

## Technical Assessment Guide

# Probabilistic Safety Analysis

### T/AST/030 – Issue 03

Comments on this guide, and suggestions for future revisions, should be made and recorded in accordance with ND's standard procedures. Comments made from outside ND should be sent via [ndenquiries@hse.gsi.gov.uk](mailto:ndenquiries@hse.gsi.gov.uk).

- [1 Purpose and scope](#)
- [2 Relationship to licence and other relevant legislation](#)
- [3 SAPs addressed and relationship with WENRA Reference Levels and IAEA Standards](#)
- [4 Advice to inspectors](#)
- [5 References \(General\)](#)
- [6 References \(Technical Assessment Guides, TAGs\)](#)
- [7 Bibliography](#)
- [Appendix 1 - T/AST/030 – Assessment Expectations for Review of PSAs for Nuclear Power Plants](#)
- [Appendix 2 – T/AST/030 – Mapping between Issue O \(Probabilistic Safety Analysis\) of the WENRA Reference Levels and the Requirements of this TAG](#)

## 1 Purpose and scope

1.1 The purpose of this technical assessment guide is to provide an interpretation of those Safety Assessment Principles ([Ref 5.1](#)) related to PSA and to provide specific guidance to inspectors engaged in the assessment of PSAs and PSA related submissions (from Licensees, Licence Applicants or Generic Design Assessment (GDA) Requesting Parties. All these are referred to as duty-holders in this TAG).

1.2 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 Nuclear Power Plants (NPPs) is provided in [Appendix 1](#).

1.3 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](#).

1.4 This TAG does not provide detailed information on how to judge the technical adequacy of the various PSA aspects assessed. The reviewers should use their own knowledge and experience for this. However, aid can be sought in the publications listed in Sections 5, 6, 7 and in [Appendix 1](#).

<b>Issue Date:</b> 2009/02/16	<b>Open Government Status:</b> Fully Open
<b>Review Date:</b> 2013/02/16	<b>Approved by:</b> R.Jennings

1.5 It is not the intention of this guide to prescribe specific methods and approaches for conducting PSA. Duty-holders may choose to use alternative methods to those covered by this TAG (and in particular its [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.

1.6 In addition, it should be noted that PSA covers a whole range of disciplines and, therefore, PSA assessment requires involvement of 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 and radiation safety. On the other hand, individual assessments of said areas of the safety case can benefit from, and should take advantage of, the insights the PSA provides on the relative importance of issues addressed in those technical areas.

1.7 Inspectors must be able to form an opinion on whether risks are ALARP and it is not unreasonable to expect numerical input to the demonstration that the risk is ALARP. T/AST/051 ([Ref 6.10](#)) provides further guidance on the role of PSA within safety cases and T/AST/005 ([Ref 6.1](#)) provides further guidance on the role of PSA in the demonstration of ALARP.

1.8 Although this TAG does not specifically cover the risk to persons on-site from nuclear accidents, it provides sufficient information to help inspectors assessing this particular aspect of the safety case provided by the duty-holders in order to address the Numerical Targets 5 and 6 of the SAPs. Development of more detailed guidance to explicitly cover worker risk may be considered for a future update of this TAG.

## **2 Relationship to licence and other relevant legislation**

2.1 The site licence conditions 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 licence conditions (LCs) relevant to PSA are LC14, LC23, LC27 and LC28.

2.2 LC14 requires the licensee to make and implement adequate arrangements for the production and assessment of safety cases. Normally, the licensee's safety case will need to contain PSA as well as deterministic analysis.

2.3 LC23 requires that the safety case identifies the conditions and limits necessary in the interest of safety and it is NII's expectation that both the probabilistic (PSA) and the deterministic aspects of the safety case will contribute to this process. Similarly, NII expects that PSA will contribute to the identification of suitable and sufficient safety mechanisms, devices and circuits, as required by LC27 and provide a significant input for LC28 in identifying plant that may affect safety for which regular, systematic examination, inspection, maintenance and testing will be required.

2.4 LC15 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 existing and comparison with relevant good practice dictates this) and using it to support the arguments for continuing operation during the period until the next review.

2.5 In addition to these principal licence conditions, LC6 requires that adequate records be made and maintained. In this regard, it is NII's expectation that licensees will establish Living PSA programmes and that, in the framework of these programmes, all relevant files and records will be maintained for the life of the facility. Also, LC 17 sets out the requirement for quality assurance (QA) arrangements for all matters that affect safety. In this respect Licensees are expected to establish an adequate QA process that is effectively applied during all phases of the PSA and its application.

2.6 Safety cases, including PSA, may be produced to support activities such as construction of new facilities, commissioning, modifications and decommissioning. These activities, covered by licence conditions 19, 20, 21, 22 and 35, require safety documentation.

### **3 SAPs addressed and relationship with WENRA Reference Levels and IAEA Standards**

#### **3.1 Introduction**

This guide interprets NII's use of the PSA related safety assessment principles as set out in HSE's SAPs (Ref 5.1) FA.10 to FA.14. This guide also addresses those aspects of the principles on 'assurance of validity', FA.17 to FA.24, that are specifically applicable to PSA. Regarding the Numerical Targets of the SAPs (which were addressed in the previous version of this TAG), the 2006 version of the SAPs has expanded considerably all the explanations that accompany the Targets and additional explanations are included in the document entitled "[Numerical Targets and Legal Limits in Safety Assessment Principles for Nuclear Facilities – An Explanatory Note](#)". Therefore guidance related to the application of the numerical targets of the SAPs is not repeated here.

#### **3.2 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”**

This principle sets the framework and requirements for a PSA study. The overriding aim of the PSA assessment is to assist NII judgements on the safety of the facility and whether the risks of its operation are being made as low as reasonably practicable.

This TAG (in particular, Sections 3.5, 4 and [Appendix 1](#)) provides guidance which will enable inspectors to judge that the above expectation for a suitable and sufficient PSA has been met by the duty-holders.

A suitable and sufficient PSA should:

- 1) Enable a judgement to be made as to the acceptability of the overall risk of the facility against the numerical targets of the SAPs.
- 2) Demonstrate that a balanced design has been achieved, such that no particular class of accident or feature of the facility makes a disproportionate (eg, of the order of one tenth or greater) contribution to the risk target of concern.
- 3) Be used to help demonstrate that the risks associated with the design and operation of the facility, as well as changes in risk associated with any modification to plant or operation, are and will remain ALARP.

The depth of the PSA for a given facility may vary depending on the magnitude of the radiological hazard and risks and the complexity of the facility. For example, for some facilities simplified analyses, or even qualitative arguments, application of good practice and DBA may be sufficient to demonstrate that the risk is ALARP. However, for complex facilities such as power reactors or reprocessing facilities, comprehensive PSAs that meet modern standards should be developed for all types of initiating faults and all operational modes.

It is relevant to stress that NII expects ALARP to be integral to all considerations of a facility and site whether new or existing, i.e. it is not a process to be carried out only after a design is completed.

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

**“PSA should reflect the current design and operation of the facility or site”**

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.

In addition, in order to meet this principle, the PSA should be kept living, ie, it should be updated 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.

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

**“PSA should cover all significant sources of radioactivity and all types of initiating faults identified at the facility or site”**

In order to meet this principle the scope of the PSA should cover all sources of radioactivity at the facility (eg, fuel ponds, fuel handling facilities, waste storage tanks, radioactive sources, reactor core, etc), all types of initiating faults (eg, internal faults, internal hazards, external hazards) and all operational modes (eg, nominal full

power/throughput, low power/throughput, shutdown, start-up, refuelling, maintenance outages).

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

**“The PSA model should provide an adequate representation of the site and its facilities”**

#### 1) General

The aim of this principle is to ensure the technical adequacy of the PSA. 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.

Starting from the list of initiating faults from SAP FA.2 (Identification of Initiating Faults), the PSA should identify systematically and comprehensively the complete range of sequences leading to the “undesired” consequences that may occur. This makes no distinction in regard to 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.

In order to address the relevant numerical targets of the SAPs, the PSA needs to have regard to accidents with severe consequences and to those that have a higher frequency but lower radiological consequence.

#### 2) PSA Models

PSA should account for all contributions to the risk, including, but not necessarily restricted to: random component individual failures, components which are failed by the initiating fault, common cause failures (and, as necessary, other dependent and consequential failures), unavailabilities due to testing and maintenance, pre-initiating fault human errors (eg, misalignments and mis-calibrations), human errors that lead to initiating faults 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.

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. Model simplifications (eg, 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.

The frequency of occurrence and consequences of each of the fault sequences identified should be estimated. Sequences should not be discounted solely on the basis that their individual frequency is low, since the total contribution from all low frequency sequences may be significant in respect to the numerical targets of the SAPs.

Where groups are used to represent several initiating faults or accident sequences, the group should be assigned a frequency equal to the summed frequency of all the contributors in the group and should be represented by the most onerous one (ie, the initiating fault which is bounding in terms of impacts or the sequence which is bounding in terms of consequences). Thus, such simplifications are always conservative. Care needs to be taken to avoid gross conservatism, since it could affect the conclusions drawn from the analysis, and could severely limit the usefulness of the PSA to support decision-making.

Best-estimate methods and data should be used 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, reasonably conservative assumptions should be made and the sensitivity of the risk to these assumptions should be established. The term “best-estimate” is defined in the SAPs Glossary ([Ref 5.1](#)).

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 the 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 by the use of this type of analysis.

### 3) PSA Data

Facility specific data should be used, to the extent possible, for the calculation of the frequencies and probabilities used in PSA.

Where facility 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.

Where facility specific data is not sufficient it should be combined with applicable generic data using a justified mathematical technique, such as Bayesian update of generic data with facility-specific data (as described, for example, in [Refs 5.2](#) and [5.3](#)).

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.

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:

- i. Probability data for personnel errors should take account of the specific task demands, psychological influences (eg 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. T/AST/012 ([Ref 6.3](#)) discusses the subject of Task Analysis which is judged a necessary precursor to any quantification.
- ii. The approach selected for the Common Cause Failure (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. T/AST/036 ([Ref 6.6](#)) provides guidance on the assessment of dependent failures, in particular CCFs.
- iii. 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 (eg 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, the codes should be state of the art and should have been validated 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. T/AST/016 ([Ref 6.4](#)) and T/AST/017 ([Ref 6.5](#)) provide guidance on the assessment of integrity of structural components.
- iv. The methodology used for the estimation of probabilities of failure of computer-based systems should meet industry accepted practices. The analysis of the software reliability should identify and take into account the influencing factors that affect the quality of the software. If the software system has been separated into parts that are treated individually in the reliability analysis, the dependencies between the various parts should be addressed explicitly. Any self-checking facilities built in the system should be taken into account in an adequate manner. The dependencies between diverse software systems should be dealt with explicitly. T/AST/046 ([Ref 6.8](#)) provides additional guidance on the assessment of reliability of computer based systems.

v. Assumptions on reliability of passive features or passive systems should be substantiated by suitable analysis covering the full range of accident conditions for which they are required and by extensive tests.

vi. Analyses to estimate the probability of occurrence of phenomena (for example in the severe accident portion of the 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.

#### 4) PSA Results

The results of the PSA should be comprehensively documented and properly interpreted. The numerical results of the PSA should always be presented together with list/s of minimal cutsets and the list of basic events and associated importance measures (as a minimum Fractional Contributions or Fussell Vesely Importance and Risk Increase factors or Risk Achievement Worth). It should be noted that the importance measures, in themselves, represent sensitivities of the results of the PSA to the inputs and, therefore, the duty-holders should provide justification of whether any high values shown are acceptable and nothing reasonable can be done to reduce unduly high risk contributions.

In all aspects of the analysis where assumptions have been made about how the plant and the operating staff behave, these and their justification should be clearly described. The sensitivity of the results of the PSA to changes in assumptions should be evaluated and clearly documented.

Uncertainty on input probability and frequency values should be estimated and propagated through the models to generate uncertainty distributions on the resulting frequencies or probabilities of undesired events. The means of these distributions should be compared against the numerical targets in the SAPs.

Based on the importance, sensitivity and uncertainty evaluations, the duty-holder should gain an understanding of which parametric and modelling uncertainties contribute most to the overall uncertainty in the probabilities or frequencies of undesired events and should, subject to reasonable practicability, take steps to reduce such uncertainties.

