016. |
| [48] | “https://www.nrc.gov/about-nrc/regulatory/research/digital.html#2,” [Online]. |
| [49] | EPRI, “Estimating Failure Rates in Highly Reliable, Electric Power Research Unit, 1021077,” 2010. [Online]. |
| [50] | ONR, “Computer Based Safety Systems Technical Assessment Guide, NS-TAST-GD-046 Revision 6.,” April 2019. |
| [51] | IAEA, “IAEA, Safe Use of Smart Devices in Systems Important to Safety in NPPs, Safety Reports Series No.111,” Jan 2023. |
| [52] | ONR, “Technical Assessment Guide, Human Reliability Analysis, NS-TAST-GD-063,” 2022. |
| [53] | EPRI, “Identification of External Hazards for Analysis in PRA, Report no. 3002005287,” 2015. |
| [54] | IAEA, “IAEA 50-P-7: Treatment of External Hazards in Probabilistic Safety Assessment,” 1995. |
| [55] | ONR, “NS-TAST-GD-013 Revision 8 External Hazards,” 2022. |
| [56] | ONR, “NS-TAST-GD-014 Revision 7.1 Internal Hazards,” 2022. |
| [57] | IAEA, “https://www.iaea.org/publications/12228/technical-approach-to-probabilistic-safety-assessment-for-multiple-reactor-units,” [Online]. |
| [58] | IAEA, “https://inis.iaea.org/collection/NCLCollectionStore/\_Public/52/073/52073213.pdf,” [Online]. |
| [59] | IAEA, “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3 (Rev. 1),” 2024. |
| [60] | ONR, “Multi-unit Level 3 PSA Research (ONR-RRR-084) ONR-1901\_Report\_final, CM9 2019/284669,” 2019. |
| [61] | NNB GenCo (HPC) Ltd, “UK PROTECT - 100774721 001 HPC NIC-PSA Main Report, CM9 2023/22810,” 2018. |
| [62] | USNRC, “Non-Light Water Review Strategy, Staff White Paper. https://www.nrc.gov/docs/ML1927/ML19275F299.pdf,” 2019. |
| [63] | ONR, “NS-TAST-GD-017 - Civil Engineering,” 2022. |

# 

# Glossary and abbreviations

|  |  |
| --- | --- |
| ABWR | Advanced Boiling Water Reactor |
| AGR | Advanced Gas Cooled Reactor |
| ALARP | As Low As Reasonably Practicable |
| ANS | American Nuclear Society |
| APET | Accident Progression Event Tree |
| ASME | American Society for Mechanical Engineers |
| AV | Assurance of Validity |
| BSL | Basic Safety Level |
| BSL (LL) | Basic Safety Level (Legal Limit) |
| BSO | Basic Safety Objective |
| CAFTA | Software for Fault Tree Analysis |
| CBSIS | Computer Based System Important to Safety |
| CCF | Common Cause Failure |
| CCR | Common Control Room |
| CDF | Core Damage Frequency |
| COSYMA | Probabilistic Accident Consequence Assessment (ACA) System |
| CSNI | Committee on the Safety of Nuclear Installations |
| DBA | Design Basis Analysis |
| DCI | Digital Control Instrumentation |
| EDF | Electricite De France |
| EIMT | Examination Inspection Maintenance and Testing |
| EPR | European Pressurised Reactor |
| EPRI | Electric Power Research Institute |
| ESS | Engineered Safety Systems |
| FA | Fault Analysis |
| FMEA | Failure Modes and Effects Analysis |
| FSA | Functional Sequence Analysis |
| GDA | Generic Design Assessment |
| GSR | General Safety Requirements |
| HAZOP | Hazards and Operability Analysis |
| HEP | Human Error Probability |
| HFE | Human Failure Event |
| HHSI | High Head Safety Injection |
| HPC | Hinkley Point C |
| HRA | Human Reliability Analysis |
| HVAC | Heating Ventilation and Air Conditioning |
| IAEA | International Atomic Energy Agency |
| ICBM | Independent Confidence Building Measures |
| ICDE | International Common cause failure Data Exchange |
| IE | Initiating Event |
| IEC | International Electrotechnical Commission |
| LC | Licence Condition |
| LERF | Large Early Release Frequency |
| LOCA | Loss of Coolant Accident |
| LRF | Large Release Frequency |
| NAME | Numerical Atmospheric-dispersion Modelling Environment |
| NASA | National Aeronautics and Space Administration |
| NEA | Nuclear Energy Agency |
| NF | Nuclear Facilities |
| NGL | Nuclear Generation Limited |
| NIC | Nuclear Island Concrete |
| NNB | Nuclear New Build |
| NPP | Nuclear Power Plant |
| NRC | Nuclear Regulatory Commission |
| NS | Nuclear Safety |
| NT | Numerical Target |
| NUREG | Nuclear Regulatory Guide |
| OECD | Organisation for Economic Cooperation and Development |
| ONR | Office for Nuclear Regulation |
| OPEX | Operating Experience |
| PACE | Probabilistic Accident Consequence Evaluation |
| PDS | Plant Damage State |
| PE | Production Excellence |
| POS | Plant Operational State |
| PRA | Probabilistic Risk Analysis |
| PSA | Probabilistic Safety Analysis |
| QA | Quality Assurance |
| RA | Risk Analysis |
| RC | Release Category |
| RGP | Relevant Good Practice |
| RHWG | Reactor Harmonization Working Group |
| RRR | Regulatory Research Register |
| SAA | Severe Accident Analysis |
| SAP | Safety Assessment Principle |
| SAR | Safety Analysis Report |
| SF | Safety Fundamentals |
| SG | Safety Guide |
| SIL | Safety Integrity Level |
| SPID | Screening Prioritization Implementation Details |
| SR | Safety Report |
| SSC | System Structures and Components |
| SSG | Specific Safety Guide |
| SSR | Specific Safety Requirements |
| SZB | Sizewell B |
| TAG | Technical Assessment Guide |
| TECDOC | Technical Document |
| TR | Technical Report |
| UK | United Kingdom |
| USNRC | United States Nuclear Regulatory Commission |
| WENRA | Western European Nuclear Regulators Association |
| WGRISK | Working Group RISK |
| ZEDB | German Risk Database |

# Appendix 1 - Assessment expectations for review of PSAs for NPPs

## Introductory note

1. This Appendix provides detailed guidance on the assessment of PSA specific for Nuclear Power Plants (NPPs). Inspectors may apply the guidance in this Table of Assessment Expectations in a risk proportionate way to the significance to relevant stages in the lifecycle of a nuclear power plant, i.e. PSAs submitted for generic design assessment (GDA), site licensing, reactor commissioning and to support NPP operation. Inspectors should bear in mind that much of the guidance in this appendix can also be applied to other types of installations.
2. There is an expectation that dutyholders will present the PSA analysis within a framework compatible with good industry practices. For NPPs this suggests a Level 1, 2, 3 PSA framework as presented in IAEA Specific Safety Guides [13] [14]. Many extant facilities had used the IAEA procedures for Level 1, 2, 3 PSA [16] [17] [15] for the performance of the studies. Inspectors will gain confidence in the acceptability of risk from the facility and ALARP compliance by reviewing the facility risk level against the numerical targets of the SAPs and the probabilistic criteria proposed by IAEA guidance [13] [14], which implies a need to calculate the appropriate risk figures of merit including core damage frequency and large release frequency.
3. However, to address the relevant numerical targets of the SAPs, dutyholders will also need to identify and study those sequences that have a higher frequency but lower radiological consequence. As an example, in PWRs, Steam Generator Tube Rupture sequences without core damage could lead to releases in the lower dose bands of Numerical Target 8 of the SAPs.   
   The guidance in this Appendix does not specifically cover assessment expectations for PSA studies addressing release categories for non-core damage sequences. ONR prefers that dutyholders present the PSAs for NPPs in the traditional Level 1, 2, 3 PSA framework as discussed above, addressing release categories for non-core damage sequences separately.
4. Other aspects not specifically covered by the guidance in this Appendix include worker risk and risk from facilities at the NPP other than the nuclear reactor. Nevertheless, these risks need to be evaluated by the dutyholders in order to address the relevant numerical targets of the SAPs.

## Use of this appendix

1. The Tables in this Appendix present check lists of items that inspectors should generally expect to see when assessing the different areas of the PSAs for nuclear reactors. The aim is to address all key aspects of modern PSA for nuclear reactors to help inspectors to assess, raise comments, questions and issues in a focused and systematic fashion, and, finally, judge the adequacy of each feature of the PSAs submitted by the dutyholders.
2. Although an attempt has been made to make this appendix comprehensive, it is meant for guidance only. It does not imply that inspectors have no discretion when choosing the scope and depth of the assessment to be undertaken.
3. In addition, it should be stressed that is not the intention of this appendix to prescribe specific methods and approaches for conducting PSA for NPPs. Dutyholders may choose to use alternative methods to those covered in this appendix as long as they are shown to lead to equally valid outcomes. In cases where the PSA or specific areas of it have been undertaken using alternative approaches, inspectors should review on a case-by-case basis and judge each on its own merits.
4. This appendix can be used in a more prescriptive manner when commissioning PSA assessment work (to be done on behalf of ONR) from external contractors. In such cases, inspectors may wish to restrict the use of discretion by the contractor and/or specify the scope and depth of assessment.

Table A1 - Table of Assessment Expectations

|  | **Assessment expectation** | **Met?** |
| --- | --- | --- |
| **Table A1-1. General Expectations** | | |
| **Table A1-1.1 Approaches and methodologies** | | |
|  | Task procedures have been developed for the individual PSA tasks and these have been provided by the dutyholder.  ONR inspectors may wish to assess or audit the PSA task procedures to gain confidence on the general adequacy of the methods and approaches and their implementation, before specific detailed assessments are undertaken of the various aspects of the PSA models and data. |  |
|  | Inspectors may wish to request information on any independent or peer review of the PSA commissioned by the dutyholders (for example, scope, findings, dutyholder’s action plan to address findings and their status) in order to plan and inform their own assessment. |  |
|  | Inspectors may consider requesting the dutyholders to conduct self-assessments against this TAG and provide the results to ONR. |  |
| **Table A1-1.2 PSA Scope** | | |
|  | The overall risk analysis of the NPP covers all sources of radioactivity at the facility (reactor core, fuel ponds, fuel handling facilities, waste storage tanks, etc).  Adequate justification is provided when sources of radioactivity are not included in the scope of the detailed PSA. |  |
|  | The PSA covers all types of initiating events (internal events, internal hazards, external hazards). |  |
|  | The PSA covers all operational modes (low power, at power, shutdown etc.). |  |
| **Table A1-1.3 Freeze Date** | | |
|  | The freeze date for the design and operational features reflected in a particular submission should be explicitly stated. |  |
|  | All the PSA models, data, documents and references that support the submission are up-to-date and consistent with the “freeze date”. |  |
| **Table A1-1.4 Computer Codes and Inputs** | | |
|  | The codes used (for example, for derivation of success criteria, accident progression analyses, analysis of structural integrity of containment and any other structures, fission product release and transport, consequences on human health, etc) have been verified, validated or qualified, as appropriate.  All codes and inputs meet ONR quality expectations as described in SAPs paragraphs 678 ff and [NS-TAST-GD-042](http://intranet/operational/nsd_bms/tech_asst_guides/tast042.htm) [7]. |  |
|  | The analyses, including the development and operation of the computer codes, have been performed by suitable qualified and experienced analysts. |  |
|  | The degree of accuracy, uncertainties and limitations associated with the selected computer codes are identified.  The codes have been used within their limit of applicability. |  |
|  | The modelling (nodalization) of the plant inputted as underlying basis for the code calculations (for example, thermal-hydraulic, accident progression, structural integrity, etc), is adequate and auditable. |  |
|  | The PSA quantification software is capable of quantifying the entire model. |  |
|  | The input data files for the code calculations are auditable.  The sources of information (for example, design documents) are identified. |  |
|  | ONR holds a license for the PSA quantification software used, or alternative suitable arrangements for PSA quantification by ONR inspectors (or their contractors) are feasible. |  |
|  | All computer files for the PSA model/s and reliability database/s have been provided to ONR. |  |
| **Table A1-1.5 Assumptions in the PSA** | | |
|  | All assumptions made throughout the study are clearly identified, described and properly justified.  The specific aspects of the PSA models or data related to these assumptions are clear.  A table of assumptions is provided. |  |
|  | The PSA may have to make use of assumptions for aspects of the facility not yet available / under development and also when factual information is missing or incomplete – it should be noted, however, that ONR would not consider acceptable the use of assumptions in the PSA in lieu of making use of factual information which is available or can be obtained. |  |
|  | A process is in place to capture, track and review assumptions made in the PSA, which could be affected by siting, design and construction, or operational matters (such as procedures, maintenance and testing strategies, training programmes, control room staffing and organisation, etc), which need to be reviewed when detailed information becomes available. |  |
|  | The system to capture, track and review PSA assumptions enables the latest available design and operational information to be transferred to the PSA so that assumptions (and models) can be reviewed accordingly. |  |
| **Table A1-2. Level 1 PSA** | | |
|  | All the criteria used in the Level 1 PSA are defined and are adequate, for example criteria for CORE DAMAGE for the Reactor PSA, criteria for FUEL DAMAGE for the Fuel Route PSA, etc. |  |
|  | If design targets for CORE DAMAGE FREQUENCY, FUEL DAMAGE FREQUENCY, etc, have been identified, these are explicitly stated. |  |
| **Table A1-2.1 Identification and Grouping of Initiating Events** | | |
|  | The task scope is explicitly stated:   * For the Reactor PSA, this task addresses all disturbances that require mitigation to prevent core damage and those that lead directly to core damage. * For the Fuel Route PSA, this task addresses all disturbances that require mitigation to prevent fuel damage and those that lead directly to fuel damage. |  |
|  | The process used in the identification and definition of initiating events is clear and leads to a systematic and comprehensive identification of initiating events. |  |
|  | Detailed records exist for all deductive analyses (for example, master logic diagrams) and / or inductive analyses (for example, failure modes and effects analyses) carried out to identify initiating events. All assumptions are captured. |  |
|  | Previous experience at similar NPPs has been searched for and fed back into the initiating event identification process. |  |
|  | The source documents (such as initiating event lists) used are identified. The applicability of the information extracted and used from these source documents is clear. |  |
|  | A database exists of abnormal events and incidents which have led (or could lead) to disruption of normal operation. This includes those equipment failures that led to an initiating event and any consequential failures to perform one or more of the safety functions required. It also includes information on any test or maintenance activity taking place at the time which could be related to the event. |  |
|  | A database exists for future recording of abnormal events and incidents which lead (or could lead) to disruption of normal operation. |  |
|  | The analysis of the applicability of the initiating events to each operating mode is transparent. |  |
|  | Consequential initiating events have been addressed and the way in which they are developed is clear. |  |
|  | Each initiating event is clearly defined and characterised (i.e. its causes and impact on plant are identified). |  |
|  | The process for grouping initiating events is clear, i.e. the grouping criteria and the mapping to derive the final initiating event groups are transparent. |  |
|  | Each initiating event group is represented by the most onerous event. |  |
|  | The initiating event groups have been defined in a way that vulnerabilities are not masked., for example, if a group is defined as plant transients causing reactor trip the source of vulnerability gets masked. |  |
|  | Each initiating event group is clearly defined and characterised. The information provided is sufficient for the quantification of initiating event frequencies (i.e. its causes are identified) and for the development of accident sequence models (i.e. its impact on plant is stated). |  |
| **Table A1-2.2 Accident Sequence Development: Determination of Success Criteria** | | |
|  | For each initiating event group, the safety functions, the systems which can perform each of the functions, and any need for operator intervention, are identified. |  |
|  | The sources and methods used for the derivation of success criteria are transparent. |  |
|  | The limiting conditions defined for success / failure (for example, cladding temperature, coolant system pressure, coolant system level, enthalpy in fuel pellets, containment temperature and pressure, etc.) are stated, justified, and are realistic. |  |
|  | The thermal-hydraulic, neutronics (and any other) analyses used for derivation of success criteria have been performed on a best-estimate basis and are specific to the facility. |  |
|  | Sufficient and representative thermal-hydraulic analyses have been performed to demonstrate that each of the success paths depicted in the event trees do indeed lead to successful outcomes (for example, non core damage). These analyses are available and traceable. |  |
|  | Sufficient and representative thermal-hydraulic analyses have been performed to demonstrate that a given system response will prevent the safety limit being exceeded. |  |
|  | Timing for operator actions is justified (for example, by sufficient and representative thermal-hydraulic analyses). |  |
|  | The supporting analyses used to define the success criteria for each success sequence in the event trees have adequately addressed the following:   * If initiating events have been grouped, the most onerous initiator is considered. * Sequence assumptions (for example, LOCA break location) have been appropriately chosen and justified to be bounding for the sequences depicted in the event trees. * The influence of the physical conditions that arise during the evolution of the sequences on the functionality and operability of the systems and the functions has been taken into consideration in the evaluation of the success criteria * The analyses have considered the mission time for each sequence (time required to reach a stable state that can be maintained without the actuation of additional systems) * Event timings and time window definitions have been adequately treated. * Timings for a manual action at a given header are based on accident sequence modelling which appropriately treats preceding manual actions. * Any conservatisms are identified, and there are no excessive conservatisms. * The use of the codes for each specific application is justified. |  |
|  | If use is made of success criteria for the various initiating event groups from sources other than facility-specific analyses, the rationale for this and the analysis of applicability are transparent and the justification is adequate. |  |
|  | The thermal-hydraulic, neutronics (and any other) analyses used for derivation of success criteria are thoroughly documented and fully traceable. |  |
|  | For each success criterion, all applicable items are identified and defined:   * Clear definition of exact meaning of ‘success’. * Minimum equipment requirements and performance for success (including mission times) * Details of the specific operator actuations required and latest time for manual actuation which can lead to success (especially considering any prior manual actions). |  |
|  | The inspector may choose to review in depth a representative subset of thermal-hydraulic, neutronics and any other supporting analyses. In these cases no significant errors have been found. |  |
|  | The inspector may choose to independently perform a representative subset of thermal-hydraulic, neutronics and any other supporting analyses. In these cases, the results obtained are consistent with those presented by the dutyholder. |  |
| **Table A1-2.3 Accident Sequence Development: Event Sequence Modelling** | | |
| Table A1-2.3.1 General | | |
|  | The general assumptions relating to all event tree development are defined up-front and adequately justified. |  |
|  | General information is provided on the type of event tree models produced and on the level at which the event tree headings are defined (safety function, system, train). |  |
|  | The descriptive text for all event tree headings is clear and consistent (and preferably expressed as functional success, e.g., “Injection of 2oo3 HHSI pumps” or “Operator starts depressurisation”, etc). |  |
|  | Sequence end states are identified and defined. |  |
|  | Any sequence end-state other than “Success” or “Core Damage” is identified and defined, the rationale for its use explained (including the overall contribution to the conclusions of the PSA). |  |
|  | As many event trees as necessary have been constructed so that the PSA model does not have asymmetries artificially built in. This is of utmost importance to ensure the suitability of the PSA to support a number of applications such as Risk Monitoring and those applications based on evaluation of the results of the Importance Analyses. |  |
| Table A1-2.3.2 Specific for each Initiating Event Group Event Tree | | |
|  | All the sequences have been developed to a point in which a safe stable state that can be maintained in the “long-term” without the actuation of additional systems has been achieved.  The sequence timings are stated and justified.  Sequences in which a safe stable state has not been achieved (within the established timing) have been assigned Core Damage states. |  |
|  | The evolution of the sequence of events following the representative initiator from each initiating event group is described. This includes the parameters that cause reactor trip, the signals / channels that initiate various safety functions, and the operators’ intervention during the sequence.  The timing of events in the sequence following the success or failure of signals / safety functions are identified and defined. |  |
|  | All dependencies (human actions, equipment, environmental, spatial, common mode failure, fluid medium) are identified and the way in which such dependencies have been treated and included in the accident sequences (either explicitly or implicitly) is correct.  Analysis to identify subtle dependencies has been carried out and these have been incorporated in the PSA models. Some examples of subtle dependencies are those which may arise between initiating event and the safety functions / systems due to software based control and protection systems, vapour locking of pipes due to high temperature, and other dependencies which may otherwise have been missed. |  |
|  | Each heading in the event tree is described, and its relationship to a functional fault tree, system fault tree, human failure event, or other event is identified. |  |
|  | When the same event tree heading is used with different boundary conditions for different sequences (for example, to capture dependencies on the success or failure of preceding event headings), the various boundary conditions for each heading are described. Its relationship, depending on each boundary condition, to one or more functional fault trees, system fault trees, human failure events, or other events is identified. The way in which this is implemented in the modelling is clearly described. |  |
|  | The mission time for each heading of each branch of the tree, when applicable, is stated and justified (see SAPs para 652).  (Note: The IAEA standard on Level 1 PSA No SSG-3 indicates in paragraph 5.49 says: *"The success criteria should specify the mission times for the safety systems, that is, the time that the safety systems will need to operate so that the reactor reaches a safe, stable shutdown state and that will allow for long term measures to be put in place to maintain this state. In many cases this has been taken to be 24 or 48 hrs for most initiating event. For new designs that provide the features to delay core damage, consideration of longer mission time may be necessary"*  There are more references to mission time in this standard (for example, paragraph 5.135, 9.28, 9.31, 9.53,).  The ASME PRA standard is also clear about this indicating that *the end states of the Level 1 PSA have to be a "Steady state condition" at the end of the mission time or "Core Damage")* |  |
|  | The link between the various headings / nodes of the event tree and the relevant thermal-hydraulic analyses performed to support the event sequence modelling is transparent. |  |
|  | The link is clear between the various headings / nodes of the event tree and the relevant operational and emergency procedures to be used. |  |
|  | Any basic event used to replace an integrated time dependent function (such as the failure to recover off-site power before a certain time interval has elapsed given that the diesel generators have failed to supply power) is properly described and substantiated. Confirmation is included that potential dependencies have been examined and also explanation of how these have been dealt with (if applicable) included. |  |
|  | The treatment of consequential initiators within the event trees is clear, as well as the transfer of the end state of sequences in one tree to initiators in other event trees. |  |
|  | Appropriate explanations are included of the functional fault trees developed to link the event tree headings with the system fault trees.  The link between the functional fault trees and the relevant success criteria is stated. |  |
|  | The functional fault trees provide an adequate representation of the functional failures intended. |  |
|  | The information required to set up the boundary conditions for the quantification of each sequence is transparent. |  |
|  | The event trees have been constructed correctly and provide adequate representations of the evolution of the accident sequences following all the initiating event groups under consideration. |  |
| **Table A1-2.4 Systems Analysis** | | |
| Table A1-2.4.1 General | | |
|  | The approach used for the definition of system boundaries is transparent and adequate. |  |