Ultimately, the results of the uncertainty and sensitivity evaluations should provide confidence that the overall conclusions obtained from the PSA are still valid.

### **3.6 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”**

The aim of this principle is to establish the expectations on what uses the duty-holders should make of the PSA to support decision-making and on how the supporting analyses should be undertaken.

## 1) Uses of PSA

The PSA should provide information for, and receive information from, the facility designers and operators so that consistency is achieved between the PSA and the design and operation of the facility. Following such an approach allows the PSA to be a powerful tool to aid decision making. Inspectors should expect the PSA to provide an input to the following:

- i. Initial design and design modifications and back-fits during the life of the facility. NII expects the PSA to be integrated into the design process in an iterative manner, i.e. the PSA should be used all the stages of the design.
- ii. Support to the safety classification of structures, systems and components.
- iii. Development of, and changes to, operating limits and conditions and testing, inspection and maintenance schedules of the facility.
- iv. Testing, inspection and maintenance planning and daily management of plant configuration.
- v. Periodic system reviews and overall Periodic Safety Review of the Facility.
- vi. Justification for any change to the way in which the facility is operated.
- vii. Development of, and changes to, operating procedures for managing all stages of incidents and accidents.
- viii. Design of, and changes to, operator-training programmes for management of incidents and accidents.
- ix. Off-site emergency planning and response including a demonstration of the effectiveness of countermeasures.
- x. Evaluation of the risk significance of the abnormal occurrences at the facility and identification of measures to avoid future recurrences of safety significant events.

In addition to the above, PSA can and should provide valuable information to NII inspectors in the following:

- i. Understanding the safety significance of the issues under consideration by the Inspectorate, e.g. modifications being assessed or events under investigation.
- ii. Focusing site inspection activities on those areas (systems, components, features, etc) with the highest safety significance.
- iii. Understanding the safety significance of inspection findings.

## 2) Technical adequacy of PSA applications

For the PSA to be an effective tool to support decision making, not only should the quality of the PSA be adequate (in line with SAP FA.13) but also the way in which the PSA is used should be appropriate, ie, PSA studies performed to support any safety submission, including the justification of any modification to plant or operation, should be comprehensive, technically sound and properly documented. In this regard:

- i. Any issue that is going to be evaluated using PSA (eg a facility design or operational feature, a proposed change to the design, or an event at the facility) should be explicitly defined together with the type of results required as input to the decision-making, including any numerical criteria that need to be met.
- ii. All aspects of the PSA model and data potentially affected by the issue under study should be identified, evaluated for impact and modified if necessary.
- iii. All the assumptions should be checked for validity against the issue under study and modified if appropriate.
- iv. Sensitivity analyses should be carried out to estimate the sensitivity of the risk to changes in relevant assumptions and areas of modelling uncertainty, to check the risk impact of different options under consideration and to carry out 'what if' analyses if appropriate. The results of the sensitivity analyses should be used to inform the decision-making process.
- v. Uncertainty analyses should be carried out as described in [3.5 above](#).
- vi. Based on the results of the sensitivity and uncertainty analyses, the duty-holder should show 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 adopting the precautionary principle (as described in paragraphs 89 and the following ones of R2P2, [Ref 5.5](#)).
- vii. The issue under study could potentially affect 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 should be recognised and identified explicitly. In order to perform a comprehensive risk analysis the PSA models should be extended and/or enhanced to cover the missing aspects. If this is not practicable (e.g. due to time constraints), the risk impact of the issue associated with areas outside the scope of the existing PSA should be analysed qualitatively.
- viii. The outcome of the PSA studies performed to evaluate issues should be clear, comprehensive and traceable and should provide recommendations based on a systematic application of decision-making criteria applied to the results of the PSA evaluations.

### **3.7 Fault analysis: assurance of validity of data and models – Theoretical models – FA.17**

#### **“Theoretical models should adequately represent the facility and site”**

Theoretical models are used throughout the PSA, eg, reliability models (including common cause failure 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.

SAP FA.17 is strongly linked to FA.18 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.

### **3.8 Fault analysis: assurance of validity of data and models – Calculation methods – FA.18**

#### **“Calculation methods used for the analysis should adequately represent the physical and chemical processes taking place”**

Calculation methods are used in support of various tasks in PSA, e.g. 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, in itself, uses 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.

For this, inspectors should satisfy themselves that the calculation algorithms have been validated with actual experience, experiments, tests or other calculation methods. Inspectors should also seek evidence that uncertainties in the calculation methods used have been recognised by the duty-holder and that methods have only been applied within their limit of applicability. As deemed appropriate, inspectors may wish to consider undertaking (or commissioning) independent calculations for some aspects of the PSA (eg, addressing areas of particular concern) using different calculation methods. This is particularly important if the PSA is being used to support a new design. TAG T/AST/042 ([Ref 6.7](#)) should be referred to for further guidance.

SAP FA.18 is strongly linked to FA.17 discussed above 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.

### **3.9 Fault analysis: assurance of validity of data and models – Use of data – FA.19**

**“The data used in the analysis of safety related aspects of plant performance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means”**

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. The use of data in PSA has been discussed in section 3.5 (3) above. Section 3.5 (4) has also discussed the need to evaluate the uncertainty in the input data and its impact on the overall PSA results. Section 3.6 (2) has addressed how to interpret this uncertainty in decision-making. Therefore, this SAP is viewed as a reinforcement of specific PSA SAPs FA.13 and FA.14.

Data about physical processes is also an input to PSA supporting calculations. Such data should be justified by reference to physical data, experiment or other appropriate means. See also 3.10.

### **3.10 Fault analysis: assurance of validity of data and models – Computer models – FA.20**

**“Computer models and datasets used in support of the analysis should be developed, maintained and applied in accordance with appropriate quality assurance procedures”**

Computer models are developed to support various tasks in PSA, e.g. for derivation of success criteria, accident progression analyses, 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 this SAP cannot be stressed enough. 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 duty-holders have put in place adequate procedures to develop, maintain and apply computer models and databases.

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 duty-holder 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 duty-holder 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 duty-holder.

Generally inspectors should expect that the Quality Assurance process applied to the PSA covers all items identified in SAP FA.20. Further guidance on the use of computer models in safety cases is provided in T/AST/042 (Ref 6.7).

### **3.11 Fault analysis: assurance of validity of data and models – Documentation – FA.21**

**“Documentation should be provided to facilitate review of the adequacy of the analytical models and data”**

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.

Good practice on PSA documentation can be found in IAEA TECDOC on Living PSA (Ref 5.4). This report recommends that, as part of the PSA documentation, individual Task Procedures should be developed to ensure that all analysts working in a task develop a consistent set of models which interface without overlap or omission, and also to be used for future revisions to the PSA. Inspectors may choose to review or audit these procedures, if available, to gain confidence on the consistent application of methods throughout the PSA.

Ref 5.4 also recommends that for each PSA task, analysis files should be compiled including relevant reports, input data, relevant calculations, and model or database files containing task results. The PSA task reports should describe the analyses performed and all the modelling assumptions; should identify interfaces with other tasks; and should list all the references used. These analysis files should be controlled documents which are maintained for the life of the facility. They enable any PSA analyst familiar with the particular task to recreate, modify or review the particular part of the PSA. Experience with large PSA models suggest that unless there is a complete set of such files, it is very difficult to define and understand each element of the computer model and the results of its quantification.

### **3.12 Fault analysis: assurance of validity of data and models – Sensitivity analyses – FA.22**

**“Studies should be carried out to determine the sensitivity of the fault analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation“**

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 FA.22.

Sensitivity analyses have been addressed in section 3.5 (4). In addition, section 3.6 (2) discusses the role of sensitivity analyses when using PSA to support decision-making. Therefore, this SAP reinforces specific PSA SAPs FA.13 and FA.14.

### **3.13 Fault analysis: assurance of validity of data and models – Data collection – FA.23**

**“Data should be collected by the licensee throughout the operating life of the facility to check or update the fault analysis“**

The validity and applicability of the initiating fault frequencies, component failure probabilities, unavailabilities, etc, used in the PSA can only be assured if these are reviewed periodically using facility specific information.

Therefore, it is reasonable to expect duty-holders 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 e.g. by PSA SAP FA.11 (above) and Assurance of Validity SAP FA.24 (below).

### **3.14 Fault analysis: assurance of validity of data and models – Update and review – FA.24**

**“The fault analysis should be updated where necessary and reviewed periodically”**

Licence Condition 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 LC15 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 (See T/AST/050, Ref 6.9).

FA.24 should also be interpreted as highlighting the principle of Living PSA, in that the Inspectorate wants to see the PSAs as living analyses that constantly reflect the best estimate of the duty-holder on the reliability of components, plant availability etc, current knowledge on plant behaviour, and modern analysis methods. In this regard, this principle reinforces the specific PSA principle FA.11 discussed above.

It is expected that review by the facility operators will identify if operating experience has proved to be significantly different from the assumptions in the analyses and then take action to ensure that risks remain ALARP.

The frequency at which an updating or reconsideration of the PSA should be carried out will depend upon a number of factors, e.g. related to the systems that are in place to collect and analyse data and to the understanding of ageing effect and trends in system reliability. Duty-holders are expected to evaluate the impact of modifications (design, procedures, operating practices, etc.) on the PSA results on a case-by-case basis. Some modifications may therefore require the PSA to be immediately updated. IAEA TECDOC on Living PSA (Ref 5.4) indicates that it is a good practice at operating nuclear power plants, not to accumulate a backlog of such evaluations for a

period longer than a year. It also suggests that, even if risk-significant modifications do not arise for a longer period, the duty-holder should still revise, update and formally amend the PSA every three years.

### **3.15 Relationship with the WENRA Reference Levels**

The Reactor Harmonization Working Group of the Western European Nuclear Regulators Association (WENRA) published Reactor Safety Reference Levels in January 2007 and a revised version in January 2008. Issue O of this document refers to Probabilistic Safety Analysis (PSA). This TAG is consistent with Issue O of the WENRA reference levels. [Appendix 2](#) presents the mapping between Issue O of the WENRA reference levels and this TAG.

### **3.16 Relationship with the IAEA Standards**

Key relevant IAEA publications on PSA are listed in Sections 5, 7, A1-4 and A1-5. The contents of this TAG, including its Appendix 1, are broadly consistent with those IAEA publications. In particular, Refs [5.4, A1-5.6 and A1-5.10] and the latest versions of the IAEA draft standards on Level 1 and Level 2 PSA, Refs [A1-5.7 and A1-5.8] have been specifically used for the preparation of [Appendix 1](#) of the TAG.

## **4 Advice to inspectors**

### **4.1 Introduction**

This section of the TAG aims to provide guidance on the assessment of a PSA which generally fall under SAPs FA.10 to FA.14. The guidance in this section is presented in the order of a typical PSA as this is likely to be of more practical value to the inspectors.

This section is split up into a number of parts dealing with the different elements of a PSA. Each part is made up of a number of specific points of guidance to NII inspectors. It should be noted that all of these points need not be met fully in each and every instance. It is left to the judgement of the individual inspector to identify both the scope of assessment and which, if any, of the shortfalls are significant.

The guidance provided in this section is generally applicable to the assessment of PSAs for all types of nuclear facilities. However, more specific and detailed assessment expectations for review of PSAs for Nuclear Power Plants (NPPs) are given in [Appendix 1](#) to this TAG. Since much of the guidance provided in [Appendix 1](#) can also be applied to other types of facilities, inspectors may wish to use [Appendix 1](#) at their discretion for the assessment of PSAs for facilities other than NPPs.

### **4.2 PSA Scope**

1) PSA should be a systematic analysis to identify all important fault sequences which can lead to radiological consequences and to evaluate their contribution to the risk. The PSA should set out to identify all the significant contributions to the risk since, otherwise the analysis is not complete and conclusions drawn from the analysis may thus be incorrect.

2) The same scope for PSAs is, in principle, applicable to both old and new facilities. However, the methods and details of analysis that would be acceptable to NII may be different as an existing facility may be able to offer operating experience and feedback as an alternative to detailed analysis in some areas.