|  | The approach used to define component boundaries in the mechanical, I&C and electrical subsystems is transparent and adequate. |  |
|  | The general approach applied for the inclusion of unavailability’s due to test and maintenance activities, in the system models is transparent and adequate. |  |
|  | The general approach used for the inclusion of pre-accident human failure events (for example, individual and common cause component misalignments and mis-calibrations of instrument and protection channels) into the system models is clear and adequate. |  |
|  | The general approach used for the inclusion of post-accident human failure events (detection, decision errors, omission errors, commission errors, etc, and common cause human failures) into the system models is clear and adequate. |  |
|  | The general approach used for the inclusion of (hardware / software) common cause failure (CCF) events into the system models is clear. The approach is adequate and includes consideration of both intra-system and inter-system CCF events. |  |
|  | The general approach applied for the inclusion of structural failures into the system models is clear and adequate. |  |
|  | The general approach applied for the inclusion of passive component failures into the system models is clear and adequate. |  |
|  | The event naming scheme is clear and consistent throughout the models. |  |
|  | Generally applicable modelling assumptions, for example, those related to inclusion or exclusion of passive components, criteria for inclusion or exclusion of diversion paths, etc, are defined up-front and properly justified. |  |
|  | The list of failure modes applicable to each component type is identified up-front and complete. |  |
|  | The descriptive text for all fault tree gates and basic events is clear and it is consistently expressed as functional failure, e.g., “2oo3 HHSI pumps fail to inject”, “Pump X fails to start”, etc. |  |
|  | A description of the way in which circular logics (also known as logic loops) have been dealt with in the fault tree models is provided and is adequate. |  |
|  | The level of detail of the system fault tree models is consistent throughout the system analysis. |  |
|  | The level of detail of the fault trees is sufficient to ensure: that they are realistic; that the logic of the models is correct; that all the dependencies are captured; that the resulting cutsets for failures of the system reflect combinations of failures that can be easily understood; and that the data used is applicable to the boundary selected for each component basic event in the PSA. |  |
|  | The fault trees do not have asymmetries artificially built in. This is of utmost importance to ensure the suitability of the PSA to support a number of applications such as Risk Monitoring and those applications based on evaluation of the results of Importance Analysis. |  |
| Table A1-2.4.2 Specific for each System Model | | |
|  | A description of the system is available that covers: the description of the system and its operation modes, its normal configuration when the reactor is at power, its configuration(s) following reactor trip, and its configuration for non-power states. |  |
|  | A simplified system diagram is presented that includes all the components modelled (adequately labelled, and without omission) and that clearly indicates the system boundaries and interfaces with other systems. |  |
|  | The references to all design information / characteristics, including environmental qualification of all system components are listed and up-to-date. |  |
|  | The system boundaries are clearly identified and any gaps and / or overlaps at the interface with other systems modelled in the PSA are justified. |  |
|  | System success criteria are stated.  The success criteria applied in the PSA model (for example, the applied front-line system success criteria) are consistent with those obtained in the task on determination of success criteria.  The success criteria for support systems are consistent with the outcome from the task analysis of front line systems. |  |
|  | The information on dependencies for each component is transparent (including the support systems / actuation signal interface points).  Any dependency on room / cabinet cooling is considered when necessary for normal and post trip conditions for all initiators.  No dependencies are missing. |  |
|  | The resulting success criteria for the system’s support systems based on the above is stated. |  |
|  | Information on system tests is provided (including, for each system test, relevant aspects such as test frequency, components and failure modes tested, system realignments and component unavailability’s due to test). |  |
|  | Information on system maintenance for all components is provided (including the mechanical and electrical tag out boundaries, i.e. an identification of all the mechanical, electrical, instrumentation, etc, components which are functionally unavailable or isolated in order to perform the maintenance). |  |
|  | Fault tree modelling assumptions specific to the system (including all those assumptions made to simplify the model) are described, justified and reasonable. |  |
|  | Appropriate explanations are included to facilitate understanding of the fault tree logic. This should also include descriptions of the way in which specific circular logics have been removed. |  |
|  | All dependencies are captured in the fault tree and have been modelled correctly. |  |
|  | All relevant component failures have been correctly included in the fault tree. |  |
|  | The events that represent unavailability’s due to testing and maintenance have been modelled correctly.  All configurations allowed by the NPP procedures are represented in the models.  The chosen modelling “solution” to avoid combinations of maintenance activities forbidden by rules and procedures has been implemented properly. |  |
|  | Hardware failures that contribute to the Human Failure Events (for example, failure of the alarms or indications) have been included in the model.  Justification has been provided for any cases where these hardware failures have not been included based on the assumption that the HFE dominates. |  |
|  | All relevant human failure events have been correctly included in the fault tree |  |
|  | All house events (or equivalent) used to deal with asymmetry in the system alignment or to enable the single fault tree model to be used for the various possible system configurations are listed and described.  The purpose of each house event (or equivalent) is clear.  A table is included that lists the house events (or equivalent) modelled in the system fault trees and their settings in each heading, sequence or event tree. |  |
|  | The use of lumped, module events or super-components has been justified. |  |
|  | If lumped, module events or super-components (beyond the pre-established component boundaries) are used in the fault trees, the contents included within the boundary of the event are clearly identified (in terms of components, failure modes and interrelations). |  |
|  | If lumped, module events or super-components are used in the fault trees, information on dependencies (outside the event boundary) is transparent. These dependencies are properly captured in the fault tree models. No dependencies are missing. |  |
|  | All intra-system and inter-system CCFs to be modelled in the system fault tree have been identified in conformance with the general approach to the analysis of CCFs. |  |
|  | All hardware recoveries modelled are described and justified. |  |
|  | All the system fault trees (top gates) are listed together with their description. |  |
|  | All the gates which are transfers to other system models (for example, support system top gates) are listed together with their description. |  |
|  | All the modelled events are listed together with their descriptions. This list is traceable to the fault trees and the system simplified diagram and description. |  |
|  | The fault tree logic is correct. No events are missing. The fault trees provide an adequate representation of the system failures for the facility under evaluation. |  |
| **Table A1-2.5 Human Reliability Analysis (HRA)** | | |
|  | Note: The expectations in this table are consistent with the guidance provided in the TAG on Human Reliability Analysis NS-TAST-GD-063 [52] |  |
|  | The methodology/ies selected for the HRA, and in particular for the evaluation of human error probabilities (HEP), including the choice of human reliability data sources, is / are justified. |  |
|  | The types of human failure events, HFEs, (i.e. those basic events in the fault trees and event trees which represent the human-induced failures of functions, systems or components) that are included in the logic model structure are identified up-front. Important types of HFEs have not been omitted. |  |
|  | Pre-initiating event HFEs include individual and common-cause misalignments and mis-calibrations. The identification of these events is complete.  If some potential pre-initiating event HFEs are not included in the model, adequate justification is provided.  The modelling of pre-initiating event HFEs events is correct. |  |
|  | If HFEs associated with initiating events are embedded in the data used in the analysis of initiating event frequencies for the Full Power PSA, justification is provided that these human actions have been adequately captured.  Explicit analysis of HFEs associated with the initiating event is generally performed for the PSA for Low Power and Shutdown modes (see Table A1- 2.8 below). |  |
|  | Post-initiating event HFEs include failures to carry out required actions in response to procedures, alarms and other cues and un-required human actions in response to situations that have been diagnosed incorrectly. The identification of these events is complete.  If cases exist where the HFE related to the detection / decision part of the human action has been modelled separately from the HFE/s related to the manual actuation part of the human action, the rationale for this is clear.  If some potential post-initiating event HFEs are not included in the model, adequate justification is provided.  The modelling of post-initiating event HFEs events is correct. |  |
|  | For each pre-initiating event HFE**,** all the operational activities which could lead to the human error are identified (for example, surveillance tests, calibrations, maintenance activities or operational realignments). |  |
|  | For each pre-initiating event HFE**,** all the alarms, indications, surveillances or tests credited to contribute to the recovery of the mis-alignment / mis-calibration are identified. The ability to recover the HFE is clear in each case. |  |
|  | For each pre-initiating event HFE which involves failure to respond to procedural steps, equipment failures, alarms or other cues, the cues are identified. |  |
|  | Occasions for misdiagnosis of the situation by the operators have been analysed systematically.  HFEs resulting from identified credible misdiagnosis have been modelled correctly (for example, human actuations due to misdiagnosis that change the course of an accident sequence will normally be modelled in the event trees. Un-required switching off of systems due to misdiagnosis will normally be modelled in the fault trees). |  |
|  | The human reliability quantification method/s selected is / are suitable for the specific type of HFEs addressed with the method. |  |
|  | Specific human error contributors to each HFE are identified:   * The task analysis is complete: sub-tasks included as possible contributors to the HFE and the ones which are not included are identified. The rationale for the exclusion of sub-tasks is clear. |  |
|  | Facility-specific and HFE-specific influences of the factors required by the quantification model (Performance Shaping Factors, PSFs) are identified.  Facility-specific information obtained from observations made during walk-downs and simulator exercises, review of procedures, discussions with, and interviews and questionnaires to personnel, etc, is used to characterise the PSFs for each HFE. The sources of information are identified and auditable. The way in which this information is used is transparent. |  |
|  | Time windows are appropriately assigned; justification is given for the choice of events that mark the start and end of the time windows (cues and limiting times), dead times and time spent on other tasks are accounted for and adjustments made as appropriate. |  |
|  | Specific expectations for the assessment of the HRA in Low Power and Shutdown PSA are included in Table A1- 2.8 below. |  |
|  | Specific expectations for the assessment of the HRA for the Hazards PSA are included in Table A1- 2.7 below. |  |
|  | The quantification of all the HFEs is transparent.  The quantification of all the HFEs has been done correctly and in accordance with the HRA method/s selected. |  |
|  | If the probabilities for some HFEs in the models have not been calculated using detailed HRA analyses (as above), an adequate justification for the generic (screening) values used is provided. |  |
|  | Dependencies between HFEs appearing in the same accident sequence are identified and accounted for.  The process by which the candidates for dependency were identified is transparent.  Any assumptions made in the dependency analysis are described and justified.  The determination of the degree of dependency is transparent and justified.  The method by which the conditional probabilities of dependent HFEs are calculated is clear.  The dependency analysis is adequate. |  |
|  | A list of all the HFEs included in the PSA, and their associated mean probabilities and uncertainty ranges is included. This list is traceable to all the supporting analysis. |  |
| **Table A1-2.6 Data Analysis** | | |
| Table A1-2.6.1 Initiating Event Frequencies | | |
|  | The initiating event definitions used in the data analysis task are fully consistent with those used in the list of initiating events. |  |
|  | The criteria for selection of analysis methods are stated.  The approaches used to quantify initiating event frequencies are suitable for each type of initiating event addressed.  The approach/es used to quantify frequencies of consequential initiating events is reasonable and adequately justified. |  |
|  | The criteria for selection / precedence of data sources are stated. |  |
|  | Facility-specific event data has been used to the extent possible.  For cases where facility-specific event data is used, the source of event records is available, comprehensive and auditable.  Facility-specific records have been interpreted correctly. |  |
|  | For cases where operational experience from NPPs of similar design is used, its applicability is justified and the data used is auditable. |  |
|  | In all cases where either NPP-specific data or data from NPPs of similar design has been used, information on the operating history of the facility/ies where the event/s occurred has been used in the determination of the denominators for the evaluation of initiating event frequencies. This information is auditable. |  |
|  | For cases where generic reactor type initiating event frequencies are used, this is justified and documented in an auditable fashion. |  |
|  | For cases where several sources of data are combined, the method of combination is mathematically correct and has identified and taken into consideration possible overlaps between the various data sources. |  |
|  | For cases where logical models are used to calculate the initiating event frequencies, these include all the foreseen inputs leading to the initiating event.  The fault trees, human reliability analyses or other models used to calculate initiating event frequencies are documented. In order to assess these, inspectors can use the relevant tables of this Appendix. |  |
|  | The initiating event groups are assigned frequencies equal to the summed frequency of all the events in the group. |  |
|  | A list of all the initiating events, together with their frequencies, is included. Each initiating event frequency is represented by a mean value and a statistical representation of its uncertainty. This list is traceable to the supporting analyses. |  |
|  | A list of all the initiating event groups, together with their frequencies, is included. Each initiating event group frequency is represented by a mean value and a statistical representation of its uncertainty. This list is traceable to the supporting analyses. |  |
| Table A1-2.6.2 Random Component Failure Probabilities | | |
|  | The component populations together with their characteristics (e.g those that define each population and make it a coherent set) are clearly identified. The component populations defined are adequate. |  |
|  | The component boundaries (for each component population) used in the data analysis task are shown to be exactly the same as those used in the fault tree models. |  |
|  | The criteria for selection / precedence of data sources are stated. |  |
|  | For each component population that has been assigned failure rates from a generic data source (or a source other than the facility itself), justification is provided that the source is appropriate. Evidence is included that the component boundaries (for the particular component population) in the PSA and in the generic source of data are consistent. |  |
|  | For cases where several sources of generic data are combined: the method of combination is transparent; it has identified, and correctly taken into consideration, possible overlaps between different sources of generic data; and it is mathematically correct. |  |
|  | Facility-specific data has been used to the extent possible.  Where facility-specific data has been used either in isolation or combined with generic data to calculate failure rates for component populations, (including the use of multiple subcomponent data within the fault tree component boundary) the event records, engineering data, and operating history data (for example, records of operating / stand-by hours, of test / maintenance / repair time history) which have been used are available and traceable.  Evidence is provided that the PSA data analysts have checked the quality and reliability of the facility-specific records used to support the PSA. |  |
|  | Facility-specific records have been interpreted correctly (in particular to identify the failure modes modelled in the fault tree)  The interpretation of historical records to reconstruct demand counts, operational times, etc. is clear. |  |
|  | The method used for estimating failure rate parameters from raw data is transparent and mathematically correct. No calculation errors are identified. |  |
|  | The method used for estimating failure rate parameters from combinations of generic and facility-specific data (or of pre-existing and new facility-specific data) is transparent, mathematically correct and state-of-the-art. No calculation errors are identified. |  |
|  | For component types where manufacturer’s data or expert-judgement has been used, a robust justification is provided that neither facility-specific, nor generic data are available.  In instances where expert judgement has been used to estimate component failure rates, the process is transparent and robust and the outcome of the process is reasonable. Error factors are assigned commensurate with the uncertainty in the process.  Instances where manufacturer’s data has been used are clearly stated and the resulting failure rates are reasonable. Error factors are assigned commensurate with the uncertainty in the data used. |  |
|  | Facility-specific information on test intervals is used to calculate probabilities for the failure modes of the components on standby. The tests selected are suitable for the failure modes of concern. This information is consistent with the information on system testing recorded in the documentation of the system analysis. |  |
|  | The mission times (used to calculate the probabilities of failure to operate of components) are appropriate and consistent with the information on mission times recorded in the documentation of the Success Criteria Determination task. |  |
|  | The methodology used for the calculation of structural failure probabilities is justified. The details of the analysis are transparent.  If use is made of data from structural (for example, pipework) failure databases, the sources of data and the way in which this data has been used are clear. The applicability of the data is justified.  If use is made of a probabilistic fracture mechanics code, the code is state of the art. Evidence is provided that the code has been validated against operational experience and / or experiments. Evidence is provided that the code users are sufficiently qualified and experienced to be aware of the code’s capabilities and limitations.  The range of loads and combinations of loads that could lead to the structural failures of concern should be adequate to represent the conditions which are possible for the NPP under evaluation.  Inspectors should refer to TAGs -016 (Metallic Structures) [39] and TAG-017 (Civil engineering structures) [63] for further guidance here. |  |
|  | Assumptions on the reliability of passive systems / features are substantiated by appropriate and sufficient analysis covering the full range of fault and accident conditions for which they are required and by appropriate tests. The supporting evidence is available. |  |
|  | The methodology used for the estimation of failure probabilities for computer-based systems is transparent and meets industry-accepted practices.  The analysis of the software reliability carried out by the dutyholder has identified the influencing factors that affect the quality of the software. The results of these analyses have been taken into account in the reliability calculation in a transparent manner.  If the software system has been separated into parts that are treated individually in the reliability analysis, the dependencies between the various parts are addressed explicitly.  The reliability analysis of the computer-based hardware is documented.  Any self-checking built into the systems is taken into account in an adequate manner.  The dependencies between diverse software systems are dealt with explicitly.  Inspectors should refer to [NS-TAST-GD-046](http://intranet/operational/nsd_bms/tech_asst_guides/tast046/index.htm) for further guidance on computer-based systems. |  |
|  | A list of all the basic events that represent random component failures together with their parameter estimates is included.  Each parameter estimate is represented by a mean value and a statistical representation of its uncertainty.  This list is traceable to the supporting analyses. |  |
| Table A1-2.6.3 Unavailabilities Due to Testing and Maintenance | | |
|  | The descriptions of events that represent unavailability’s due to testing and maintenance (planned and unplanned) in the data analysis task are fully consistent with the unavailability events modelled in the system fault trees. |  |
|  | The criteria for selection / precedence of data sources are stated. |  |
|  | For cases where generic data has been used, a justification is provided.  Assumptions regarding unavailability time are stated and are reasonable. |  |
|  | Use of facility-specific data is traceable to existing records.  Justification is provided that the time span of the facility-specific data used in the PSA is sufficient to obtain realistic estimates of the unavailability’s. |  |
|  | The probabilities assigned to events that represent configurations not observed during the data collection period are reasonable best estimates. |  |
|  | The calculation of unavailability’s due to testing and maintenance (planned and unplanned) is correct and applicable for the operational state of the facility to which they are applied. |  |
|  | A list of all the basic events that represent unavailability’s due to testing and maintenance (planned and unplanned) together with their parameter estimates is included.  Each parameter estimate is represented by a mean value and a statistical representation of its uncertainty.  This list is traceable to the supporting analyses. |  |
| Table A1-2.6.4 Common Cause Failures (CCFs) | | |
|  | The approach selected for the CCF basic event modelling and analysis is justified.  The method chosen for CCF parameter estimation is transparent and meets good international practice. |  |
|  | The approach selected for the CCF modelling and analysis is detailed enough to adequately represent all levels of redundancy provided for in the specific facility design and to obtain appropriate CCF parameter estimates for such levels of redundancy.  The approach selected for modelling CCFs addresses both intra-system and inter-system CCF events. |  |
|  | The CCF event names and definitions are the same as those used in the fault tree models. |  |
|  | The criteria for selection / precedence of data sources are stated.  The applicability of the CCF data sources used is justified. |  |
|  | If a screening approach has been adopted to narrow down the number of detailed analysis to be performed, the screening criteria used is stated. The screening values for the CCF model parameters are justified. |  |
|  | If generic CCF parameters are used, the reasons why these values are considered appropriate are clear. Evidence is provided that the component boundaries, failure modes and failure root causes are consistent with those assumed in the generic data sources. |  |
|  | If CCF evaluation has been performed using a pseudo-facility-specific database for which industry-wide data has been reinterpreted for the specific conditions of the NPP under evaluation, the analysis of NPP-specific defences against CCFs relative to those expected for the facility from which the data were originally taken is traceable and appropriate. |  |
|  | If CCF raw data or information available internationally is used (for example, data from the International Common Cause Failure Data Exchange, ICDE, project), its applicability is justified and the way in which the data or information is used is transparent. |  |
|  | For cases where expert-judgement has been used for CCF parameter estimation, a justification is provided. The expert judgement process is transparent and robust and the outcome of the process is reasonable. Error factors are assigned commensurate to the uncertainty in the process. |  |
|  | The quantification of all the CCF events is transparent and has been done in accordance with the CCF method/s selected. No errors are apparent. |  |
|  | A list of all the CCF events, together with their parameter estimates is included. Each CCF parameter estimate is represented by a mean value and a statistical representation of its uncertainty. This list is traceable to the supporting analyses. |  |
| **Table A1-2.7 Analysis of Hazards** | | |
| Table A1-2.7.1 General | | |
|  | The analysis of hazards starts from a complete list of internal and external (natural and man-made) hazards. |  |
|  | The approach and criteria for the screening of hazards are auditable and justified. |  |
|  | The reasons why the hazards selected for further analysis are applicable to the NPP under evaluation are included.  The reasons why the hazards excluded from the analysis are not applicable to the NPP under evaluation are clear and justified. |  |
|  | The frequencies and magnitude of all hazards selected for analysis are identified. |  |
|  | The hazard impact analysis (as a function of the magnitude of the hazard if appropriate) is auditable and covers possible initiating events, damage to equipment and structures, and impact on human performance.  The hazard impact analysis has been undertaken using an adequate method and is auditable. |  |
|  | The hazard analyses reflect facility-specific and site-specific features appropriately. |  |
|  | Specific modifications made to the internal events PSA models (event trees and fault trees) and parameters (for example, HEPs), or any new models and parameters developed to analyse the risk associated with the hazard under evaluation are auditable. |  |
|  | Tables A1-2.7.2, A1-2.7.3 and A1-2.7.4 provide specific expectations when assessing PSA for internal fires, internal flooding and seismic events. This guidance may also be applied by inspectors assessing PSA for other types of internal or external hazard, provided care is taken to ensure its applicability. |  |
| Table A1-2.7.2 Analysis of Internal Fires | | |
|  | The method selected for the analysis of internal fires is justified. |  |
|  | The approach chosen is sufficiently detailed to allow a realistic estimation of the fire risk and the identification of specific strengths and vulnerabilities. |  |
|  | Where appropriate, evidence that walk-downs have been conducted is included and documented in detail . The link between the information compiled during the walk-downs and the various aspects of the Fire PSA is apparent throughout. |  |
|  | General assumptions of the fire analysis are stated and properly justified. |  |
|  | If screening processes are undertaken during the various steps of the Fire PSA to reduce the amount of detailed analysis to be performed, the qualitative and quantitative criteria applied for screening fire compartments are stated.  The qualitative and quantitative screening criteria are adequate to ensure that the risk from individually screened-out scenarios and their cumulative contribution to the risk (in terms of contributions to the frequencies of core damage and significant releases) are acceptably low.  Assumptions made in support of the initial quantification of fire compartments for the purpose of quantitative screening are transparent (for example, assumptions on the impact of fires on equipment, human reliability, etc) and adequate. |  |
|  | The global boundary of the analysis is defined so that this includes all locations at the NPP relevant to the risk calculations (for example, all areas of the facility associated with normal and emergency reactor operating plant and support systems, with power production, areas associated with a sister unit containing shared equipment etc). |  |
|  | The Fire PSA is based upon a subdivision of the NPP into well-defined compartments with non-combustible barriers (i.e. which substantially confine the heat and products of combustion associated with a fire). In cases where the barriers are not fire-rated, these are identified and addressed in the inter-compartment analysis.  Details of the compartmentalisation of the facility are transparent and include a description of the partitioning elements or features which have been assumed.  A list of all compartments is included using a consistent identification scheme.  Up-to-date drawings or references showing compartment boundaries are available. |  |
|  | The process to identify essential equipment has identified all equipment whose failure or mal-operation will cause an initiating event or will adversely impact credited functions or operator actions. The location of this equipment, together with its normal, desired and failed positions on loss of services are identified. |  |
|  | Established procedures are in place and implemented for evaluating circuits and selecting cables required to support the operation of essential equipment. |  |
|  | Equipment circuits and cables required to support the credited functionality of essential equipment are identified.  All potentially impacting power supplies are identified. This may include power supplies not evaluated in the internal events PSA. For example, the power supply to a normally closed valve which is required to remain in position and which would remain closed on loss of power would have been excluded from the fault trees for internal events. However, these power supplies need to be identified for the analysis of internal fires, since a fire may lead to spurious energisation and opening of the valve.  Cable routing information (including associated equipment, cable IDs, raceways, locations etc) is stored in a database. This information should be readily retrievable and kept up-to-date. |  |
|  | If a first qualitative screening of fire compartments is undertaken, the details of this are transparent.  The screening has been performed in accordance with established criteria.  A list of all compartments screened-in is included. This list includes all compartments that could make a potential contribution to the risk from fire. |  |
|  | Descriptions of all fire compartments qualitatively screened-in are available. The descriptions include information on equipment allocation, potential fire sources and targets, fire load, passive protection, detection and suppression equipment, fire spreading paths (for example, failed barriers or ventilation ducts and fire dampers) and other information necessary for the analysis, such as the control programmes for combustible and ignition sources for the specific compartment. |  |
|  | Evaluation of fire frequencies has been performed for all the compartments qualitatively screened-in.  The method for the calculation of fire frequencies, including the input data and information used, is clear.  Generic and NPP-specific fire history information is used to establish fire frequencies associated with individual fire source types. The use of data from generic sources and facility-specific sources is justified and transparent.  If fire severity is used as a criterion to screen generic and NPP-specific events from frequency evaluations, then this should be transparent and justified.  NPP-specific fire characteristics (such as the type and number of fire ignition sources and evaluation of transient combustibles) are used to apportion the expected influence on the likelihood of ignition in specific fire compartments in a transparent and adequate manner. Assumptions made in lieu of facility-specific information are only made for NPPs not yet built and when used, are identified explicitly.  Fire suppression is not taken into account in the calculation of fire frequencies.  The calculation of fire frequencies for all fire compartments is documented explicitly. No errors are apparent.  A list of all the compartments together with their fire frequencies is included. Each fire frequency is represented by a mean value and a statistical representation of its uncertainty. This list is traceable to the supporting analyses. |  |
|  | If a quantitative screening of fire compartments is undertaken, the details of this are transparent.  The screening has been performed in accordance with established criteria.  A list of all compartments with an indication of whether they have been quantitatively screened-out (and the reason why), or screened-in (retained for detailed compartment analysis) is included. |  |