3) The inspector may consider:

- i. In cases where there is currently no PSA, whether producing one would be worthwhile.
- ii. In cases where there is a PSA, whether the objectives of the analysis are appropriate and its scope adequate to meet them;
- iii. whether the scope of the PSA covers all the sources of radioactivity on the facility;
- iv. whether the scope of the PSA allows a meaningful comparison to be made with the numerical targets of the SAPs;
- v. whether the scope of the PSA covers all classes of initiating faults and hazards;
- vi. whether the scope of the PSA covers all foreseeable operating modes of the facility;
- vii. whether any reductions in scope of the PSA from the above pointers are identified;
- viii. whether, where the scope of the PSA has been reduced, a justification is provided to confirm that this would not change the conclusions of the PSA.

4) Specific assessment expectations for review of the scope of the PSA for Nuclear Power Plants can be found in Table A1-1.2 (PSA Scope) of [Appendix 1](#).

### **4.3 PSA Methodology**

1) The starting point for the PSA is a detailed description of the design and operation of the facility and its associated protection system, 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:

- i. the detailed design of the facility and its equipment to which the PSA refers is identified;
- ii. 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);

- iii. the methods of analysis used in the PSA are defined and are suitable to meet the objectives of the analysis;
  - iv. the PSA has been fully documented;
  - v. the PSA has been carried out in accordance with written QA procedures;
  - vi. the PSA has undergone an independent assessment/peer review and the findings are acceptable.
- 3) Specific assessment expectations for review of the adequacy of the documentation provided in support of each technical task of the PSAs for Nuclear Power Plants can be found in the various Tables of [Appendix 1](#).

#### **4.4 Fault and Hazard Identification**

- 1) The fault schedule should list all the identifiable initiating faults and hazards within the scope of the PSA which could lead directly or in combination with other failures to a release of radioactive material.
- 2) The inspector may consider whether:
  - i. the fault schedule covers all the sources of radioactive material in the facility;
  - ii. the quantity, form and location of all radioactive material in the facility is identified;
  - iii. 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;
  - iv. the fault schedule, covers all the operating modes of the facility;
  - v. if any operating mode is not covered in the fault schedule, justification is given that the contribution to the risk is small during this operating mode;
  - vi. the fault and hazard identification process is shown to be comprehensive so that all possible initiating faults are identified;
  - vii. the fault schedule includes partial failures as well as total failure;
  - viii. all relevant internal hazards are listed;
  - ix. all relevant external hazards are listed;
  - x. each initiating fault and hazard on the schedule is defined;
  - xi. the causes of each initiating fault are identified;
  - xii. features such as administrative systems, control systems, interlocks etc which limit the frequency of an initiating fault are identified;

xiii. failures of protection system equipment which can occur as a consequence of an initiating fault are identified;

xiv. a list is prepared of faults which are not included on the fault schedule because of very low frequency or "incredibility", with reference to the justification;

xv. full records of the fault and hazard identification process are available and are of suitable quality;

xvi. any fault or hazard screening criteria adopted are clearly described and justified.

3) Specific assessment expectations for review of the adequacy and completeness of the list of Initiating Faults considered in the PSAs for Nuclear Power Plants can be found in Tables A1-2.1 (Identification and grouping of Initiating Faults), A1-2.7 (Analysis of Hazards) and A1-2.8 (Low Power and Shutdown modes) of [Appendix 1](#).

#### **4.5 Protection and Mitigation Systems**

1) The PSA should identify the safety systems which are required to operate for each of the initiating faults and hazards and identify the minimum level of performance needed for each of the safety functions.

2) The inspector may consider whether for each initiating fault and hazard:

i. the safety functions have been identified;

ii. the minimum safety systems requirements to achieve the safety functions have been identified;

iii. the minimum protection system requirements are consistent with any deterministic / transient analysis presented;

iv. the protection listed in the fault schedule takes account of failures in protection system equipment which can occur as a consequence of the initiating fault or hazard;

v. for automatic protection actions, the parameters and systems used to initiate the action have been identified;

vi. for manually initiated protection actions, the alarms and indications which would alert the operator to the need for the action are identified;

vii. a fault schedule should be provided linking initiating faults to protective and mitigating systems and operator actions, and identifying the link to maintenance requirements and procedures.

3) Specific assessment expectations for review of the adequacy of the credited safeguards in PSAs for Nuclear Power Plants can be found in Table A1-2.2 (Accident sequence development: determination of success criteria) of [Appendix 1](#).

## 4.6 Event Sequence Analysis

1) The next stage of the PSA is the event sequence analysis which models the behaviour of the facility for the initiating fault groups and hazards chosen for detailed analysis. The analysis should cover all possible combinations of success or failure of the protection systems to perform the safety functions and should identify the fault sequences which involve failure to maintain the facility within safe limits.

2) The end points of the events sequence analysis should be categorised in terms compatible with the numerical targets of the SAPs addressed. This does not necessarily mean that the categories defined by the duty-holders have to be identical to those corresponding to the numerical targets of the SAPs. However, safety cases should be presented in a manner which allows inspectors to make judgements against the SAPs' targets. The inspector may check that, for each initiating fault or hazard:

- i. the event sequence analysis covers all the safety functions required and all the combinations of protection system equipment which can operate to perform the safety functions;
- ii. the event sequence analysis takes account of all the functional dependencies between safety functions and protection systems;
- iii. the event sequence analysis covers all the mechanisms which could lead to failure of the physical barriers such as a reactor pressure vessel or the containment;
- iv. the event sequence analysis covers the factors which affect the release and transport of radioactive and toxic materials to the environment and their effects on humans;
- v. sufficient radiological analysis is available to justify the categorisation of the end-points of the event sequence analysis or that reasonably conservative assumptions have been made;
- vi. the transient, radiological and other deterministic analyses used to support the PSA models do not contain undue pessimisms (these should preferably be best estimate);
- vii. where faults are grouped, the fault group frequency is the sum of the individual faults grouped and the group is represented by the most onerous one.

3) Specific assessment expectations for review of the adequacy of the grouping of Initiating Faults in PSAs for Nuclear Power Plants can be found in Table A1-2.1 of [Appendix 1](#). Specific assessment expectations for review of the Event Sequence Analysis in PSAs for Nuclear Power Plants can be found in Table A1-2.3 of [Appendix 1](#).

## 4.7 Protection and Mitigation Systems Failure Analysis

1) The events sequence analysis identifies combinations of initiating faults/hazards 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 which would lead to the failure. The basic events would typically include; component failure, common cause failure, component unavailability during maintenance or test and operator error.

2) The most usual method of safety system analysis is fault tree analysis; other techniques are acceptable but may need additional scrutiny.

3) The inspector may consider whether:

i. the systems failure analysis covers all the failure states identified by the event sequence analysis;

ii. the analysis has been carried out to a low enough level of detail (e.g. individual component level) so that the design and operation of the system is adequately modelled;

iii. all the relevant failure modes of protection system equipment have been included;

iv. where components have been grouped together in the analysis (eg in "super-components"), failure of each of the components in the mode specified has the same effect on the system;

v. the systems failure analysis models all the support systems required and that all interdependencies due to common services have been represented;

vi. the systems failure analysis takes account of consequential failures which could occur due to the initiating fault or hazard;

vii. common cause failures are included in the models at an appropriate level (see also SAP EDR.03 and T/AST/036, [Ref 6.6](#));

viii. all operator errors which can contribute to the failure of a protection system have been identified and modelled in the analysis, with due consideration of dependencies;

ix. the unavailability of components, trains of systems or the entirety of systems during periods of maintenance or testing has been addressed in the analysis.

4) Specific assessment expectations for review of the System Analysis in PSAs for Nuclear Power Plants can be found in Table A1-2.4 of [Appendix 1](#).

## 4.8 PSA Input Data

1) Data is required to estimate the frequencies and probabilities in the PSA.

2) The inspector may consider whether:

i. data is provided for all the basic events and initiating fault frequencies included in the PSA;

ii. the data provided is preferably best estimate and appropriate for the use made of it in the PSA;

iii. where use is made of operating experience data in calculating initiating fault 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;

iv. where insufficient directly relevant data are available, the source of any quoted generic data and the basis of any judgements are stated;

v. for initiating fault frequencies

a. the data covers all the causes of the initiating fault which have been identified;

b. where the initiating fault 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;

c. where no relevant operating data is available and judgement has been used to assign the initiating fault frequency, the basis for this judgement has been stated and shown to be valid, as far as possible;

vi. for component failure rates (or probabilities)

a. the boundaries of the component for which the data is specified are defined;

b. the data covers all relevant failure modes of the component;

c. the data used corresponds to the component in terms of type, manufacture, operating environment, usage and maintenance regime;

d. 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;

e. 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;

f. 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;

vii. for component unavailabilities

- a. the data covers all causes of component unavailability including tests (scheduled and unscheduled), maintenance (scheduled and unscheduled) and repair;
- b. justification is given that the frequency and duration of the component unavailabilities adequately represents typical facility operation;

viii. for common cause failures

- a. a suitable limit has been placed on the reliability which is claimed for any non-diverse system. Claims of less than  $10^{-5}$  f/d need to be closely scrutinised (EDR.3);
- b. 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 (see T/AST/036, [Ref 6.6](#))

ix. operator error probabilities

- a. should reflect the complexity of the task required and the factors which may be present which influence the performance of the operator (stress, the time available, training, procedures and environmental conditions);
- b. where judgements have been made, the basis for the judgement is stated and shown to be valid as far as possible;

x. 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;

xi. the possibility of component failure rates or unavailabilities increasing with time, e.g. through ageing, is considered.

3) Specific assessment expectations for review of the Data Analysis in PSAs for Nuclear Power Plants can be found in Tables A1-2.5 (Human Reliability Analysis) and A1-2.6 (Data Analysis) of [Appendix 1](#).

#### **4.9 Analysis of Internal and External Hazards**

1) The development of generic assessment expectations for review of the Analysis of Internal and External Hazards in PSAs for all types of facilities is being considered for a future update of this TAG. In the interim, Table A1-2.7 of [Appendix 1](#) can be used, with due care, for this purpose.

2) Specific assessment expectations for review of the Analysis of Internal and External Hazards in PSAs for Nuclear Power Plants can be found in Table A1-2.7 of [Appendix 1](#).

#### **4.10 Analysis of Other Operating Modes**

1) The Development of generic assessment expectations for review of the Analysis “other operating modes” in PSAs for all types of facilities is being considered for a future update of this TAG.

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

#### **4.11 Evaluation of Release Frequencies**

1) The development of generic assessment expectations for review of the Evaluation of Release Frequencies in PSAs for all types of facilities is being considered for a future update of this TAG.

2) Specific assessment expectations for review of the Level 2 PSA\* for Nuclear Power Plants can be found in Table A1-3 of [Appendix 1](#).

\* For NPPs, Level 1 PSA is the part of the overall PSA that focuses on the potential for core damage; Level 2 PSA widens this analysis to consider release magnitudes and frequencies from losses of containment or otherwise; while Level 3 PSA is wider still, and considers risks to the public from off-site releases.

#### **4.12 Evaluation of Off-site Risks and Consequences**

1) The development of generic assessment expectations for review of Off-site Risks and Consequences in PSAs for all types of facilities is being considered for a future update of this TAG.

2) Specific assessment expectations for review of the Level 3 PSA for Nuclear Power Plants can be found in Table A1-4 of [Appendix 1](#).

#### **4.13 Quantification of the Analysis**

1) The PSA should determine the combinations of basic events such as component failure, common cause failure, operator error and plant unavailability which lead to the fault sequence 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 FA.20) and the evidence of this should be provided by the duty-holder (FA.21).

2) The inspector may consider whether:

i. where computer programs are used, they and their results are verified, manual calculations should have been independently checked by the duty-holder;

- ii. the combinations of basic events (minimal cut sets) which lead to failure of the protection systems are identified and listed for each of the initiating faults and hazards analysed;
- iii. that single order minimal cut sets are identified and brought to the attention of the assessors dealing with compliance with the single failure criteria;
- iv. the combinations of basic events do lead to the protection system failure (for this, inspectors should review a sample of the cut sets including those which make the highest contributions to the frequency/probability calculated);
- v. 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;
- vi. 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;
- vii. the importance of initiating faults, components, systems, operator errors and dependencies in the calculation of the risk have been identified.

3) Specific assessment expectations for review of the Quantification of PSAs for Nuclear Power Plants can be found in Table A1-2.9.2 of [Appendix 1](#).