|  | Detailed analysis has been performed for all the compartments quantitatively screened-in.  The fire scenario (or scenarios) associated with each compartment is properly characterised in terms of source, propagation, detection, human response and damage:   * For each compartment, details of the specific fire sources and targets are transparent. Evidence that all potential ignition sources have been addressed is provided. * The analysis of fire growth within each compartment is transparent. Evidence is provided that the fire model used to analyse fire growth has been validated and verified. * The analysis of fire impact in each fire compartment is transparent and takes into account: * Equipment damaged in the compartment by flame, plume, ceiling jet, hot gases and radiant heat. * Electrical faults (open circuits, shorts to ground, short circuits and hot shorts) and their impact, e.g., loss of equipment function, spurious actuation of equipment (for example, undesired reconfiguration of valves or actuation of standby systems), loss and / or false signals and indications. * Explosions and their impact, including high-energy arcing faults. * Collapse of structures and their impact. * Missiles and their impact. * Smoke and heat effects and their propagation to neighbouring compartments. * Identification of initiating events in each compartment as the result of the fire. * For each compartment, a fire progression tree (or equivalent) has been developed that shows the fire source, defined fire growing stages, success / failure of fire suppression before reaching a given damage stage or triggering of an initiating event. The end points of these analyses are one or more fire damage states for each compartment with associated frequencies. These are taken forward for quantification. * The reliability of the various fire protection measures (both in terms of equipment as well as human performance) is substantiated.   For compartments where more than one fire scenario has been identified, clear and unambiguous identification of the various fire scenarios in the compartment is included. Individual analyses for the separate fire scenarios in the compartment is provided (the above bullets also apply to individual scenarios).  In cases where compartments have been further divided into sub-compartments for the detailed analysis, the rationale for this is transparent and details of this are documented explicitly. The design features and the automatic and manual actions that prevent fire propagation between sub-compartments are identified explicitly. Adequate justification of the effectiveness of these measures is provided. Individual analyses for the separate sub-compartments is provided (the above bullets also apply to individual sub-compartments). |  |
|  | The analysis of inter-compartment fire propagation is documented explicitly.  The requirements listed above for fire modelling of single compartments are applied to the modelling of multi-compartment scenarios.  Evidence is provided that passive fire barriers credited for preventing inter-compartment propagation (in the absence of suppression activities) are adequately rated and properly installed and maintained.  The effectiveness and reliability of any active fire barrier (for example, damper, suppression system) is explicitly addressed in the fire risk model and the risk contribution associated with its failure is evaluated.  Details of the fire barrier and propagation analysis (barrier penetration analysis) are transparent.  Scenarios involving two or more compartments are identified and characterised explicitly. Screening criteria applied to multi-compartment analysis are consistent with the single compartment qualitative criteria.  Multi-compartment scenarios which cannot be screened-out are carried onto the next stages of the Fire PSA. |  |
|  | Details of the accident sequence modelling and quantification for each identified scenario are transparent. In particular:   * The most onerous initiating event has been selected to be the basis for the quantification of each fire scenario. The rationale for this selection is clear. * The internal events PSA model has been suitably modified so as to be capable of representing fire-induced equipment failures and mal-operations or degraded human errors in combination with non-fire-related, random failures. For example potential failures or combinations of failures may have been neglected on the grounds of low probability in the internal events analysis, which may be significant in the event of a fire. * Details of the human reliability analysis in fire scenarios are auditable. The impact of specific actions that operators may take in accordance with post fire procedures, or erroneously due to spurious indications following a fire, which may degrade credited PSA functions, have been modelled appropriately. The impact of fire on human performance, for example in terms of potential enhanced stress, accessibility for local actuations (for example, in scenarios of CCR abandonment), etc, is analysed fully and transparently. The HRA for fire scenarios is adequate. * The quantitative and qualitative results of the quantification of each fire scenario are included. * The results of the Fire PSA also include an estimate of the core damage and significant release frequency arising from the set of compartments screened-out from the analysis. |  |
| Table A1-2.7.3 Analysis of Internal Flooding | | |
|  | The approach to Flooding PSA adopted is sufficiently detailed to allow a realistic estimation of the risk from flooding and the identification of specific strengths and vulnerabilities. |  |
|  | Evidence that walk-downs have been conducted is included and documented in detail (since flooding risk analyses can only be realistic when supported by local walk-downs). The link between the information compiled during the walk-downs and the various aspects of the Flooding PSA is apparent throughout. |  |
|  | General assumptions of the flooding analysis are explicitly stated and properly justified. |  |
|  | If screening processes are undertaken during the various steps of the Flooding PSA to reduce the amount of detailed analysis to be performed, the qualitative and quantitative criteria applied for screening flood compartments are stated.  The qualitative and quantitative screening criteria are adequate to ensure that the risk from individually screened-out scenarios and their cumulative contribution to the risk (in terms of contributions to the frequencies of core damage and significant releases) are acceptably low.  Assumptions made in support of the initial quantification of flood compartments for the purpose of quantitative screening are transparent (for example, assumptions on the impact of floods on equipment, human reliability, etc) and adequate. |  |
|  | The global boundary of the analysis is defined so that this includes all locations at the NPP relevant to the risk calculations (for example, all areas of the facility associated with normal and emergency reactor operating plant and support systems, with power production, areas associated with a sister unit containing shared equipment etc.). |  |
|  | The Flooding PSA is based upon the subdivision of the NPP into well-defined compartments (physically separate areas where flood is generally viewed as independent of other areas in terms of impact).  Details of the compartmentalization of the facility are available including physical barriers (walls, floors, bunds etc), mitigating features (sumps, drains) adjacent compartments and propagation paths (open hatches, etc).  A list of all compartments showing compartment boundaries is included. Up-to-date drawings or references to these are included. |  |
|  | Descriptions of the content of all flood compartments are available. The descriptions include information on all equipment susceptible to flood located in each of compartment, the minimum water volume needed to affect water-sensitive equipment by immersion / splashing, internal flood barriers and spray shields, potential flood sources and types (for example, high energy steam pipework), automatic and manual flood detection and isolation means, possible flood effects in each compartment (for example, initiating events, damage to safety equipment) and in compartments to which the flooding may propagate, etc. |  |
|  | The susceptibility of each type of component appearing in the PSA to flood-induced failure mechanisms is identified and justified (for example, submergence, jet impingement, pipe whip, humidity, condensation, temperature) |  |
|  | For each flood source, the propagation path from the source compartment to the point of accumulation is identified, including the potential for structural failures of walls, doors, back flow device failures, HVAC ducts, etc. |  |
|  | Details of the first qualitative screening of flood compartments and flood sources are auditable.  The screening has been performed in accordance with established criteria.  A list of all compartments screened-in is included. This includes all compartments that could make a potential contribution to the risk from internal flooding. |  |
|  | Evaluation of flooding frequencies has been performed for all the compartments qualitatively screened-in.  Generic and NPP-specific flood history information is used to establish flood frequencies and severities associated with individual flood source types. The use of data from generic sources and NPP-specific sources is justified and transparent.  The method for the calculation of flood frequencies, including the input data and information used, is clear.  For each compartment, the nature of possible flood causes is identified, for example, maintenance activities, pipe breaks, expansion joint breaks, etc. Assumptions made in lieu of facility-specific information are only made for NPPs not yet built and when used are identified explicitly.  For each compartment, the location and characterisation of flood sources, describing, for example, the system that is the source of the flooding, source location, flow rate maximal flood volume and flood frequency, are transparent. Assumptions made in lieu of facility-specific information are only made for NPPs not yet built and when used are identified explicitly.  Similar flood cases are adequately grouped in the modelled scenarios. All the assumptions made in this process are transparent.  The calculation of flood frequencies for all identified flooding scenarios is documented explicitly. No errors are apparent.  A list of all the identified flooding scenarios, together with their frequencies, is included. Each frequency is represented by a mean value and a statistical representation of its uncertainty. This list is traceable to the supporting analyses. |  |
|  | Details of the quantitative screening of flood scenarios are transparent.  The screening has been performed in accordance with established criteria.  A list of all flood scenarios with indication of whether they have been quantitatively screened out (and the reason why), or screened in (retained for detailed analysis) is included. |  |
|  | Detailed analysis has been performed for all the flood scenarios quantitatively screened-in, including:   * For each compartment where a flooding scenario has been identified, the rate at which a flood could develop is provided. * The equipment which is assumed to be damaged by water spray, jet impingement, pipe whip etc. due to the flood source is identified. * Flood effects in the compartment due to, for example, equipment immersion, humidity and temperature are identified. These cover both initiating events and equipment damage. * Adverse effects in compartments affected by the propagation of floods are identified. * For each flooding scenario, a flood progression tree (or equivalent) has been developed that identifies flood progression stages reached (leading to an initiating event or to damage to any relevant system) depending on the success or failure of flood isolation actions. * Indications, events and any other cues which can provide flood symptoms and allow for flood detection are identified explicitly. * Actions needed for flood isolation before a given flood progression stage is reached are described explicitly. * The reliability of the flooding protection measures (both in terms of equipment as well as human performance) are substantiated. |  |
|  | Details of the accident sequence modelling and quantification for each identified scenario are transparent. In particular:   * The initiating event identified for each flood scenario is justified. * The modifications made to the internal event PSA event trees and fault trees (and any new models developed) to calculate the probability of core damage and significant release at various evaluated progression stages, taking into account the impact of the flood on safety systems and operating crew actions are transparent. The resulting models reflect the plant and justified. * Details of the human reliability analysis for flooding scenarios are transparent. The flood-related factors that may influence human performance are identified explicitly. The analysis is complete and transparent. The HRA for flooding scenarios is adequate. * The quantitative and qualitative results of the quantification of each flooding scenario are included. * The results of the Flooding PSA also include an estimate of the core damage frequency and significant release frequency arising from the set of flooding compartments / scenarios screened-out from the analysis. |  |
| Table A1-2.7.4 Seismic Analysis | | |
|  | The approach used to evaluate and represent the hazard from earthquakes is described and appropriate |  |
|  | The seismic hazard analysis is documented in detail.  The assumptions and models used for aspects such as the characterisation of sources and attenuation relationships are clearly identified.  All the values for the parameters used in the model are identified and the way the final hazard curves have been constructed is auditable.  The mean curve for the site is represented together with its uncertainty bounds. This is traceable to the underlying analyses. |  |
|  | All the references to historical data used are identified and auditable. |  |
|  | The approach used to evaluate the impact of earthquakes on the NPP structures and components is described and appropriate. |  |
|  | All the equipment that requires analysis of the probability of failure against earthquake magnitudes is identified, i.e. all equipment required to trip, shutdown, cool and monitor the reactor, all structures whose failure could hamper core cooling, and all equipment and structures required to mitigate severe accidents or whose failure could impact releases (Level 2 PSA), etc.  This list is traceable to safety case / internal events PSA sources. |  |
|  | Any screening criteria used to limit the number of components for which detailed fragility analysis has been performed is defined and is adequate.  The screening analysis is traceable. |  |
|  | The design parameters used for the derivation of fragilities of equipment and structures are identified. |  |
|  | The method used to evaluate seismic fragilities is described.  If different methods have been to evaluate the fragilities for different components or structures, the methods lead to consistent results. |  |
|  | The fragility analysis is auditable. |  |
|  | The results of the screening analysis of relay and contactor chatter for the safety systems are included with a list of relays and associated fragilities included in the final model. |  |
|  | The initiating events arising from the full range of earthquakes are identified. |  |
|  | Any screening criteria used to limit the number of earthquake-induced initiating events considered in the Seismic PSA quantification is defined and is adequate.  The screening analysis is traceable. |  |
|  | The potential for secondary hazards, for example, earthquake-induced fires and floods has been analysed systematically during the seismic walk-down and the results are auditable. |  |
|  | The way in which the seismic failures and successes and random component failures have been combined is traceable.  If seismic damage states have been developed, each of them correctly represents the frequency of the associated seismic failures by the mathematically correct inclusion of the combination of failure and success paths.  Any modifications to the event and fault tree logic models to incorporate the impact of earthquakes on the NPP are auditable and correct.  The potential for the correlation of seismically-induced component or structural failures has been addressed and any assumptions made regarding the correlation are identified and justified.  The Human Reliability Analysis has been revisited to address the operator response following the seismic events of concern. Details of this analysis are auditable. |  |
|  | The quantitative and qualitative results of the quantification are included.  Sensitivity, uncertainty and importance analyses are provided. |  |
| **Table A1-2.8 Low Power and Shutdown Modes** | | |
|  | Note: The expectations listed in the tables A1-2.1 to A1-2.7 above are also applicable to the Low Power and Shutdown parts of the PSA. Table A1- 2.8 therefore only deals with additional expectations applicable specifically to this part of the analysis. |  |
|  | The identification of the Plant Operational States (POS) during non-full power modes is justified.  Any gaps and / or overlaps between the POS addressed in the Low power and Shutdown PSA and those covered in the PSA for full power are justified.  All the characteristics considered for the identification of possible stages during low power and shutdown (pre-POS) are clear. No important characteristic is missing.  The grouping of pre-POS into the final list of POS is justified and visible. The grouping is adequately justified. |  |
|  | A table listing all the POS with their characteristics is included. The information about all the POS’ characteristics is presented and complete.  Information about plant configuration (decay heat removal method, cooling circuit configuration, etc) in each POS, frontline system availability in each POS, length of time in each POS, assumed decay heat levels is presented. |  |
|  | The definition and characterisation of each POS is traceable to facility-specific information. |  |
|  | The analysis of initiating events for each POS is transparent.  The analysis of initiating events has considered events based on plant failures, those triggered by operator interactions and those caused by internal and external hazards. The details of the analysis are transparent. |  |