#### **4.14 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 carried out to determine the degree of sensitivity to ensure that the conclusions drawn from the analysis are still valid in the light of these uncertainties (FA.22). 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. Standard importance functions may be used to identify the critical basic events to be covered by the sensitivity studies, as well as providing the means by which the impact to the risk can be gauged.

2) The inspector may check that:

- i. 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;
- ii. as far as the basic event data is concerned, the error factors used are justified, systematically assigned and are a reasonable representation of the uncertainty.

3) Specific assessment expectations for review of the Sensitivity and Uncertainty Analyses in PSAs for Nuclear Power Plants can be found in Table A1-2.9.1 of [Appendix 1](#).

#### **4.15 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 duty-holder's own criteria.
- 2) The inspector may consider:
  - i. whether sufficient information is provided to allow NII to make a comparison with the SAPs;
  - ii. the extent to which the results of the PSA meet the numerical target in the SAPs;
  - iii. whether suitable judgements has been made, where possible, of the magnitude of "excluded" contributions to the risk in relation to those calculated in the PSA;
  - iv. 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 NII's ALARP guidance, T/AST/005 ([Ref 6.1](#)).
  - v. whether, in cases where changes to the design or operation of the facility are proposed, the corresponding reduction in the risk has been calculated.
- 3) Specific assessment expectations for review of the Results of the PSAs for Nuclear Power Plants 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](#).

#### **5 References (General)**

- 5.1 [HSE, Safety Assessment Principles for Nuclear Facilities, 2006 Edition.](#)
- 5.2 US NUCLEAR REGULATORY COMMISSION, Handbook of Parameter Estimation for Probabilistic Risk Assessment, NUREG/CR-6823 (2002)
- 5.3 BEDFORD, T, COOKE, R, Probabilistic Risk Analysis – Foundations and Methods, Cambridge University Press (2001)
- 5.4 INTERNATIONAL ATOMIC ENERGY AGENCY, Living Probabilistic Safety Assessment (PSA), IAEA-TECDOC-1106, IAEA, Vienna (1999)
- 5.5 [HSE, Reducing Risks and Protecting People – HSE's Decision Making Process, 2001](#)

#### **6 References (Technical Assessment Guides, TAGs)**

- 6.1 [T/AST/005, NSD Guidance on the demonstration of ALARP.](#)
- 6.2 [T/AST/011, The single failure criterion.](#)

- 6.3 T/AST/012, Human reliability analysis (in preparation)
- 6.4 [T/AST/016, Structural integrity.](#)
- 6.5 [T/AST/017, Structural integrity: civil engineering aspects.](#)
- 6.6 [T/AST/036, Diversity, redundancy, segregation and Layout of mechanical plan.](#)
- 6.7 [T/AST/042, Validation of computer codes and calculational method.](#)
- 6.8 [T/AST/046, Computer based safety systems.](#)
- 6.9 [T/AST/050, Periodic Safety Reviews \(PSRs\).](#)
- 6.10 [T/AST/051, Guidance on the purpose, scope and content of nuclear safety cases.](#)

## **7 Bibliography**

(See also list of [References](#) and [Bibliography](#) of Appendix 1)

7.1 INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessment for Non-Reactor Nuclear Facilities, IAEA TECDOC-1267, IAEA, Vienna (2002)

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

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

## Appendix 1 - T/AST/030 – Assessment Expectations for Review of PSAs for Nuclear Power Plants

### A1-1 Introductory note

A1-1.1 This Appendix provides detailed guidance on the assessment of PSA specific for Nuclear Power Plants (NPPs). This is presented in the form of a Table of Assessment Expectations for different 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 provided in [Appendix 1](#) can also be applied to other types of installations.

A1-1.2 There is an expectation that duty-holders will present the PSA analysis within a framework compatible with good industry practices. For Nuclear Power Plants this suggests a traditional Level 1, 2, 3 PSA framework as presented in IAEA Guidance (Refs A1-4.1 – A1-4.4). 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 INSAG (Ref A1-4.5), which implies a need to calculate the appropriate risk figures of merit including core damage frequency and large release frequency.

A1-1.3 However, in order to address the relevant numerical targets of the SAPs, duty-holders 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. NII prefers that duty-holders 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.

A1-1.4 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 duty-holders in order to address the relevant numerical targets of the SAPs.

### A1-2 Explanatory notes to Appendix 1

The following information is necessary to interpret the Table of Assessment Expectations:

**DA:** PSA submitted for generic design assessment (GDA).

**Lic:** PSA submitted for reactor licensing.

**Co:** PSA submitted for reactor commissioning.

**Op:** PSA used to support NPP operation.

Black	The expectation is, in principle, not applicable at this point in the regulatory process / NPP lifecycle
Grey	The expectation is applicable if the facility specific information is already available.
White	The expectation is applicable at this point in the regulatory process / NPP lifecycle

### **A1-3 Use of this Appendix**

A1-3.1 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 duty-holders.

A1-3.2 Although an attempt has been made to make this Appendix comprehensive, it is only meant for guidance and by no means should be taken to imply that inspectors have no discretion when choosing the scope and depth of the assessment to be undertaken.

A1-3.3 In addition, it should be stressed that is not the intention of Appendix 1 to prescribe specific methods and approaches for conducting PSA for NPPs. Duty-holders 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.

A1-3.4 This Appendix can be used in a more prescriptive manner when commissioning PSA assessment work (to be done on behalf of NII) 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.

### **A1-4 References**

A1-4.1 INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series, Safety Guide NS-G-1.2, IAEA, Vienna (2001)

A1-4.2 INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessment of Nuclear Power Plants (Level 1), Safety Series No 50-P-4, IAEA, Vienna (1992)

A1-4.3 INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms, Safety Series No. 50-P-8, IAEA, Vienna, 1995

A1-4.4 INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), IAEA-Safety Series 50-P-12, IAEA, Vienna (1996).

A1-4.5 INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999)

## **A1-5 Bibliography**

A1-5.1 AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-S-2005 (2005)

A1-5.2 AMERICAN NUCLEAR SOCIETY, External Events PRA Methodology, American National Standard, ANSI/ANS-58.21-2007 (2007)

A1-5.3 EPRI/NRC-RES, Fire PRA Methodology for Nuclear Power Facilities, NUREG/CR-6850 (2005)

A1-5.4 AMERICAN NUCLEAR SOCIETY, Fire PRA Methodology, American National Standard, ANSI/ANS-58.23-2007 (2007)

A1-5.5 EUROPEAN UTILITY REQUIREMENTS FOR LWR NUCLEAR POWER PLANTS, Volume 2: Generic Nuclear Island Requirements – Chapter 17: PSA Methodology, Revision C (2001)

A1-5.6 INTERNATIONAL ATOMIC ENERGY AGENCY, Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants, IAEA-TECDOC-1511, IAEA, Vienna (2006)

A1-5.7 INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Draft Safety Guide DS394 (Information about this document can be found in [‘Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants’](#)).

A1-5.8 INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Draft Safety Guide DS393 (Information about this document can be found in [‘Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants’](#)).

A1-5.9 INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic safety assessments of nuclear power plants for low power and shutdown modes, IAEA-TECDOC-1144, IAEA (2000)

A1-5.10 INTERNATIONAL ATOMIC ENERGY AGENCY, Review of Probabilistic Safety Assessments by Regulatory Bodies, IAEA-Safety Report Series No 25, IAEA, Vienna (2002)

A1-5.11 INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Report Series No. 10, IAEA, Vienna (1998)

A1-5.12 NUCLEAR ENERGY INSTITUTE, Probabilistic Risk Assessment (PRA) Peer Review Process Guidance, NEI 00 02 (2000)

A1-5.13 NUCLEAR ENERGY INSTITUTE, Process for Performing Follow on PRA Peer Reviews using the ASME PRA standard, NEI 05-04 (January 2005)

**A1-6 Table of Assessment Expectations**

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<b>Table A1-1. General Expectations</b>				
<b>Table A1-1.1 Approaches and methodologies</b>				
<p>This table lists PSA Assessment Expectations for all the technical areas of Level 1, 2 and 3 PSA. It is not the intention of this guide to prescribe specific methods and approaches for all those technical areas.</p> <p>The duty-holder may chose to use alternative methods to those covered by this table of expectations as long as they lead to equally valid outcomes.</p> <p>In cases where the PSA or specific areas of it have been undertaken using alternative approaches, NII will review them on a case-by-case basis and judge them on their own merits. External expert support should be sought where necessary.</p> <p>If task procedures have been developed for the individual PSA tasks and these have been provided by the duty-holder, NII inspectors may wish to assess or audit them 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.</p> <p>Inspectors may wish to request information on any independent or peer review of the PSA commissioned by the duty-holders (eg, scope, findings, duty-holder’s action plan to address findings and their status) in order to plan and inform their own assessment.</p>				
<b>Table A1-1.2 PSA Scope</b>				
<p>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).</p> <p>Adequate justification is provided when sources of radioactivity</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
are not included in the scope of the detailed PSA.				
The PSA covers all types of initiating faults (internal events, internal hazards, external hazards)				
The PSA covers all operational modes				
<b>Table A1-1.3 Freeze Date</b>				
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”.				
<b>Table A1-1.4 Computer codes and inputs</b>				
The codes used (e.g. 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 NII quality expectations as described in SAPs paragraphs 551ff and <a href="#">T/AST/042</a> .				
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 (eg, thermal-hydraulic, accident progression, structural integrity, etc), is adequate and auditable.				
The input data files for the code calculations are auditable.  The sources of information (e.g. design documents) are identified.				
Facility-specific and site-specific information are used.  If walk downs are used to obtain input data, these are documented in an auditable fashion.				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
In the absence of facility-specific and/or site-specific details, all the assumptions regarding geometry, construction, materials, topography, weather, population, etc, are stated. A process is in place to ensure that the assumptions made are captured in the future completion of the design and construction, or are revised, as appropriate, when information about the site becomes available				
NII holds a licence for the PSA quantification software used, or alternative suitable arrangements for PSA quantification by NII inspectors (or their contractors) are feasible.				
All computer files for the PSA model/s and reliability database/s have been provided to the NII.				
<b>Table A1-2. Level 1 PSA</b>				
The criteria for CORE DAMAGE are defined. The definition of CORE DAMAGE is adequate.				
If a design target for CORE DAMAGE FREQUENCY has been identified, this is explicitly stated.				
<b>Table A1-2.1 Identification and Grouping of Initiating Faults</b>				
The task aim is explicitly stated: it addresses all disturbances that require mitigation to prevent core damage and those that lead directly to core damage.				
The process used in the identification and definition of initiating faults is clear and leads to a systematic and comprehensive identification of initiating faults.				
Detailed records exists of all deductive analyses (e.g. master logic diagrams) and/or inductive analyses (e.g. failure modes and effects analyses) done to identify initiating faults. All assumptions are captured.				
Previous experience at similar NPPs has been searched for and fed back into the initiating fault identification process.				
The source documents 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 fault				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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 faults to each operating mode is transparent.				
Consequential initiating faults have been addressed and the way in which they are developed is clear.				
Each initiating fault is clearly defined and characterised (i.e. its causes and impact on plant are identified).				
The process for grouping initiating faults is clear, i.e. the grouping criteria and the mapping to derive the final initiating fault groups are transparent.				
Each initiating fault group is represented by the most onerous fault.				
The initiating fault groups have been defined in a way that vulnerabilities are not masked.				
Each initiating fault group is clearly defined and characterised. The information provided is sufficient for the quantification of initiating fault frequencies (ie, its causes are identified) and for the development of accident sequence models (ie, its impact on plant is stated).				
<b>Table A1-2.2 Accident sequence development: determination of success criteria</b>				
For each initiating fault 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.				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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 a given system response will prevent the safety limit being exceeded.				
Timing for operator actions is justified (e.g. by sufficient and representative thermal-hydraulic analyses).				
The thermal-hydraulic, neutronics (and any other) analyses used for derivation of success criteria are thoroughly documented and fully traceable.				
The regulator 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 regulator 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 duty-holder.				
If use is made of success criteria for the various initiating fault 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 success criteria for each safety function for each initiating fault Group are stated and include: minimum equipment requirements and mission times, details of the specific operator actuations required and time available for operator actuation. This information is traceable to the underlying analyses.				
<b>Table A1-2.3 Accident sequence development: Event Sequence Modelling</b>				
<b>Table A1-2.3.1 General</b>				
The general assumptions relating to all event tree development are defined up-front and properly 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, eg,				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
"Injection of 2003 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).				
<b>Table A1-2.3.2 Specific for each Initiating Fault Group Event Tree</b>				
<p>The evolution of the sequence of events following the representative initiator from each initiating fault group is described. This includes the parameters that cause reactor trip, the signals/channels that initiate various safety functions, and the operators' intervention in the course of the sequence.</p> <p>The timing of events in the sequence following the success or failure of signals/safety functions are identified and defined.</p>				
<p>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.</p> <p>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 fault 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.</p>				
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 (eg, 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.				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
The mission time for each heading of each branch of the tree, when applicable, is stated and justified.				
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.				
In the absence of fully developed procedures, the link is clear between the various headings/nodes of the event tree and assumptions on potential operational and emergency procedures to be developed.  A process is in place to ensure that these assumptions are captured in the future development of operational and emergency procedures.				
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 are correct. They 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 fault groups under consideration.				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<b>Table A1-2.4 System analysis</b>				
<b>Table A1-2.4.1 General</b>				
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 unavailabilities 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 (e.g. 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, e.g. 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				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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, eg, “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.				
<b>Table A1-2.4.2 Specific for each system model</b>				
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.				
If the system design is not complete, all the assumptions on system design are stated.  A process is in place to ensure that these assumptions are captured in the future completion of the system design.				
The system boundaries are clearly identified and there are no gaps and/or overlaps at the interface with other systems modelled in the PSA.				
System success criteria are stated.  The success criteria applied in the PSA model (e.g. the applied front-line system success criteria) are consistent with those				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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 unavailabilities due to test).				
System testing activities or assumptions on system testing strategies to be developed are stated. A process is in place to ensure that assumptions are captured in the future development of the testing schedule.				
Information on system maintenance for all components is provided (including the mechanical and electrical tag out boundaries, ie, an identification of all the mechanical, electrical, instrumentation, etc, components which are functionally unavailable or isolated in order to perform the maintenance).				
Assumptions on system maintenance strategies to be developed are stated. A process is in place to ensure that these assumptions are captured in the future development of the maintenance schedule.				
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.				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
All relevant component failures have been correctly included in the fault tree.				
<p>The events that represent unavailabilities due to testing and maintenance have been modelled correctly.</p> <p>All configurations allowed by the NPP procedures are represented in the models.</p> <p>The chosen modelling “solution” to avoid combinations of maintenance activities forbidden by rules and procedures has been implemented properly.</p>				
<p>Hardware failures that contribute to the Human Failure Events (e.g. failure of the alarms or indications) have been included in the model.</p> <p>Justification has been provided for any cases where these hardware failures have not been included based on the assumption that the HFE dominates.</p>				
All relevant human failure events have been correctly included in the fault tree				
<p>All house events 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.</p> <p>The purpose of each house event is clear.</p> <p>A table is included that lists the house events modelled in the system fault trees and their settings in each heading, sequence or event tree. The settings are correct.</p>				
<p>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).</p> <p>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.</p>				
All intra-system and inter-system common cause failures to be modelled in the system fault tree have been identified in conformance with the general approach to the analysis of common cause failures.				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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 (e.g. 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.				
<b>Table A1-2.5 Human Reliability Analysis (HRA)</b>				
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, (ie 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 fault HFEs include individual and common-cause misalignments and mis-calibrations. The identification of these events is complete.  If some potential pre-initiating fault HFEs are not included in the model, adequate justification is provided.  The modelling of pre-initiating fault HFEs events is correct.				
If HFEs associated with initiating faults are embedded in the data used in the analysis of initiating fault 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 fault is generally performed for the PSA for Low Power and Shutdown modes (see Table A1- 2.8 below).				
Post-initiating fault 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				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>been diagnosed incorrectly. The identification of these events is complete.</p> <p>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.</p> <p>If some potential post-initiating fault HFEs are not included in the model, adequate justification is provided.</p> <p>The modelling of post-initiating fault HFEs events is correct.</p>				
<p>For each pre-initiating fault HFE, all the operational activities which could lead to the human error are identified (e.g. surveillance tests, calibrations, maintenance activities or operational realignments).</p> <p>Any operational activities screened out are justified.</p> <p>(Note: This should be consistent with the guidance for the assessment of task analysis in the TAG on HRA to be developed. Ultimately, in order to avoid duplication, this may be removed from the PSA TAG and may be replaced by an entry point to the HRA TAG.)</p>				
<p>In the absence of facility specific information, for each pre-initiating fault HFE, any assumptions regarding tests, maintenance tasks or operational realignments that could lead to the human error are stated.</p> <p>A process is in place to ensure that these assumptions are captured in the future development of testing, maintenance and operational procedures and strategies and completion of system designs.</p> <p>(Note: This should be consistent with the guidance for the Assessment of task analysis in the TAG on HRA to be developed. Ultimately, in order to avoid duplication, this may be removed from the PSA TAG and may be replaced by an entry point to the HRA TAG.)</p>				
<p>For each post-initiating fault HFE which involves failure to respond to procedural steps, equipment failures, alarms or other cues, the cues are identified.</p> <p>(Note: This should be consistent with the guidance for the Assessment of task analysis in the TAG on HRA to be developed. Ultimately, in order to avoid duplication, this may be removed from the PSA TAG and may be replaced by an entry point to the HRA TAG.)</p>				
<p>In the absence of facility specific information, for each post-</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>initiating fault HFE which involves failure to respond to procedural steps, equipment failures, alarms or other cues, the assumptions regarding the cues available to the operator are identified.</p> <p>A process is in place to ensure that these assumptions are captured in the future development of procedures and completion of design.</p> <p>(Note: This should be consistent with the guidance for the assessment of task analysis in the TAG on HRA to be developed. Ultimately, in order to avoid duplication, this may be removed from the PSA TAG and may be replaced by an entry point to the HRA TAG.)</p>				
<p>Occasions for misdiagnosis of the situation by the operators have been analysed systematically.</p> <p>HFEs resulting from identified credible mis-diagnosis have been modelled correctly (e.g. human actuations due to mis-diagnosis that change the course of an accident sequence will normally be modelled in the event trees. Un-required switching off of systems due to mis-diagnosis will normally be modelled in the fault trees).</p>				
<p>The human reliability quantification method/s selected is/are suitable for the specific type of HFEs addressed with the method.</p>				
<p>Specific human error contributors to each HFE are identified:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• The possible human failure modes included (i.e. commission, omission, etc.) are identified.</li> </ul> <p>(Note: This should be consistent with the guidance for the assessment of task analysis in the TAG on HRA to be developed. Ultimately, in order to avoid duplication, this may be removed from the PSA TAG and may be replaced by an entry point to the HRA TAG.)</p>				
<p>Facility-specific and HFE-specific influences of the factors required by the quantification model (Performance Shaping Factors, PSFs) are identified.</p> <p>Facility-specific information obtained from observations made during walk-downs and simulator exercises, review of procedures, discussions with, and interviews and questionnaires</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>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.</p> <p>(Note: This should be consistent with the guidance for the assessment of the Human Reliability Analysis in the TAG on HRA to be developed. Ultimately, in order to avoid duplication, this may be removed from the PSA TAG and may be replaced by an entry point to the HRA TAG.)</p>				
<p>In the absence of facility specific information, all the assumptions made to characterise the PSFs (e.g. quality of man-machine interface, quality and availability of procedures, level of training, degree of supervision, accessibility, etc) are described and justified. A process is in place to ensure that relevant assumptions are captured in the future development of procedures and completion of the design.</p> <p>(Note: This should be consistent with the guidance for the assessment of the Human Reliability Analysis in the TAG on HRA to be developed. Ultimately, in order to avoid duplication, this may be removed from the PSA TAG and may be replaced by an entry point to the HRA TAG.)</p>				
<p>Time windows are correctly 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.</p> <p>(Note: This should be consistent with the guidance for the assessment of the Human Reliability Analysis in the TAG on HRA to be developed. Ultimately, in order to avoid duplication, this may be removed from the PSA TAG and may be replaced by an entry point to the HRA TAG.)</p>				
<p>Specific expectations for the assessment of the HRA in Low Power and Shutdown PSA are included in Table A1- 2.8 below.</p>				
<p>Specific expectations for the assessment of the HRA for the Hazards PSA are included in Table A1- 2.7 below.</p>				
<p>The quantification of all the HFES is transparent.</p> <p>The quantification of all the HFES has been done correctly and in accordance with the HRA method/s selected.</p>				
<p>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</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
provided.				
<p>Dependencies between HFEs appearing in the same accident sequence are identified and accounted for.</p> <p>The process by which the candidates for dependency were identified is transparent.</p> <p>Any assumptions made in the dependency analysis are described and justified.</p> <p>The determination of the degree of dependency is transparent and justified.</p> <p>The method by which the conditional probabilities of dependent HFEs are calculated is clear.</p> <p>The dependency analysis is adequate.</p>				
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.				
<b>Table A1-2.6 Data Analysis</b>				
<b>Table A1-2.6.1 Initiating fault frequencies</b>				
The initiating fault definitions used in the data analysis task are fully consistent with those used in the list of initiating faults.				
<p>The criteria for selection of analysis methods are stated.</p> <p>The approaches used to quantify initiating fault frequencies are suitable for each type of initiating fault addressed.</p> <p>The approach/es used to quantify frequencies of consequential initiating faults is/are correct.</p>				
The criteria for selection/precedence of data sources are stated.				
<p>Facility-specific event data has been used to the extent possible.</p> <p>For cases where facility-specific event data is used, the source of event records is available, comprehensive and auditable.</p> <p>Facility-specific records have been interpreted correctly.</p>				
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				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>history of the facility/ies where the event/s occurred has been used in the determination of the denominators for the evaluation of initiating fault frequencies. This information is auditable.</p> <p>In the absence of information on facility operating history, any assumptions made to determine the denominators for the evaluation of initiating fault frequencies are stated and reasonable.</p>				
<p>For cases where generic reactor type initiating fault frequencies are used, this is justified and documented in an auditable fashion.</p>				
<p>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.</p>				
<p>For cases where logical models are used to calculate the initiating fault frequencies, these include all the foreseen inputs leading to the initiating fault.</p> <p>The fault trees, human reliability analyses or other models used to calculate initiating fault frequencies are documented. In order to review these, inspectors can use the relevant tables of this Appendix.</p>				
<p>In the absence of specific information about the site, generic site assumptions used to calculate frequencies of initiating faults (such as “Loss of offsite power”, “Loss of heat sink”, etc) are stated.</p>				
<p>The initiating fault groups are assigned frequencies equal to the summed frequency of all the faults in the group.</p>				
<p>A list of all the initiating faults, together with their frequencies, is included. Each initiating fault frequency is represented by a mean value and a statistical representation of its uncertainty. This list is traceable to the supporting analyses.</p>				
<p>A list of all the initiating fault groups, together with their frequencies, is included. Each initiating fault group frequency is represented by a mean value and a statistical representation of its uncertainty. This list is traceable to the supporting analyses.</p>				
<b>Table A1-2.6.2 Random component failures</b>				
<p>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</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
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.				
<p>Facility-specific data has been used to the extent possible.</p> <p>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 (eg, records of operating/stand-by hours, of test/maintenance/repair time history) which have been used are available and traceable.</p> <p>The collection of facility records is comprehensive and exhaustive.</p> <p>Evidence is provided that the PSA data analysts have checked the quality and reliability of the facility-specific records used to support the PSA.</p>				
<p>Facility-specific records have been interpreted correctly (in particular to identify the failure modes modelled in the fault tree)</p> <p>The interpretation of historical records to reconstruct demand counts, operational times, etc. is clear.</p> <p>When facility-specific event records are not complete or clear, the assumptions made by the analysts are clearly stated and reasonable.</p>				
The method used for estimating failure rate parameters from raw data is transparent and mathematically correct. No				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
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.				
<p>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.</p> <p>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.</p> <p>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.</p>				