|  | A systematic examination of NPP procedures for changing configurations, equipment testing and maintenance procedures has been carried out to identify potential human errors during the execution of such normal procedures that are, or may lead, to initiating events. The analysis process is transparent. |  |
|  | A table showing the initiating event groups defined and their applicability to each POS is presented. No errors are apparent |  |
|  | The derivation of the frequency of the initiating events is specific for each POS (i.e. it has taken into consideration the specific characteristics of each POS). The analysis is transparent.  The models used to calculate IE frequencies are presented.  The frequency of each initiating event is calculated on a per calendar year basis (so that the risks associated with each POS can be compared). Otherwise the units used are explained. |  |
|  | If screening of combinations of initiating event groups / POS is undertaken to reduce the amount of detailed analysis to be performed, the screening approach, criteria and process are clear and acceptable. The screening process does not lead to the removal of events that may be significant for the intended applications of the PSA. |  |
|  | The thermal-hydraulic, neutronics (or any other) analyses performed to support the determination of success criteria for the Low Power and Shutdown PSA are presented.  The thermal-hydraulic analyses performed to support the determination of success criteria for the Low Power and Shutdown PSA have taken into consideration the specific characteristics of these operating modes, for example, reactor coolant system water inventory, steam generator availability, core inventory, decay heat curve. The boundary conditions used in these analyses are stated.  The success criteria for the Low Power and Shutdown PSA are developed on a realistic basis. |  |
|  | Event trees have been developed for each combination initiating event-POS that has been screened-in. |  |
|  | System models have been developed taking into consideration the specific characteristics of each POS. Details of this are transparent. |  |
|  | References to all maintenance procedures and work plans which are used to define the event tree boundary conditions and system status modelled in the fault trees are explicitly stated. |  |
|  | The HRA method selected can adequately represent the aspects of the NPP shutdown relevant to human reliability which may be different to when the reactor is operating at power, for example, long time windows for operator actuation, status of procedural guidance and training, familiarity with shutdown accident transients, levels of supervision, availability of indications / status of the control room, difficulties in diagnosing events, increased workload, etc.  The HRA has considered all the aspects of the NPP shutdown relevant to human reliability mentioned above clearly and systematically. |  |
|  | Specific aspects of the low power and shutdown modes that may affect the risk due to hazards (which may differ from when the reactor is operating at power) have been clearly and systematically addressed.  Examples of specific aspects that inspectors should expect the PSA to address are:   * Internal fires: amount of hot work; additional inventories of combustible materials introduced into some areas; status of automatic fire suppression systems, fire barriers, fire doors and penetration seals, etc. * Internal flooding: temporary water systems and hose connections; different plant configurations and possibilities of valve misalignments leading to flooding; status of drainage systems, doors in segregation barriers and penetration seals, increased possibility of maintenance errors leading to floods, etc. * Dropped loads: number of heavy loads lifted during maintenance outages; potential for dropped loads to directly affect spent fuel during the refuelling, etc. |  |
| **Table A1-2.9 Uncertainty analyses, Quantification and Interpretation of the Level 1 PSA Results** | | |
| Table A1-2.9.1 Uncertainty and Sensitivity Analyses | | |
|  | The sources of uncertainty in the Level 1 PSA are identified explicitly.  Suitable methods are chosen to address the various types of uncertainty, to evaluate their impact on the results of the PSA and to interpret their significance. |  |
|  | Sensitivity studies have been carried out to evaluate the risk significance of assumptions.  The sensitivity studies address the effects of key assumptions and combinations of assumptions.  The sensitivity studies and their results are transparent. |  |
|  | Uncertainties in input probability and frequency values have been estimated.  Uncertainties in input probability and frequency values have been propagated through the models to generate uncertainty distributions for the results of the Level 1 PSA.  The means resulting from the uncertainty propagation are the values that have been compared against the relevant numerical criteria (rather than using the point estimate means which result from a simple arithmetic evaluation of the PSA cutsets). |  |
|  | Based on the uncertainty and sensitivity evaluations, an understanding has been gained of which parametric and modelling uncertainties most contribute to the overall uncertainty of the results of the Level 1 PSA. This analysis is transparent.  The results of the uncertainty and sensitivity evaluations demonstrate that the overall conclusions obtained from the Level 1 PSA are still valid.  Steps have been taken to reduce the most important uncertainties (and hence the uncertainties in the overall PSA results). These are explicitly described. |  |
| Table A1-2.9.2 Quantification of the Level 1 PSA | | |
|  | The results obtained from the quantification are reproducible:   * The type of quantification and related approximations are explicitly stated. * The cut-offs used for the quantification are explicitly stated and adequate. * Any minimal cutset editing performed is transparent. * A description of the way in which circular logic has been removed between front line / support and support / support system fault trees if done within the quantification process is provided. |  |
|  | Complete results of the quantification are provided. These include:   * Minimal cutsets with numerical results and description of the basic events. * Lists of basic events and associated importance measures, as a minimum fractional contributions (Fussell Vesely Importance) and risk increase factors (Risk Achievement Worth). * Lists of relevant groups of components or basic events and associated importance functions as for basic events. |  |
|  | Quantification has been carried out (and results provided) at different levels:   * Level 1 PSA (for full power operation). * Level 1 PSA (for operation at low power and shutdown). * Individual initiating event groups (event trees). * Individual accident sequences (in the event trees). * Individual hazards for power operation and non-power conditions. * Individual hazard scenarios for power operation and non-power conditions. * Total annual contribution from all NPP operations (power and non-power) for all internal initiators and hazards and the breakdown of this for the different operational states. * The estimated level of risk associated with each operational state in order to support the ALARP arguments. |  |
|  | A survey of the PSA results has been carried out by the dutyholder to confirm the correctness of the Level 1 PSA quantification. |  |
| Table A1-2.9.3 Presentation and Interpretation of the Level 1 PSA Results | | |
|  | A summary of the Level 1 PSA results is included in the PSA documentation.  The summary of the Level 1 PSA results together with any accompanying discussions are sufficient for PSA and non-PSA specialists to get a clear understanding of how big the risk of core damage is, where this risk comes from and which are the most significant uncertainties. |  |
|  | All vulnerabilities identified by the PSA are transparent. The corrective actions proposed to address these vulnerabilities are described explicitly. The PSA has been used to support the optioneering analysis and details of this are auditable.  An evaluation of the risk improvements expected from the proposed corrective actions is documented explicitly. This has been used as an input to assigning the level of priority of these proposals.  A formal process is in place to ensure that the proposed corrective actions are captured, as appropriate, in the NPP design or design modification processes, in the NPP process for procedure development or modification, etc. |  |
|  | A demonstration is included that the risk of core damage for the facility under evaluation is ALARP. |  |
| **Table A1-3. Level 2 PSA** | | |
|  | The basis for the definition of LARGE RELEASE is presented and explained. |  |
|  | The basis for the definition of LARGE EARLY RELEASE is presented and explained. |  |
|  | If a design target for LARGE RELEASE FREQUENCY has been used, this is stated explicitly. |  |
|  | If a design target for LARGE EARLY RELEASE FREQUENCY has been used, this is stated explicitly. |  |
|  | The Level 2 PSA has been designed so that its output forms an adequate input to perform a Level 3 PSA. |  |
| **Table A1-3.1 Interface between Level 1 and Level 2 PSA** | | |
|  | The entirety of the Level 1 PSA has been taken forward to the Level 2 analysis (Internal initiating events, internal and external hazards for the reactor at power, low power and shutdown, and for the fuel route) |  |
|  | The analysis of the interface between Level 1 and Level 2 PSA has addressed systematically all the attributes of the Level 1 core damage sequences that can affect the accident progression.  The analysis has identified all attributes of the Level 1 core damage sequences that can affect the mode and timing of containment failure, containment bypass or affect the source term. Steps have been taken to give confidence that a complete set of attributes has been identified, including as appropriate, the investigation of attributes identified in other studies and justifications for inclusion or exclusion of features are presented.  The analysis is performed in a way which, together with the Level 2 model and the mechanism for transferring information between the two parts of the analysis, ensures that all dependencies between Level 1 core damage sequences and the Level 2 model (including event logic, system-related and human error dependencies) truly represent the plant, operating rules, and operating procedures.  The analysis is transparent. |  |
|  | Based on the above, a complete set of Plant Damage States (PDS) is defined, each of which represents a set of core damage sequences with a unique expected severe accident progression and set of source term characteristics.  The characterisation of each PDSs is clearly presented in terms of the attributes of the Level 1 sequences it represents and the status of each of these attributes.  The identification and characterisation of PDSs is adequate.  A sufficient number of PDS has been defined to avoid masking important ways of accident progression while ensuring a manageable scope of analysis. |  |
|  | Any modification made to the original Level 1 PSA event trees to address Level 2 issues (features that can affect the accident progression but were not considered originally in the Level 1 PSA models), is clear.  The models truly represent the plant, operating rules, and operating procedures. |  |
|  | Relevant systems not already covered in the Level 1 PSA are analysed to the same specification and level of detail as the other systems included in the Level 1 PSA.  All the dependencies are properly captured. |  |
|  | Relevant human failure events not already covered in the Level 1 PSA are analysed to the same specification and level of detail as the HFEs included in the Level 1 PSA. |  |
|  | The criteria used to group the (Level 1 - Level 2 interface) event tree sequences into the defined PDSs are identified explicitly and correct.  The process of mapping the resulting accident sequences from the modified event trees to the relevant Pant Damage States is transparent.  If the binning process (allocation of sequences to end state categories) is automated, an auditable record exists of this process.  The identification and characterisation of PDSs is traceable in both directions, i.e. Level 1 cutset / sequence to PDS and PDS back to Level 1 sequence. No errors are identified in the grouping of accident sequences into the defined PDSs. |  |
|  | Each PDS has been assigned a frequency equal to the summed frequency of all the sequences in the group.  For the follow-up Level 2 analysis, each PDS is represented by the most onerous sequence. In general, if the PDS structure is a proper one, there should not be any significant differences in the sequences within a PDS, and therefore, the PDS representative sequence would be the one with the highest frequency. |  |
|  | If a separate code is used for Level 2 PSA, the way in which the sequence or cutset definitions and frequencies from the Level 1 – Level 2 interface have been transferred to the Level 2 PSA is transparent. |  |
| **Table A1-3.2 Deterministic Accident Progression Analysis** | | |
|  | The code/s used for analysing the progression of severe accidents has / have been qualified for the design of the NPP under evaluation. For example, the computer model has been successfully used to simulate steady state operating behaviour and a variety of initiating events (such as unanticipated transients). Alternatively, the code has been applied to experimental facilities or to other NPPs of similar design with equivalent fidelity.  The code and inputs meet ONR quality expectations (for example, as described in Table A1- 1.4 of this Appendix). The input data used by the code represents the facility in sufficient detail and with sufficient fidelity to provide the output required by the Level 2 PSA model.  The code/s used include deterministic models for all known severe accident phenomena that could occur with high probability and have a first-order impact on the response to the postulated fault.  The analytical models contained in the computer code have been sufficiently validated (both individually and collectively; i.e. against separate effects and integral experimental measurements) to provide reasonable confidence in the calculated results.  The codes have been used within their limit of applicability. |  |
|  | Modelling options (if any) selected by the code user reflect ‘best-practice’ recommendations of the code developers or a recognised and experienced user community.  Deviations from best-practice choices of options are documented and justified. |  |
|  | The modelling options available in the computer code are applied consistently throughout the calculations performed for different fault sequences.  Differences in the codes, models or modelling options used (if any) are documented and justified. |  |
|  | In cases where some of the severe accident phenomena have not been addressed directly via code calculations, the applicability of the sources of information used to address these phenomena is justified. |  |
|  | No relevant and potentially important phenomena have been neglected or dismissed without an adequate technical justification. |  |
|  | All the assumptions made are stated explicitly.  All the assumptions made are justified, i.e. the rationale for choosing these assumptions and for rejecting alternatives is clear and reasonable.  The way in which each assumption may bias the outcomes of the analysis is indicated, or the effect(s) of alternative, reasonable assumptions on the calculated results is demonstrated to be negligible. |  |
|  | The accident progression analyses have been performed on a best-estimate basis and are specific to the facility. |  |
|  | In the absence of facility-specific details, all the assumptions regarding facility design and construction are stated.  A process is in place to ensure that these assumptions are captured to support the future design and construction. |  |
|  | The accident scenarios selected as input to the accident progression calculations are appropriate and transparent throughout the various accident progression analyses.  The accident scenarios selected as input to the accident progression calculations are consistent with the Level 1 PDS sequences (which are the starting point for the accident scenarios evaluated) and with the Level 2 event tree sequences to which they are applied. |  |
|  | Assumptions made in the accident progression analyses regarding operator actions are consistent with the operator actions in the corresponding Level 2 PSA accident progression event tree sequences. |  |
|  | The accident progression analyses are documented and traceable. |  |
|  | The regulator may choose to review in depth a representative subset of the accident progression analyses. In these cases no significant errors have been found. |  |
|  | The regulator may choose to independently perform a representative subset of accident progression analyses. In these cases, the results obtained are consistent with those presented by the dutyholder. |  |
| **Table A1-3.3 Containment Performance Analysis** | | |
|  | The method used for analysing the probability of failure of the containment (i.e. the method used for analysing the containment structural response) under different stress conditions caused by the severe accidents is transparent.  The method is state-of-the-art and meets accepted industry standards. |  |
|  | The code and inputs used for analysing containment structural integrity meet ONR quality expectations as described in Table A1-1.4 of this Appendix.  The input data used by the code represents the facility in sufficient detail and with sufficient fidelity to provide the quality of output required by the Level 2 PSA model. |  |
|  | The models used to characterise the loss of containment integrity (for example, the models used for thresholds and / or leak before break) are explicitly stated and justified. |  |