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.	■	■		
<p>In the absence of facility-specific information on test intervals to calculate probabilities for the failure modes of each component, the assumptions on system testing strategies to be developed are stated.</p> <p>A process is in place to ensure that these assumptions are captured in the future development of the testing schedule.</p>			■	■
The mission times (used to calculate the probabilities of failure to operate of components) are correct and consistent with the information on mission times recorded in the documentation of the Success Criteria Determination task.				
<p>The methodology used for the calculation of structural failure probabilities is justified. The details of the analysis are transparent.</p> <p>If use is made of data from structural (e.g. 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.</p> <p>If use is made of a probabilistic fracture mechanics code, the</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>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.</p> <p>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.</p> <p>Inspectors should refer to TAGs <a href="#">T/AST/016</a> and <a href="#">T/AST/017</a> for further guidance here.</p>				
<p>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.</p>				
<p>The methodology used for the estimation of failure probabilities for computer-based systems is transparent and meets industry-accepted practices.</p> <p>The analysis of the software reliability carried out by the duty-holder 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.</p> <p>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.</p> <p>The reliability analysis of the computer-based hardware is documented.</p> <p>Any self-checking built into the systems is taken into account in an adequate manner.</p> <p>The dependencies between diverse software systems are dealt with explicitly.</p> <p>Inspectors should refer to <a href="#">T/AST/046</a> for further guidance on computer-based systems.</p>				
<p>A list of all the basic events that represent random component failures together with their parameter estimates is included.</p> <p>Each parameter estimate is represented by a mean value and a statistical representation of its uncertainty.</p> <p>This list is traceable to the supporting analyses.</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<b>Table A1-2.6.3 Unavailabilities due to testing and maintenance</b>				
The descriptions of events that represent unavailabilities 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 unavailabilities.				
The probabilities assigned to events that represent configurations not observed during the data collection period are reasonable best estimates.				
The calculation of unavailabilities 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 unavailabilities 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.				
<b>Table A1-2.6.4 Common Cause Failures (CCFs)</b>				
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.				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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 (e.g. 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.				
If suitable facility-specific data or information is not available, any assumptions made in regard to the defences against CCFs are stated.  A process is in place to ensure that these assumptions are captured in the future development of the design, testing schedule and strategy, etc.				
For cases where expert-judgement has been used for CCF parameter estimation, a justification is provided that no better source of data is available.  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				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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.				
<b>Table A1-2.7 Analysis of Hazards</b>				
<b>Table A1-2.7.1 General</b>				
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 faults, 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.				
In the absence of information about the site, assumptions regarding generic site are stated and justified.				
In the absence of complete/detailed facility-specific information to support the hazard analyses, all the assumptions made are identified (eg, assumptions on specific hazard sources, hazard control programmes, hazard protection features, exact location of equipment, etc.)  A process is in place to ensure that relevant assumptions are captured in the future development of hazard protection strategies and procedures, in the completion of system designs,				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
in the finalisation of equipment allocation, and in the facility construction.				
Specific modifications made to the internal events PSA models (event trees and fault trees) and parameters (e.g. 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. The development of specific, detailed guidance to address a wider range of internal and external hazards will be considered when this TAG is next updated.				
<b>Table A1-2.7.2 Analysis of Internal Fires</b>				
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.				
Evidence that walk-downs have been conducted is included and documented in detail (since fire 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 fire PSA is apparent throughout.				
General assumptions of the fire analysis are stated and properly justified.				
<p>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.</p> <p>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.</p> <p>Assumptions made in support of the initial quantification of fire compartments for the purpose of quantitative screening are transparent (e.g. assumptions on the impact of fires on equipment, human reliability, etc) and adequate.</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>The global boundary of the analysis is defined so that this includes all locations at the NPP relevant to the risk calculations (e.g. 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).</p>				
<p>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.</p> <p>Details of the compartmentalisation of the facility are transparent and include a description of the partitioning elements or features which have been assumed.</p> <p>A list of all compartments is included using a consistent identification scheme.</p> <p>Up-to-date drawings or references showing compartment boundaries are available.</p>				
<p>The process to identify essential equipment has identified all equipment whose failure or mal-operation will cause an initiating fault 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.</p>				
<p>Established procedures are in place and implemented for evaluating circuits and selecting cables required to support the operation of essential equipment.</p>				
<p>Equipment circuits and cables required to support the credited functionality of essential equipment are identified.</p> <p>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.</p> <p>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.</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>In the absence of complete/detailed facility-specific information to support the fire PSA, all the assumptions made in support of the analysis are identified (e.g, assumptions on ignition sources, amount of combustible material, control programmes for combustible and ignition sources, allocation of equipment/cables, fire barriers, separation, segregation, fire detection and suppression equipment, performance of the fire brigade, etc.)</p> <p>A process is in place to ensure that these assumptions are captured in the future development of fire protection strategies and procedures, in the completion of system designs, in the finalisation of cable routings, and in the final construction.</p>				
<p>If a first qualitative screening of fire compartments is undertaken, the details of this are transparent.</p> <p>The screening has been performed in accordance with established criteria.</p> <p>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.</p>				
<p>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 (e.g. 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.</p>				
<p>Evaluation of fire frequencies has been performed for all the compartments qualitatively screened-in.</p> <p>The method for the calculation of fire frequencies, including the input data and information used, is clear.</p> <p>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.</p> <p>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.</p> <p>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</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>adequate manner. Assumptions made in lieu of facility-specific information are only made for NPPs not yet built and when used, are identified explicitly.</p> <p>Fire suppression is not taken into account in the calculation of fire frequencies.</p> <p>The calculation of fire frequencies for all fire compartments is documented explicitly. No errors are apparent.</p> <p>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.</p>				
<p>If a quantitative screening of fire compartments is undertaken, the details of this are transparent.</p> <p>The screening has been performed in accordance with established criteria.</p> <p>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.</p>				
<p>Detailed analysis has been performed for all the compartments quantitatively screened-in.</p> <p>The fire scenario (or scenarios) associated with each compartment is properly characterised in terms of source, propagation, detection, human response and damage:</p> <ul style="list-style-type: none"> <li>• For each compartment, details of the specific fire sources and targets are transparent. Evidence that all potential ignition sources have been addressed is provided.</li> <li>• 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.</li> <li>• The analysis of fire impact in each fire compartment is transparent and takes into account: <ul style="list-style-type: none"> <li>– Equipment damaged in the compartment by flame, plume, ceiling jet, hot gases and radiant heat.</li> <li>– Electrical faults (open circuits, shorts to ground, short circuits and hot shorts) and their impact, eg, loss of equipment function, spurious actuation of equipment (e.g., undesired reconfiguration of valves or actuation of standby systems), loss and/or false signals and indications.</li> <li>– Explosions and their impact, including high-energy arcing</li> </ul> </li> </ul>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>faults.</p> <ul style="list-style-type: none"> <li>– Collapse of structures and their impact.</li> <li>– Missiles and their impact.</li> <li>– Smoke and heat effects and their propagation to neighbouring compartments.</li> <li>– Identification of initiating faults in each compartment as the result of the fire.</li> </ul> <ul style="list-style-type: none"> <li>• 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 fault. 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.</li> <li>• The reliability of the various fire protection measures (both in terms of equipment as well as human performance) is substantiated.</li> </ul> <p>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).</p> <p>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).</p>				
<p>The analysis of inter-compartment fire propagation is documented explicitly.</p> <p>The requirements listed above for fire modelling of single compartments are applied to the modelling of multi-compartment scenarios.</p> <p>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.</p> <p>The effectiveness and reliability of any active fire barrier (e.g. damper, suppression system) is explicitly addressed in the fire</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>risk model and the risk contribution associated with its failure is evaluated.</p> <p>Details of the fire barrier and propagation analysis (barrier penetration analysis) are transparent.</p> <p>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.</p> <p>Multi-compartment scenarios which cannot be screened-out are carried onto the next stages of the fire PSA.</p>				
<p>Details of the accident sequence modelling and quantification for each identified scenario are transparent. In particular:</p> <ul style="list-style-type: none"> <li>• The most onerous initiating fault has been selected to be the basis for the quantification of each fire scenario. The rationale for this selection is clear.</li> <li>• 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.</li> <li>• 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 (e.g. in scenarios of CCR abandonment), etc, is analysed fully and transparently. The HRA for fire scenarios is adequate.</li> <li>• The quantitative and qualitative results of the quantification of each fire scenario are included.</li> <li>• 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.</li> </ul>				
<b>Table A1-2.7.3 Analysis of Internal Flooding</b>				
<p>The approach to flooding PSA adopted is sufficiently detailed to allow a realistic estimation of the risk from flooding and the</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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.				
<p>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.</p> <p>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.</p> <p>Assumptions made in support of the initial quantification of flood compartments for the purpose of quantitative screening are transparent (e.g., assumptions on the impact of floods on equipment, human reliability, etc) and adequate.</p>				
The global boundary of the analysis is defined so that this includes all locations at the NPP relevant to the risk calculations (e.g. 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.).				
<p>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).</p> <p>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).</p> <p>A list of all compartments showing compartment boundaries is included. Up-to-date drawings or references to these are included.</p>				
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				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>minimum water volume needed to affect water-sensitive equipment by immersion/splashing, internal flood barriers and spray shields, potential flood sources and types (e.g. high energy steam pipework), automatic and manual flood detection and isolation means, possible flood effects in each compartment (e.g. initiating faults, damage to safety equipment) and in compartments to which the flooding may propagate, etc.</p>				
<p>The susceptibility of each type of component appearing in the PSA to flood-induced failure mechanisms is identified and justified (e.g. submergence, jet impingement, pipe whip, humidity, condensation, temperature)</p>				
<p>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.</p>				
<p>In the absence of complete/detailed facility-specific information to support the flooding PSA, all the assumptions made in support of the analysis are identified (e.g. assumptions on flooding sources, allocation of equipment, segregation, flood detection and protection measures, etc).</p> <p>A process is in place to ensure that these assumptions are captured in the future development of flood protection strategies and procedures, in maintenance procedures, in the completion of system designs and allocation of equipment, and in the final construction.</p>				
<p>Details of the first qualitative screening of flood compartments and flood sources are auditable.</p> <p>The screening has been performed in accordance with established criteria.</p> <p>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.</p>				
<p>Evaluation of flooding frequencies has been performed for all the compartments qualitatively screened-in.</p> <p>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.</p> <p>The method for the calculation of flood frequencies, including the input data and information used, is clear.</p> <p>For each compartment, the nature of possible flood causes is</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>identified, e.g. 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.</p> <p>For each compartment, the location and characterisation of flood sources, describing e.g. 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.</p> <p>Similar flood cases are adequately grouped in the modelled scenarios. All the assumptions made in this process are transparent.</p> <p>The calculation of flood frequencies for all identified flooding scenarios is documented explicitly. No errors are apparent.</p> <p>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.</p>				
<p>Details of the quantitative screening of flood scenarios are transparent.</p> <p>The screening has been performed in accordance with established criteria.</p> <p>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.</p>				
<p>Detailed analysis has been performed for all the flood scenarios quantitatively screened-in, including:</p> <ul style="list-style-type: none"> <li>• For each compartment where a flooding scenario has been identified, the rate at which a flood could develop is provided.</li> <li>• The equipment which is assumed to be damaged by water spray, jet impingement, pipe whip etc due to the flood source is identified.</li> <li>• Flood effects in the compartment due to e.g. equipment immersion, humidity and temperature are identified. These cover both initiating faults and equipment damage.</li> <li>• Adverse effects in compartments affected by the propagation of floods are identified.</li> <li>• For each flooding scenario, a flood progression tree (or equivalent) has been developed that identifies flood progression stages reached (leading to an initiating fault or</li> </ul>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>to damage to any relevant system) depending on the success or failure of flood isolation actions.</p> <ul style="list-style-type: none"> <li>• Indications, events and any other cues which can provide flood symptoms and allow for flood detection are identified explicitly.</li> <li>• Actions needed for flood isolation before a given flood progression stage is reached are described explicitly.</li> <li>• The reliability of the flooding protection measures (both in terms of equipment as well as human performance) are substantiated.</li> </ul>				
<p>Details of the accident sequence modelling and quantification for each identified scenario are transparent. In particular:</p> <ul style="list-style-type: none"> <li>• The initiating fault identified for each flood scenario is justified.</li> <li>• 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 are correct.</li> <li>• 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.</li> <li>• The quantitative and qualitative results of the quantification of each flooding scenario are included.</li> <li>• 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.</li> </ul>				
<b>Table A1-2.7.4 Seismic Analysis</b>				
<p>The approach used to evaluate and represent the hazard from earthquakes is described and appropriate</p>				
<p>The seismic hazard analysis is documented in detail.</p> <p>The assumptions and models used for aspects such as the characterisation of sources and attenuation relationships are clearly identified.</p> <p>All the values for the parameters used in the model are</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
<p>identified and the way the final hazard curves have been constructed is auditable.</p> <p>The mean curve for the site is represented together with its uncertainty bounds. This is traceable to the underlying analyses.</p>				
<p>All the references to historical data used are identified and auditable.</p>				
<p>The approach used to evaluate the impact of earthquakes on the NPP structures and components is described and appropriate.</p>				
<p>All the equipment that requires analysis of the probability of failure against earthquake magnitudes is identified, ie, 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.</p> <p>This list is traceable to safety case / internal events PSA sources.</p>				
<p>If the number of components for which detailed fragility analysis has been performed has been limited using some type of screening, the screening criteria is defined and is adequate.</p> <p>The screening analysis is traceable.</p>				
<p>The design parameters used for the derivation of fragilities of equipment and structures are identified.</p> <p>The fragility analysis is auditable.</p>				
<p>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.</p>				
<p>The initiating faults arising from the full range of earthquakes are identified.</p>				
<p>If the number of earthquake-induced initiating faults considered in the seismic PSA quantification has been limited using some type of screening, the screening criteria is defined and is adequate.</p> <p>The screening analysis is traceable.</p>				
<p>The potential for secondary hazards, e.g. earthquake-induced fires and floods has been analysed systematically during the</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
seismic walk-down and the results are auditable.				
<p>The way in which the seismic failures and successes and random component failures have been combined is traceable.</p> <p>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.</p> <p>Any modifications to the event and fault tree logic models to incorporate the impact of earthquakes on the NPP are auditable and correct.</p> <p>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.</p> <p>The Human Reliability Analysis has been revisited to address the operator response following the seismic events of concern. Details of this analysis are auditable.</p>				
<p>The quantitative and qualitative results of the quantification are included.</p> <p>Sensitivity, uncertainty and importance analyses are provided.</p>				
<b>Table A1-2.8 Low power and shutdown modes</b>				
<p>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.</p>				
<p>The identification of the Plant Operational States (POS) during non-full power modes is justified.</p> <p>There are no gaps and/or overlaps between the POS addressed in the low power and shutdown PSA and those covered in the PSA for full power.</p> <p>All the characteristics considered for the identification of possible stages during low power and shutdown (pre-POS) are clear. No important characteristic is missing.</p> <p>The grouping of pre-POS into the final list of POS is justified and visible. The grouping is adequately justified.</p>				
<p>A table listing all the POS with their characteristics is included. The information about all the POS' characteristics is presented and complete.</p> <p>Information about plant configuration (decay heat removal</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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.				
In the absence of complete/detailed NPP-specific information to support the definition and characterisation of POSs, all the assumptions made to form the information basis for this analysis are identified.  A process is in place to ensure that relevant assumptions are captured in the future development of low power and shutdown strategies and procedures, outage schedules, technical specifications, etc.				
The analysis of initiating faults for each POS is transparent.  The analysis of initiating faults 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 faults. The analysis process is transparent.				
In the absence of complete/detailed facility-specific information to support the identification of human actions leading to initiating faults, all the assumptions made to form the information basis for this analysis are identified explicitly.  A process is in place to ensure that relevant assumptions are captured in the future development of low power and shutdown strategies and procedures.				
A table showing the initiating fault groups defined and their applicability to each POS is presented. No errors are apparent				