|  | The way in which analysis of the failure of penetrations has been performed is transparent and adequate. |  |
|  | The loads and combinations of loads studied are clear.  The range of loads and combinations of loads addressed is adequate to represent the conditions of the severe accident sequences, which are possible for the facility under evaluation. Temperature effects are addressed and the assumptions made are consistent with the conditions arising in the accident sequences for which the results of the analysis are used. |  |
|  | In the absence of facility-specific details, all the assumptions regarding containment geometry, construction and materials are transparent.  A process is in place to ensure that these assumptions are captured to support the future design and construction. |  |
|  | The material properties assumed are realistic. |  |
|  | A systematic review of the containment structure has been performed to identify plausible and credible failure modes. |  |
|  | Failure criteria for containment structures are clearly defined. |  |
|  | Uncertainties associated with the capacity of the containment under extreme loads have been identified explicitly.  Uncertainties have been appropriately treated and the results of the analysis are presented in a form consistent with their use in the probabilistic accident progression models. ONR expectation is that the results of the structural analysis would be presented as probabilistic fragility curves, unless it has been justified that the uncertainties are small enough for the use of a bounding point-value structural capacity to be used. |  |
|  | Any expert judgement used to derive the containment capacity and uncertainty parameters has been documented.  The expert judgement process adopted is appropriate. |  |
|  | The containment performance analyses are thoroughly documented and fully traceable. |  |
| **Table A1-3.4 Probabilistic Modelling Framework – Accident Progression Event Trees (APET)** | | |
|  | The approach used for the delineation of the severe accident sequences (accident progression event trees, APETs, or equivalent) is transparent. That is, the chronological progression of events can be traced either via graphical diagrams or an equivalent method, and the logical end-states of individual accident sequences (for example, pathways through an event tree) are associated with a single, unique outcome (for example, a release category). |  |
|  | The Level 2 PSA code used to develop the APETs provides the necessary capability to support the modelling approach selected, for example, the capability to handle multiple branches for a single event tree node, headings represented by models other than fault trees (for example, event trees, user defined code), global variables (for example, to allow tracking of hydrogen generation and combustion at different points in an accident sequence), etc.  If the Level 2 PSA code does not provide the necessary capability to support all aspects of the probabilistic modelling approach selected, the way in which these aspects of the model have been handled in the quantification is clear. |  |
|  | An APET has been developed for each PDS. |  |
|  | The APETs are clearly described (i.e. structure and headings).  The phenomena addressed are clearly identified. All relevant phenomena significantly affecting the accident progression or source term magnitudes (as far as required to comply with table A1-3.5) have been included. The selection of phenomena for inclusion has followed a systematic process which addresses generic accident phenomena and specific plant issues, and no relevant phenomena have been neglected or dismissed without an adequate technical justification.  The time frames depicted are transparent and organised in the correct order with proper treatment of chronological dependencies.  When uncertainties are addressed via the APET structure, the way in which this has been done is transparent.  All assumptions are described and justified.  All simplifications (for example, issues excluded from the APET) are described and justified.  The dependencies between / among phenomena are explicitly identified and properly captured in the logic model and in the assignment of event probabilities.  Dependencies within the Level 1 core damage sequences are adequately modelled.  The structure of each APET, and associated event probabilities, are traceable to the underlying deterministic accident progressions analyses carried out to support their development. |  |
|  | The APET includes HFEs for severe accident management actions. Table A1-.2.5 of this appendix applies for the assessment of these actions.  The dependencies with the HFEs in the Level 1 PSA are identified and treated appropriately.  Potential adverse effects of severe accident management actions are modelled. |  |
|  | The method used to assign probabilities to the events of the APET is described. The approach selected is valid and is used to assign probabilities consistently throughout the Level 2 PSA. In particular:   * Event probabilities which represent random events (i.e. events representing aleatory or stochastic uncertainty, such as those similar to the ones included in the Level 1 PSA models, e.g., equipment random failures) are calculated using methods consistent with similar events in the Level 1 PSA. * Event probabilities which represent uncertainty about deterministic outcomes (i.e. events representing so-called epistemic uncertainty, such as the likelihood of structural failure due to temperature and pressure loads from an energetic event) are assigned based on a clear and consistent method. If expert judgment is used to assign event probabilities, the rationale for numerical values chosen is clearly described and applied consistently throughout the Level 2 PSA. |  |
|  | In cases where APET probability values represent uncertainty about deterministic outcomes, the analyses performed to generate have:   * Identified the relevance of the defined severe accident time frames and has taken this into account adequately * Used up-to-date information on accident phenomenology. * Justified the applicability of the sources of information used. * Used facility-specific information wherever possible. * Used an acceptable analysis method - for example, decomposition event trees, Monte Carlo simulation, or another method justified as adequate. * Been performed in a transparent and consistent manner. |  |
|  | APET drawings are included.  Computer files for the APETs are provided. |  |
|  | System design, operability and survivability modelling is described clearly and justified.  In cases where the environment or operating conditions for system(s) exceed their design or qualification limits, assumptions on system design, operability and survivability are explicitly stated.  A process is in place to ensure that these assumptions are captured to support the future system design, installation and qualification. |  |
| **Table A1-3.5 Source Term Analysis** | | |
|  | The parameters that influence fission product release, retention and transport through each of the major barriers to the environment are identified explicitly.  The attributes that define the characteristics of the radiological releases and potential off-site consequences are identified explicitly.  The attributes required in order to perform a Level 3 PSA are identified explicitly, for example, magnitude of radionuclides, isotopic composition, release timing, height of the release, physical and chemical characteristics of the release, heat content of the release (plume), etc. |  |
|  | Based on the above, an adequate set of release categories (RCs) has been defined and justified, each one representing a different way of radiological release.  The release duration and release profile considered and the rationale for their choice are transparent and adequate.  The characterisation of each RC is clear. All the attributes relevant to each RC are identified explicitly.  The identification and characterisation of RCs is adequate.  A sufficient number of RCs has been defined to avoid masking important source terms while maintaining a manageable scope for the analysis. |  |
|  | The method or criteria used to group the severe accident sequences from the APETs into the defined RCs is stated explicitly and is justified.  The process of mapping the resulting severe accident sequences from the APETs to the relevant RCs is transparent.  If the binning process (allocation of sequences to end state categories) is automated, an auditable record exists of this process.  No errors are identified in the grouping of severe accident sequences into the defined RCs. |  |
|  | Each RC has been assigned a frequency equal to the summed frequency of all the severe accident sequences in the group.  Each RC provides an adequate representation of the individual sequences within the group. |  |
|  | The code and inputs meet ONR quality expectations as described in Table A1-1.4 of this Appendix. |  |
|  | The modelling method/s used to perform source term analysis are clear.  The radionuclide grouping scheme used for the source term analysis is consistent with current state-of-the-art practice.  All the assumptions made to obtain source terms are described and justified.  The computer code calculations used as the basis for estimating facility-specific source terms for selected accident sequences are documented.  If there are cases where facility-specific computer code calculations were not performed, the method by which source terms have been estimated is described and justified. Also the relationship between the deterministic accident progression analyses and deterministic source term analyses are clearly described and justified. |  |
|  | A set of sensitivity analyses has been performed to explore the impact of the assumptions made in the source terms analysis. |  |
|  | The source term analyses are thoroughly documented and fully traceable. |  |
|  | The regulator may choose to review in depth a representative subset of the source term analyses. In these cases no significant errors have been found. |  |
|  | The regulator may choose to independently perform a representative subset of source term analyses. In these cases, the results obtained are consistent with those presented by the dutyholder. |  |
| **Table A1-3.6 Quantification of the Level 2 PSA** | | |
|  | The quantification process is adequately documented and reproducible.  The quantification setup, settings and any approximations are adequately documented. The quantification results are reproducible.  Any cut-offs used for the quantification are documented and adequate.  Any minimal cutset editing or other post-processing performed is transparent and reproducible.  To the extent relevant, descriptions are provided of the way in which circular logic has been removed for any systems modified or developed for the Level 2 PSA. |  |
|  | Complete results of the quantification are provided, including:   * Minimal cutsets with numerical results and description of the basic events. * Basic event importance measures. * Importances for relevant groups of components or basic events. * Contribution of significant accident sequences to the Release Categories and risk metrics. |  |
|  | Results are summarised at different levels (to the extent consistent with the scope of the PSA):   * Full power operation * Low power and shutdown * Individual initiating event groups * Hazards during power operation and non-power conditions * Plant operational states * Point in time risk for each operational state (to support ALARP) |  |
|  | A review of results has been carried out to confirm their correctness.  A review of why the risk profile is similar or different to that of similar plants has been performed, to the extent practicable given the availability of results for similar plants. |  |
|  | The treatment of success branches is sufficiently accurate and the approach taken is justified, especially for headings where failure probabilities are large. |  |
|  | The summated total RC frequency (including RCs with minimal or no release) has been compared to the Level 1 CDF. A justification is provided that the magnitude of any differences is acceptable. Any significant differences are explained. |  |
|  | Uncertainties are propagated to generate uncertainty bounds on the RC results and on the values of the risk metrics generated.  Uncertainty propagation includes both Level 1 and Level 2 uncertainties.  The Level 2 and Level 1 models may use event probabilities which represent random events (sometimes referred to as aleatory events) and event probabilities that represent uncertainties about deterministic outcomes (sometimes referred to as epistemic events). The distinction between these types of events is recognised in the uncertainty propagation and uncertainty distributions are assigned following a method that is appropriate to the type of event.  For aleatory events, the method used to generate uncertainty distributions is consistent with the methods applied in the Level 1. Deviations from or inconsistencies with the Level 1 methodology are described and justified.  For epistemic events, the method used to generate uncertainty distributions used in for the uncertainty propagation takes account of the uncertainty information and modelling used to generate the mean values for those events. The assigned distribution is consistent with that modelling. 1/0 (or double delta) sampling (for binary or multiple branchings) is used where appropriate; otherwise the approach used is explained, justified and mathematically sound.  Where different events modelled in the Level 2 PSA depend on shared or similar parameters, the effect of the correlation introduced by these parameters is modelled unless a justification is provided that the correlation is not significant or is adequately bounded. If the latter bounding approach is used, a justification is provided that the realism of the overall models is not compromised. |  |
| **Table A1-3.7 Presentation and Interpretation of the Level 2 PSA Results** | | |
|  | The Level 2 PSA results are clearly and thoroughly presented in the PSA documentation.  The results of the uncertainty and sensitivity evaluations provide a high degree of confidence that the overall conclusions obtained from the Level 2 PSA are valid.  A summary of the Level 2 PSA results together with accompanying discussions is included. This summary is sufficient for PSA and non-PSA specialists to get a clear understanding of the risk of the defined categories of radioactive releases, where this risk comes from and which are the most significant uncertainties. A clear explanation is included of why the results of the Level 2 PSA are considered valid despite the identified uncertainties. |  |
|  | All vulnerabilities identified by the Level 2 PSA are documented explicitly. The corrective actions proposed to address the vulnerabilities are clear.  An evaluation of the risk improvements expected from the proposed corrective actions has been carried out and is documented explicitly. This has been used as the basis for assigning a level of priority to these proposals.  A formal process is in place to ensure that the proposed corrective actions are captured, as appropriate, in the NPP design or design modification processes, or in the NPP process for procedure development or modification, etc. |  |
|  | A demonstration that the risk of radioactive release for the NPP is ALARP is included. |  |
| **Table A1-4. Level 3 PSA** | | |
| **Table A1-4.1 Assessment of the Level 3 analysis** | | |
|  | The interfaces between the output of the Level 2 PSA and the input to the Level 3 PSA (approach and code/s used) are consistent. |  |
|  | The end-point(s) of the Level 3 PSA are unambiguously stated and the scope is clearly defined.  The range of consequences addressed by the Level 3 PSA and the way in which these consequences are to be presented are identified. These are adequate to allow comparison against the relevant targets in the SAPs |  |
|  | The calculation methods used in the Level 3 PSA are auditable and reflect the current state of knowledge. These include:   * The method(s) used to address the relevant phenomena and pathways, for example, for calculation of atmospheric dispersion, surface deposition, re-suspension, migration through food chains, etc. * The method(s) used for the calculation of dose (external irradiation, irradiation from inhalation, irradiation from ingestion). * The method(s) used for the calculation of health effects (deterministic, stochastic somatic, stochastic hereditary). * The method(s) used for the calculation of the economic consequences to support ALARP justification. * The selection and justification of parameter values. |  |
|  | The sources of specific items of data needed to perform probabilistic consequence analysis (meteorological, population, agricultural production, land, food distribution data, etc) are auditable and valid.  The approach used for meteorological sampling is appropriate.  The data used is up-to-date.  The site-specific data used to perform the consequence calculations is auditable.  Assumptions made are justified. |  |
|  | The input information used in the Level 3 PSA calculations regarding countermeasures and protective actions is stated.  The countermeasure strategies modelled are either reasonable bounding assumed strategies (in which case the countermeasures are feasible and consistent with national requirements) or are based on the NPP’s existing emergency plan. |  |
|  | Where default data provided by the code is used, its applicability is justified explicitly.  The usage of default data is documented in an auditable fashion. |  |
|  | The method by which the full spectrum of severe accident source terms generated in the Level 2 PSA are linked to a limited number of actual consequences in the Level 3 PSA is documented and auditable. |  |
|  | The calculations performed are auditable. |  |
|  | The computational process used to integrate the entire PSA model (Level 1 through Level 3) is appropriate. |  |
|  | Sensitivity analyses have been performed and are documented. The sensitivity analyses capture key assumptions and combinations of assumptions.  Uncertainties associated with the input parameters have been quantified using an acceptable method.  Based on the uncertainty and sensitivity evaluations, an understanding has been gained of which parametric and modelling uncertainties contribute most to the overall uncertainty in the results of the Level 3 PSA. This analysis is documented.  The results of the uncertainty and sensitivity evaluations demonstrate that the overall conclusions obtained from the L3 PSA are still valid. |  |
|  | The regulator may choose to review in depth a representative subset of Level 3 calculations. In these cases no significant errors have been found. |  |
|  | The regulator may choose to independently perform a representative subset of Level 3 calculations. In these cases, the results obtained are consistent with those presented by the dutyholder. |  |
| **Table A1-4.2 Presentation and Interpretation of the Level 3 PSA Results** | | |
|  | The Level 3 PSA results are clearly presented in the PSA documentation.  A summary of the Level 3 PSA results together with accompanying discussions is included. This summary is sufficient for PSA and non-PSA specialists to get a clear understanding of the risk of various types of consequences, where this risk comes from and which are the most significant uncertainties. A clear explanation is included of why the results of the Level 3 PSA are considered valid despite the identified uncertainties. |  |
|  | All issues or vulnerabilities identified by the Level 3 PSA are documented explicitly. The corrective actions proposed to address the vulnerabilities are clear.  An evaluation of the risk improvements expected from the proposed corrective actions has been carried out and is documented explicitly. This has been used as the basis for assigning a level of priority to these proposals.  A formal process is in place to ensure that the proposed corrective actions are captured, as appropriate, in the emergency procedures and arrangements |  |
|  | A demonstration that the individual and societal risks from the facility under evaluation are ALARP is included. |  |
| **Table A1-5 Overall Conclusions from the PSA** | | |
|  | The PSA is documented thoroughly. The PSA documentation enables the event and fault tree model, assumptions and quantification results to be traceable to the design documentation, drawings, analyses, operating procedures, and any other supporting information. |  |
|  | All aspects of the PSA have been subject to sufficient level of independent review by the dutyholder to provide confidence in its technical adequacy. These reviews are documented. |  |
|  | The PSA has a credible and defensible basis. |  |
|  | The PSA reflects the design of the NPP at the freeze date. |  |
|  | The PSA reflects the operation of the NPP up to the freeze date. |  |
|  | A process is in place to ensure that the assumptions regarding design and operation of the facility reflected in the PSA are captured in the development of future procedures, policies and strategies, design, design modifications and back-fits, etc. |  |
|  | The PSA is fully accepted by the NPP operator. |  |
|  | A process is in place to keep the PSA living, i.e. to be updated as necessary (at least every three years) to reflect the current design and operational features / practices and to incorporate feedback from internal and external operational experience, improved understanding of physical processes or accident progression and advances in modelling techniques. |  |
|  | The PSA has enabled a judgement to be made as to the acceptability of the overall risk of the facility against the SAPs numerical targets, and in particular targets 7 (individual risk) and 9 (societal risk). |  |
|  | The PSA has demonstrated that a balanced design has been achieved, such that no particular class of accident or feature of the facility makes a disproportionate contribution to the overall risk. |  |
|  | The PSA has been used effectively to demonstrate that the risk associated with the design and operation of the NPP is ALARP |  |
| **Table A1-6. Use of PSA to Support Decision-Making** | | |
|  | Note: This table is only generic. Detailed guidance on review of specific PSA applications is discussed in the TAG on Use of PSA and probabilistic insights [2] |  |
| **Table A1-6.1 Expected uses of PSA** | | |
|  | The PSA has been used to support the NPP design process. There is evidence that this has been done iteratively, i.e. that the PSA has been used to inform all the stages of the design. |  |
|  | The PSA has been used to support design modifications and back-fits, including the analyses of options considered during the preparatory stages of modifications projects. |  |
|  | The PSA has been used to provide an input to the development of, and changes to, operating rules / technical specifications and testing, inspection and maintenance schedules of the NPP. |  |
|  | The PSA has been used to provide an input to the optimal planning of testing, inspection and maintenance activities and to the daily management of plant configuration (i.e. when releasing plant for testing, inspection or maintenance). |  |
|  | The PSA has provided an input to the justification for any change to the way in which the facility is operated. |  |
|  | The PSA has been used to produce performance measures to demonstrate that the NPP is operated in such a way as to ensure that the numerical risk is kept ALARP. |  |
|  | The PSA is used to understand the risk significance of any abnormal occurrences at the NPP and to identify measures to avoid future re-occurrences of safety significant events. |  |
|  | The PSA has been used to support and inform Periodic Safety Reviews of the Facility. |  |
|  | The PSA has been used to support development of, and changes to, operating procedures for managing all stages of incidents and accidents (including severe accidents). |  |
|  | The PSA has been used to provide an input to the design of, and changes to, operator-training programmes for management of incidents and accidents (including severe accidents). |  |
|  | The results of the PSA have been used to provide an input for off-site emergency planning and response including a demonstration of the effectiveness of countermeasures. |  |
| **Table A1-6.2 Quality of the safety submissions supported by PSA** | | |
|  | The issue being evaluated using the PSA is explicitly defined.  The type of results required as input to the decision-making are identified up-front.  Any applicable numerical criteria are identified up-front.  (In general, the inspector should expect that the impact of the issue on the overall risk should have been addressed by evaluating the Core Damage Frequency, Large Release Frequency, and Societal Risk). |  |
|  | All aspects of the PSA model and data potentially affected by the issue under study are identified explicitly. |  |
|  | All aspects of the PSA model and data identified as being potentially affected by the issue under study have been analysed for impact and modified if necessary. The analysis is transparent. The modifications are adequate. |  |
|  | All the assumptions in the PSA have been checked for validity against the issue under study and modified if appropriate. The analysis is documented explicitly. |  |
|  | Sensitivity analyses have been carried out to evaluate the sensitivity of the risk to changes in relevant assumptions and areas of modelling uncertainty. The analyses are documented explicitly. |  |
|  | Sensitivity analyses have been carried out to check the risk impact of different options under consideration. The analyses are documented explicitly. |  |
|  | Sensitivity analyses have been performed to address ‘what if’ scenarios. The analyses are documented explicitly. |  |
|  | The results of the sensitivity analyses have been used to inform the final decision. The way in which the final decision has been informed by the results of the sensitivity analyses is transparent. |  |
|  | Uncertainties in input probability and frequency values have been estimated and propagated through the models to generate uncertainty distributions on the resulting risk figures.  The means resulting from the uncertainty propagation have been compared against the numerical criteria relevant to the application (rather than using the point estimate means which result from a simple arithmetic evaluation of the PSA cutsets). |  |
|  | Based on the results of the sensitivity and uncertainty analyses, it has been shown that the most important modelling and parametric uncertainties have been minimised, or that the results of the application are not affected by these uncertainties, or that the decision based on the results of the application takes account of the uncertainties by application of the precautionary principle (as described in R2P2). Details of this are documented explicitly. |  |
|  | If the issue under study affects aspects of the risk not covered within the scope of the existing PSA. These limitations in the PSA in relation to the issue under evaluation have been recognised and identified explicitly.  In such cases, the PSA models have been adequately extended and / or enhanced to cover the missing aspects. The new models and data are adequate.  If extending the PSA is considered not to be practicable (for example, due to time constraints), the risk impact of the issue associated with areas outside the scope of the existing PSA has been analysed qualitatively. The analysis of this is transparent and adequate. |  |
|  | The outcome of the PSA studies performed to evaluate issues is clear, comprehensive and traceable.  The outcome of the PSA studies performed to evaluate issues includes the following:   * A description of the issue under study. * A description of the PSA evaluations undertaken including any numerical criteria established. * A description of the new (or modified) assumptions. * A description of the modifications to models and data and relevant drawings. * The identification of key areas of uncertainty in relation to the issue. * Relevant numerical results. * Lists of cutsets and importance measures. * Risk profile (identification of dominant initiating events, accident sequences, and protection failures). * Results of the sensitivity and uncertainty analyses and conclusions obtained from these. * Qualitative risk arguments used. * A clear interpretation of all the information above and unambiguous recommendations based on a systematic application of decision-making criteria applied to the results of the PSA evaluations. |  |

# Appendix 2 – Mapping between Issue O of the WENRA Reference Levels and this TAG

| WENRA RLs (Issue O) [9] | Section(s) of this TAG | Comments |
| --- | --- | --- |
| **1. Scope and content of PSA** | | |
| 1.1 For each plant design, a specific PSA shall be developed for level 1 and level 2, considering all relevant58 operational states, covering fuel in the core and in the spent fuel storage and all relevant internal and external initiating events. External hazards shall be included in the PSA for level 1 and level 2 as far as practicable, taking into account the current state of science and technology. If not practicable, other justified methodologies shall be used to evaluate the contribution of external hazards to the overall risk profile of the plant. | Section 4.5 describes SAP FA.12 on scope and extend of PSA  Advice to inspectors is provided in: Section 5.2 on Scope Section 5.3 on General Aspects of PSA  Note: a Level 3 PSA is required to address some of the numerical targets of the SAPs | Specific, detailed requirements to address scope and level in PSAs for NPPs are spread throughout Appendix 1, for example, Tables A1-1.2, A1-2.1, A1-2.7.1, A1-2.8 and A1-5 (paragraph starting The PSA has enabled…) |
| 1.2 PSA shall include relevant dependencies. | Section 5.5 PSA Model  Section 5.6 Protection and Mitigation systems modelling  Section 5.7 Accident Sequence Analysis  Section 5.8 Digital Control Instrumentation in PSA  Section 5.19 Multi-unit and site-level considerations | Specific requirements to address dependencies in PSAs for NPPs are spread throughout Appendix 1, for example, Table A1-2.3.2 (paragraph starting “All dependencies…”, Table A1-2.4.1 paragraph starting “The general approach for the inclusion on (hardware/software) common cause failure events…”. Table A1-2.4.2 paragraph starting “The information on dependencies…” and paragraph starting “all intra-system and inter system common cause failures…) |
| 1.3 The Level 1 PSA shall contain sensitivity and uncertainty analyses. The Level 2 PSA shall contain sensitivity analyses and, as appropriate, uncertainty analyses. | Section 4.13 on AV.6 sensitivity analysis Section 5.3 on General Aspects of PSA  Section 5.8 Digital Control Instrumentation in PSA  Section 5.10 Human Reliability Analysis  Section 5.17 sensitivity and Uncertainty Studies  Section 5.19 Multi-unit and site-level considerations | Specific requirements to perform sensitivity and uncertainty analyses in PSAs for NPPs are spread throughout Appendix 1, for example, Table A1-2.9.1, and Table A1-3.6. See also Tables A1-3.i for expectations on sensitivity and uncertainty analyses in the Level 2 PSA |
| 1.4 PSA shall be based on a realistic modelling of plant response, using data relevant for the design, and taking into account human action to the extent assumed in operating and accident procedures. The mission times in the PSA shall be justified. | Section 4.6 describes SAP FA.13 on Adequate representation of plant  Section 5.3 on General Aspects of PSA  Section 5.5 PSA Model | Specific requirements to ensure that in PSAs for NPPs the models and data are realistic are spread throughout Appendix 1, for example, Table A1-2.2 and A1-2.6. Table A1-2.3.2 includes specific expectations for mission times (as does SAP para 652) |
| 1.5 Human reliability analysis shall be performed, taking into account the factors which can influence the performance of the operators in all plant states | Section 5.10 Human Reliability Analysis | Specific requirements for the Human Reliability Analysis in PSAs for NPPs are included in Table A1-2.5 |
| **2. Quality of PSA** | | |
| 2.1 PSA shall be performed, documented, and maintained according to the quality management system of the licensee. | Sections 5.3, 5.8 address the various aspects and expectations of maintaining quality of PSA | LC 17 requires an appropriate licensee QA system |
| 2.2 PSA shall be performed according to an up to date proven methodology, taking into account international experience currently available. | Section 5.3 on General aspects of PSA | The TAG taken as a whole will ensure that the PSA is performed according to an up to date proven methodology. A large amount of International experience is embodied in the TAG (see A1-4 and A1-5) |
| **3. Use of PSA** | | |
| 3.1 PSA shall be used to support safety management. The role of PSA in the decision making process shall be defined. | Section 4.7 of FA.14 on Use of PSA.  Additional guidance on the topic could be found in the TAG on 'Use of PSA and Probabilistic Insights' [2] |  |
| 3.2 PSA shall be used to identify the need for modifications to the plant and its procedures, including for severe measures, in order to reduce the risk from the plant. | Section 4.7 of FA.14 on Use of PSA.  Additional guidance on the topic could be found in the TAG on 'Use of PSA and Probabilistic Insights' [2] | Specific expectations are included in Table A1-2.9.3, A1-3.6, and A1-6.1. |
| 3.3 PSA shall be used to assess the overall risk from the plant, to demonstrate that a balanced design has been achieved, and to provide confidence that there are no "cliff-edge effects". | Section 5.14 on quantification of analysis see also SAP FA.25 and paras 676 and 677 for “cliff edge effects” | Appendix 1 Table A1-5 |
| 3.4 PSA shall be used to assess the adequacy of plant modifications, changes to operational limits and conditions and procedures and to assess the significance of operational occurrences. | Section 4.4 on FA.11 – PSA Validity |  |
| 3.5 Insights from PSA shall be used as input to development and validation of the safety significant training programmes of the licensee, including simulator training of control room operators. | Section 4.7 of FA.14 on Use of PSA. |  |
| 3.6 The results of PSA shall be used to ensure that the items are included in the verification and test programmes if they contribute significantly to risk. | Section 4.7 of FA.14 on Use of PSA. |  |
| **4. Demands and conditions on the use of PSA** | | |
| 4.1 The limitations of PSA shall be understood, recognized and taken into account in all its use. The adequacy of a particular PSA application shall always be checked with respect to these limitations. | Section 4.7 of FA.14 on Use of PSA. |  |
| 4.2 When PSA is used, for evaluating or changing the requirements on periodic testing and allowed outage time for a system or a component, all relevant items, including states of systems and components and safety functions they participate in, shall be included in the analysis. | Section 4.7 of FA.14 on Use of PSA. |  |
| 4.3 The operability of components that have been found by PSA to be important to safety shall be ensured and their role shall be recorded in the SAR. | Section 4.4 on FA.11 – PSA Validity |  |

1. Hardware reliability is normally characterised numerically as probability of failure (for example, PFD or Failure Rate) depending upon the mode (i.e. demand (low or high) or continuous) of a C&I systems operation. [↑](#footnote-ref-2)