The derivation of the frequency of the initiating faults 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 fault 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.				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>If screening of combinations of initiating fault 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.</p>				
<p>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.</p> <p>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, e.g. reactor coolant system water inventory, steam generator availability, core inventory, decay heat curve. The boundary conditions used in these analyses are stated.</p> <p>The success criteria for the Low Power and Shutdown PSA are developed on a realistic basis.</p>				
<p>Event trees have been developed for each combination initiating fault-POS that has been screened-in.</p>				
<p>System models have been developed taking into consideration the specific characteristics of each POS. Details of this are transparent.</p>				
<p>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.</p>				
<p>In the absence of facility-specific maintenance procedures and work plans, the assumptions made to define the event tree boundary conditions and system status modelled in the fault trees are justified and documented.</p> <p>A process is in place to ensure that these assumptions are captured in the future development of low power and shutdown strategies and procedures.</p>				
<p>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, e.g. 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,</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>increased workload, etc.</p> <p>The HRA has considered all the aspects of the NPP shutdown relevant to human reliability mentioned above clearly and systematically.</p>				
<p>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.</p> <p>Examples of specific aspects that inspectors should expect the PSA to address are:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Dropped loads: number of heavy loads lifted during maintenance outages; potential for dropped loads to directly affect spent fuel during the refuelling, etc.</li> </ul>				
<b>Table A1-2.9 Uncertainty analyses, Quantification and Interpretation of the Level 1 PSA Results</b>				
<b>Table A1-2.9.1 Uncertainty and Sensitivity analyses</b>				
<p>The sources of uncertainty in the Level 1 PSA are identified explicitly.</p> <p>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.</p>				
<p>All assumptions made throughout the study are clearly identified, described and properly justified.</p> <p>The specific aspects of the PSA models or data related to these assumptions are clear.</p> <p>A table of assumptions is provided.</p> <p>Sensitivity studies have been carried out to evaluate the risk significance of assumptions.</p> <p>The sensitivity studies address the effects of key assumptions</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>and combinations of assumptions.</p> <p>The sensitivity studies and their results are transparent.</p>				
<p>Uncertainties in input probability and frequency values have been estimated.</p> <p>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.</p> <p>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).</p>				
<p>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.</p> <p>The results of the uncertainty and sensitivity evaluations demonstrate that the overall conclusions obtained from the Level 1 PSA are still valid.</p> <p>Steps have been taken to reduce the most important uncertainties (and hence the uncertainties in the overall PSA results). These are explicitly described.</p>				
<b>Table A1-2.9.2 Quantification of the Level 1 PSA</b>				
<p>The results obtained from the quantification are reproducible:</p> <ul style="list-style-type: none"> <li>• The type of quantification and related approximations are explicitly stated.</li> <li>• The cut-offs used for the quantification are explicitly stated and adequate.</li> <li>• Any minimal cut-set editing performed is transparent.</li> <li>• 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.</li> </ul>				
<p>Complete results of the quantification are provided. These include:</p> <ul style="list-style-type: none"> <li>• Minimal cut sets with numerical results and description of the basic events.</li> <li>• Lists of basic events and associated importance measures, as a minimum fractional contributions (Fussell Vesely</li> </ul>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>Importance) and risk increase factors (Risk Achievement Worth).</p> <ul style="list-style-type: none"> <li>• Lists of relevant groups of components or basic events and associated importance functions as for basic events.</li> </ul>				
<p>Quantification has been carried out (and results provided) at different levels:</p> <ul style="list-style-type: none"> <li>• Level 1 PSA (for full power operation).</li> <li>• Level 1 PSA (for operation at low power and shutdown).</li> <li>• Individual initiating fault groups (event trees).</li> <li>• Individual accident sequences (in the event trees).</li> <li>• Individual hazards for power operation and non-power conditions.</li> <li>• Individual hazard scenarios for power operation and non-power conditions.</li> <li>• 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.</li> <li>• Annualised frequencies (ie, point in time risk) for each operational state in order to support the ALARP arguments.</li> </ul>				
<p>A sample survey of the PSA results has been carried out to improve confidence in the correctness of the Level 1 PSA quantification.</p>				
<b>Table A1-2.9.3 Presentation and Interpretation of the Level 1 PSA Results</b>				
<p>A summary of the Level 1 PSA results is included in the PSA documentation.</p> <p>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.</p>				
<p>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.</p> <p>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.</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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.				
<b>Table A1-3. Level 2 PSA</b>				
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.				
<b>Table A1-3.1 Interface between Level 1 and Level 2 PSA</b>				
The entirety of the Level 1 PSA has been taken forward to the Level 2 analysis (Internal initiating faults, internal and external hazards at power, low power and shutdown)				
<p>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.</p> <p>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.</p> <p>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</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
<p>human error dependencies) are correctly represented.</p> <p>The analysis is transparent.</p>				
<p>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.</p> <p>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.</p> <p>The identification and characterisation of PDSs is adequate.</p> <p>A sufficient number of PDS has been defined to avoid masking important ways of accident progression while ensuring a manageable scope of analysis.</p>				
<p>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.</p> <p>The models are correct.</p>				
<p>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.</p> <p>All the dependencies are properly captured.</p>				
<p>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.</p>				
<p>The criteria used to group the (Level 1 - Level 2 interface) event tree sequences into the defined PDSs are identified explicitly and correct.</p> <p>The process of mapping the resulting accident sequences from the modified event trees to the relevant Plant Damage States is transparent.</p> <p>If the binning process (allocation of sequences to end state categories) is automated, an auditable record exists of this process.</p> <p>The identification and characterisation of PDSs is traceable in both directions, i.e. Level 1 cut-set/sequence to PDS and PDS back to Level 1 sequence. No errors are identified in the grouping of accident sequences into the defined PDSs.</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>Each PDS has been assigned a frequency equal to the summed frequency of all the sequences in the group.</p> <p>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.</p>				
<p>If a separate code is used for Level 2 PSA, the way in which the sequence or cut-set definitions and frequencies from the Level 1 – Level 2 interface have been transferred to the Level 2 PSA is transparent.</p>				
<b>Table A1-3.2 Deterministic Accident Progression Analysis</b>				
<p>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 faults (such as unanticipated transients). Alternatively, the code has been applied to experimental facilities or to other NPPs of similar design with equivalent fidelity.</p> <p>The code and inputs meet NII quality expectations (e.g. 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.</p> <p>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.</p> <p>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.</p> <p>The codes have been used within their limit of applicability.</p>				
<p>Modelling options (if any) selected by the code user reflect 'best-practice' recommendations of the code developers or a recognised and experienced user community.</p> <p>Deviations from best-practice choices of options are documented and justified.</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>The modelling options available in the computer code are applied consistently throughout the calculations performed for different fault sequences.</p> <p>Differences in the codes, models or modelling options used (if any) are documented and justified.</p>				
<p>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.</p>				
<p>No relevant and potentially important phenomena have been neglected or dismissed without an adequate technical justification.</p>				
<p>All the assumptions made are stated explicitly.</p> <p>All the assumptions made are justified, i.e. the rationale for choosing these assumptions and for rejecting alternatives is clear and reasonable.</p> <p>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.</p>				
<p>The accident progression analyses have been performed on a best-estimate basis and are specific to the facility.</p>				
<p>In the absence of facility-specific details, all the assumptions regarding facility design and construction are stated.</p> <p>A process is in place to ensure that these assumptions are captured to support the future design and construction.</p>				
<p>The accident scenarios selected as input to the accident progression calculations are appropriate and transparent throughout the various accident progression analyses.</p> <p>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.</p>				
<p>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.</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
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 duty-holder.				
<b>Table A1-3.3 Containment Performance Analysis</b>				
<p>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.</p> <p>The method is state-of-the-art and meets accepted industry standards.</p>				
<p>The code and inputs used for analysing containment structural integrity meet NII quality expectations as described in Table A1-1.4 of this Appendix.</p> <p>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.</p>				
The models used to characterise the loss of containment integrity (e.g. 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.				
<p>The loads and combinations of loads studied are clear.</p> <p>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.</p>				
<p>In the absence of facility-specific details, all the assumptions regarding containment geometry, construction and materials are transparent.</p> <p>A process is in place to ensure that these assumptions are</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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. The NII 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.				
<b>Table A1-3.4 Probabilistic Modelling Framework – Accident Progression Event Trees (APETs)</b>				
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 (e.g., pathways through an event tree) are associated with a single, unique outcome (e.g. a release category).				
The Level 2 PSA code used to develop the APETs provides the necessary capability to support the modelling approach selected, e.g. the capability to handle multiple branches for a single event tree node, headings represented by models other than fault trees (e.g. event trees, user defined code), global variables (e.g. 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				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>approach selected, the way in which these aspects of the model have been handled in the quantification is clear.</p>				
<p>An APET has been developed for each PDS.</p>				
<p>The APETs are clearly described (ie, 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.</p> <p>The time frames depicted are transparent and organised in the correct order with proper treatment of chronological dependencies.</p> <p>When uncertainties are addressed via the APET structure, the way in which this has been done is transparent.</p> <p>All assumptions are described and justified.</p> <p>All simplifications (e.g. issues excluded from the APET) are described and justified.</p> <p>The dependencies between/among phenomena are explicitly identified and properly captured in the logic model and in the assignment of event probabilities.</p> <p>Dependencies within the Level 1 core damage sequences are adequately modelled.</p> <p>The structure of each APET, and associated event probabilities, are traceable to the underlying deterministic accident progressions analyses carried out to support their development.</p>				
<p>The APET includes HFES for severe accident management actions. Table A1-.2.5 of this appendix applies for the assessment of these actions.</p> <p>The dependencies with the HFES in the Level 1 PSA are identified and treated appropriately.</p> <p>Potential adverse effects of severe accident management actions are modelled.</p>				
<p>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:</p> <ul style="list-style-type: none"> <li>• Event probabilities which represent random events (i.e.,</li> </ul>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>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.</p> <ul style="list-style-type: none"> <li>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.</li> </ul>				
<p>In cases where APET probability values represent uncertainty about deterministic outcomes, the analyses performed to generate have:</p> <ul style="list-style-type: none"> <li>Identified the relevance of the defined severe accident time frames and has taken this into account adequately</li> <li>Used up-to-date information on accident phenomenology.</li> <li>Justified the applicability of the sources of information used.</li> <li>Used facility-specific information wherever possible.</li> <li>Used an acceptable analysis method - for example, decomposition event trees, Monte Carlo simulation, or another method justified as adequate.</li> <li>Been performed in a transparent and consistent manner.</li> </ul>				
<p>APET drawings are included. Computer files for the APETs are provided.</p>				
<p>System design, operability and survivability modelling is described clearly and justified.</p> <p>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.</p> <p>A process is in place to ensure that these assumptions are captured to support the future system design, installation and qualification.</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<b>Table A1-3.5 Source Term Analysis</b>				
<p>The parameters that influence fission product release, retention and transport through each of the major barriers to the environment are identified explicitly.</p> <p>The attributes that define the characteristics of the radiological releases and potential off-site consequences are identified explicitly.</p> <p>The attributes required in order to perform a Level 3 PSA are identified explicitly, eg magnitude of radionuclides, isotopic composition, release timing, height and frequency of the release, physical and chemical characteristics of the release, heat content of the release (plume), etc.</p>				
<p>Based on the above, a set of release categories (RCs) has been defined, each one representing a different way of radiological release.</p> <p>The time periods considered for the release and the rationale for their choice are transparent and adequate.</p> <p>The characterisation of each RC is clear. All the attributes relevant to each RC are identified explicitly.</p> <p>The identification and characterisation of RCs is adequate.</p> <p>A sufficient number of RCs has been defined to avoid masking important source terms while maintaining a manageable scope for the analysis.</p>				
<p>The method or criteria used to group the severe accident sequences from the APETs into the defined RCs is stated explicitly.</p> <p>The process of mapping the resulting severe accident sequences from the APETs to the relevant RCs is transparent.</p> <p>If the binning process (allocation of sequences to end state categories) is automated, an auditable record exists of this process.</p> <p>No errors are identified in the grouping of severe accident sequences into the defined RCs.</p>				
<p>Each RC has been assigned a frequency equal to the summed frequency of all the severe accident sequences in the group.</p> <p>Each RC provides an adequate representation of the individual sequences within the group.</p>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
The code and inputs meet NII quality expectations as described in Table A1-1.4 of this Appendix.				
<p>The modelling method/s used to perform source term analysis are clear.</p> <p>The radionuclide grouping scheme used for the source term analysis is consistent with current state-of-the-art practice.</p> <p>All the assumptions made to obtain source terms are described and justified.</p> <p>The computer code calculations used as the basis for estimating facility-specific source terms for selected accident sequences are documented.</p> <p>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.</p>				
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 duty-holder.				
<b>Table A1-3.6 Presentation and Interpretation of the Level 2 PSA Results</b>				
<p>The Level 2 PSA results are clearly and thoroughly presented in the PSA documentation.</p> <p>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.</p> <p>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</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
significant uncertainties. A clear explanation is included of why the results of the Level 2 PSA are considered valid despite the identified uncertainties.				
<p>All vulnerabilities identified by the Level 2 PSA are documented explicitly. The corrective actions proposed to address the vulnerabilities are clear.</p> <p>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.</p> <p>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.</p>				
A demonstration that the risk of radioactive release for the NPP is ALARP is included.				
<b>Table A1-4. Level 3 PSA</b>				
<b>Table A1-4.1 Assessment of the Level 3 analysis</b>				
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.				
<p>The end-point(s) of the Level 3 PSA are unambiguously stated and the scope is clearly defined.</p> <p>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</p>				
<p>The calculation methods used in the Level 3 PSA are auditable and reflect the current state of knowledge. These include:</p> <ul style="list-style-type: none"> <li>• The method(s) used to address the relevant phenomena and pathways, e.g. for calculation of atmospheric dispersion, surface deposition, re-suspension, migration through food chains, etc.</li> <li>• The method(s) used for the calculation of dose (external irradiation, irradiation from inhalation, irradiation from ingestion).</li> <li>• The method(s) used for the calculation of health effects (deterministic, stochastic somatic, stochastic hereditary).</li> </ul>				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<ul style="list-style-type: none"> <li>The method(s) used for the calculation of the economic consequences.</li> <li>The selection and justification of parameter values.</li> </ul>				
<p>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.</p> <p>The approach used for meteorological sampling is appropriate.</p> <p>The data used is up-to-date.</p> <p>The site-specific data used to perform the consequence calculations is auditable.</p> <p>Assumptions made are justified.</p>				
<p>If the Level 3 PSA is performed for a generic site, the site generic information and assumptions used to perform the consequence calculations (meteorological, population, agricultural production, land, food distribution data, etc) are stated and justified.</p>				
<p>The input information used in the Level 3 PSA calculations regarding countermeasures and protective actions is stated.</p> <p>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.</p>				
<p>If the Level 3 PSA is performed for a generic site, assumptions on countermeasures and emergency response strategies are stated. These assumptions are reasonable and consistent with national requirements.</p> <p>A process is in place to ensure that these assumptions are captured in the future development of the NPPs' emergency plans.</p>				
<p>Where default data provided by the code is used, its applicability is justified explicitly.</p> <p>The usage of default data is documented in an auditable fashion.</p>				
<p>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</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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.				
<p>Sensitivity analyses have been performed and are documented. The sensitivity analyses capture key assumptions and combinations of assumptions.</p> <p>Uncertainties associated with the input parameters have been quantified using an acceptable method.</p> <p>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.</p> <p>The results of the uncertainty and sensitivity evaluations demonstrate that the overall conclusions obtained from the L3 PSA are still valid.</p>				
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 duty-holder.				
<b>Table A1-4.2 Presentation and Interpretation of the Level 3 PSA Results</b>				
<p>The Level 3 PSA results are clearly presented in the PSA documentation.</p> <p>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.</p>				
<p>All issues or vulnerabilities identified by the Level 3 PSA are documented explicitly. The corrective actions proposed to address the vulnerabilities are clear.</p> <p>An evaluation of the risk improvements expected from the</p>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
<p>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.</p> <p>A formal process is in place to ensure that the proposed corrective actions are captured, as appropriate, in the emergency procedures and arrangements</p>				
A demonstration that the individual and societal risks from the facility under evaluation are ALARP is included.				
<b>Table A1-5 Overall Conclusions from the PSA</b>				
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 duty-holder 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 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				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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				
<b>Table A1-6. Use of PSA to Support Decision-Making</b>				
Note: This table is only generic. Detailed guidance on how to review specific PSA applications will be added as appendices to this TAG. Alternatively, stand-alone TAGs will be released for each application.				
<b>Table A1-6.1 Expected uses of PSA</b>				
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).				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
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.				
<b>Table A1-6.2 Quality of the safety submissions supported by PSA</b>				
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.				

ASSESSMENT EXPECTATION	DA	Lic	Co	Op
<p>Uncertainties in input probability and frequency values have been estimated and propagated through the models to generate uncertainty distributions on the resulting risk figures.</p> <p>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).</p>				
<p>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.</p>				
<p>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.</p> <p>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.</p> <p>If extending the PSA is considered not to be practicable (eg, 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.</p>				
<p>The outcome of the PSA studies performed to evaluate issues is clear, comprehensive and traceable.</p> <p>The outcome of the PSA studies performed to evaluate issues includes the following:</p> <ul style="list-style-type: none"> <li>• A description of the issue under study.</li> <li>• A description of the PSA evaluations undertaken including any numerical criteria established.</li> <li>• A description of the new (or modified) assumptions.</li> <li>• A description of the modifications to models and data and relevant drawings.</li> <li>• The identification of key areas of uncertainty in relation to the issue.</li> <li>• Relevant numerical results.</li> </ul>				

<b>ASSESSMENT EXPECTATION</b>	<b>DA</b>	<b>Lic</b>	<b>Co</b>	<b>Op</b>
<ul style="list-style-type: none"> <li>• Lists of cut-sets and importance measures.</li> <li>• Risk profile (identification of dominant initiating faults, accident sequences, and protection failures).</li> <li>• Results of the sensitivity and uncertainty analyses and conclusions obtained from these.</li> <li>• Qualitative risk arguments used.</li> <li>• 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.</li> </ul>				

**Appendix 2 – T/AST/030 – Mapping between Issue O (Probabilistic Safety Analysis) of the WENRA Reference Levels and the Requirements of this TAG**

<b>TABLE A2: COMPARISON WITH THE WENRA REFERENCE LEVELS</b>		
<b>WENRA REFERENCE LEVELS (ISSUE O)</b>	<b>TAG</b>	<b>COMMENTS</b>
<b>1. Scope and content of PSA</b>		
1.1 For each plant design, a specific PSA shall be developed for level 1 and level 2 including all modes of operation and all relevant initiating events including internal fire and flooding. Severe weather conditions and seismic events shall be addressed.	3.4 3.2.1) (Note: a Level 3 PSA is required to address the numerical targets of the SAPs)	Specific requirements to address scope and level in PSAs for NPPs are spread throughout Appendix 1, e.g. 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.	3.5.2) (2nd paragraph)	Specific requirements to address dependencies in PSAs for NPPs are spread throughout Appendix 1, e.g. 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 basic Level 1 and Level 2 PSAs shall contain uncertainty and sensitivity analyses. The basic Level 2 PSA shall contain sensitivity analyses and, as appropriate, uncertainty analyses.	3.5.4) 3.12	Specific requirements to perform sensitivity and uncertainty analyses in PSAs for NPPs are spread throughout Appendix 1, e.g. 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.	3.4 3.5.2) (paragraph starting Best-estimate), 3.5.3)	Specific requirements to ensure that in PSAs for NPPs the models and data are realistic are spread throughout Appendix 1, eg Table A1-2.2 and A1-2.6

<b>TABLE A2: COMPARISON WITH THE WENRA REFERENCE LEVELS</b>		
<b>WENRA REFERENCE LEVELS (ISSUE O)</b>	<b>TAG</b>	<b>COMMENTS</b>
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	3.5.3)i	Specific requirements for the Human Reliability Analysis in PSAs for NPPs are included in Table A1-2.5
<b>2. Quality of PSA</b>		
2.1 PSA shall be performed, documented, and maintained according to the quality management system of the licensee.	3.11, 3.14	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.	3.3	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)
<b>3. Use of PSA</b>		
3.1 PSA shall be used to support safety management. The role of PSA in the decision making process shall be defined.	3.6.1)	
3.2 PSA shall be used to identify the need for modifications to the plant and its procedures, including for severe accident management measures, in order to reduce the risk from the plant.	3.6.1)	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".	3.2.3)	
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	3.6.1)	

<b>TABLE A2: COMPARISON WITH THE WENRA REFERENCE LEVELS</b>		
<b>WENRA REFERENCE LEVELS (ISSUE O)</b>	<b>TAG</b>	<b>COMMENTS</b>
significance of operational occurrences.		
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.	3.6.1)	
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.	3.6.1)	
<b>4. Demands and conditions on the use of PSA</b>		
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.	3.6.2)	
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.	3.6.2)	
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.	3.6.1)	