|  |
| --- |
|  |
| ONR Technical Assessment Guide  Use of probabilistic safety analysis (PSA) and probabilistic insights |



ONR Technical Assessment Guide (TAG)

Use of probabilistic safety analysis (PSA) and probabilistic insights

**Head of Profession**: Fault Analysis

**Authored by**: Inspector

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

**Issue**: 1

**Published**: September 2024

**Next scheduled review**: September 2027

**Document reference**: NS-TAST-GD-116

**Record reference**: 2023/36861

Revision commentary

|  |  |
| --- | --- |
| Issue | Description of update(s) |
| 1 | A new TAG providing information on use of PSA and probabilistic insights for a wide audience of inspectors. This TAG gives information at a high level and is complementary to NS-TAST-GD030 on PSA which provides detailed guidance for PSA specialists.  The TAG focusses on the information PSA can provide to non-PSA disciplines and the questions inspectors should have in mind when interacting with PSA and probabilistic analysis. |

Contents

[1. Introduction 4](#_Toc176864789)

[2. Purpose and scope 5](#_Toc176864790)

[3. Relationship to licence and other relevant legislation 10](#_Toc176864791)

[4. Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides 12](#_Toc176864792)

[5. Advice to Inspectors 19](#_Toc176864793)

[Appendix 1 – Examples of use of PSA 50](#_Toc176864794)

[Appendix 2 – Mapping between Issue O WENRA Reference Levels 52](#_Toc176864795)

[Appendix 3 – A brief overview of the development of nuclear power plant PSA in the UK 54](#_Toc176864796)

[References 56](#_Toc176864797)

[Glossary and abbreviations 59](#_Toc176864798)

# Introduction

1. ONR has established its [Safety Assessment Principles](http://www.onr.org.uk/saps/saps2014.pdf) (SAPs) [1] which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other dutyholders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR’s inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide (TAG) is one of these guides.

# Purpose and scope

1. The purpose of this technical assessment guide is to provide guidance to inspectors on use of probabilistic safety analysis (PSA), quantitative risk analysis (QRA) and probabilistic insights. This TAG is complementary to another TAG, ‘Adequacy of PSA Modelling and Supporting Analysis’ [2]. While [2] is aimed at PSA specialists, this TAG is intended to have a wider audience and to be written in a way that is easily understood by non-PSA specialists.
2. This TAG is intended to provide an interpretation of those SAPs related to use of PSA, QRA and PSA insights, and to provide general guidance to inspectors that may interact with PSA and QRA during their duties.   
   These safety submissions may come from licensees, licence applicants or generic design assessment (GDA) requesting parties. All these are referred to as ‘dutyholders’ in this TAG.
3. PSA is an engineering analysis tool that uses structured logic modelling, real life performance data, system design and operation information as well as engineering insights and calculations to generate numerical estimates of risk. In the context of this TAG, PSA is carried out for nuclear facilities, but it has also been applied outside of the nuclear industry. A PSA model is a logical structure that represents plant responses to a broad range of initiators and failures under different operating modes. The probabilistic evaluation of these models offers insights into the relative safety importance of initiators, response of structures, systems, components (SSC’s) and of operating procedures. PSA provides an overall view of safety characteristics, including both equipment and operator’s behaviour. PSA helps to assess whether the design objectives regarding reliability, protection against vulnerabilities and effectiveness of different lines of defence have been achieved satisfactorily. Further high-level information on PSA can be found in an Explanatory Note from the WENRA Reactor Harmonisation Working Group [3].
4. Sometimes the term QRA is used interchangeably with PSA (for example, outside of the nuclear industry) or can be used to describe a broad range of techniques to understand and quantify risk insights. While this TAG typically refers to PSA, much of the guidance is also applicable to any type of quantitative analysis. In the USA, PSA is referred to as Probabilistic Risk Assessment (PRA) and US standards refer to PRA rather than PSA.
5. As a PSA model all credible faults and hazards affecting a facility, and associated system responses, inspectors from a wide range of specialisms may encounter PSA within safety cases or situations where QRA or probabilistic insights have been used to inform decision making or plant operations. Inspectors who may interact with PSA can come from a range of areas including fault studies and thermal-hydraulic analysis, mechanical, electrical and control and instrumentation (C&I) systems, civil engineering, human factors, software reliability, structural integrity, internal and external hazards, severe accident analysis (SAA) and radiation safety.
6. ONR assessors can use this TAG to gain an understanding of how PSA can be used by dutyholders during GDA, the permissioning process for new build and plant modification projects for operating facilities. This TAG will also explain the uses of PSA within ONR.
7. The main aspects of PSA and probabilistic insights addressed by this TAG are as follows:

* overview of PSA
* what facilities should have PSA?
* interfaces with other disciplines
* use of PSA for design, modifications, safety case and ALARP
* use of PSA for risk monitors, classification of SSCs and off-site planning
* use of PSA for risk informed decision making, examination inspection maintenance testing (EIMT), claims on operators and technical specifications
* uncertainty and limitations of PSA
* quantification and presentation of results
* comparison with numerical targets
* probabilistic insights within industry and ONR

1. The ‘SAPs addressed’ section of this TAG concentrates on interpretation of the SAPs; general guidance on the use and insights from PSA is given in Section ‎5 on advice to inspectors.
2. 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.

## Terminology

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

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

**Facility***:* A part of a nuclear site identified as being a separate unit for the purposes of nuclear or radiological risk.A facility may, for example, be a single reactor, a group of processing plants as on a nuclear fuel-cycle facility or a dock and its support systems containing a naval reactor plant. The term encompasses both the terms ‘nuclear installations’ as defied in the Nuclear Installations Act 1965   
(as amended) and the term ‘plant’ as used in nuclear site licences.

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

# Relationship to licence and other relevant legislation

1. The nuclear site licence conditions (LCs) give a legal framework which can be drawn on in assessment and are, in general, set out in the form of requiring the licensee to make adequate arrangements, in the interests of safety, to secure certain objectives [4].
2. The principal LCs relevant to use of PSA and probabilistic insights are:

* **LC 14 - safety documentation** - requires the licensee to make and implement adequate arrangements for the production and assessment of safety cases. For complex and high hazard facilities the licensee’s safety case will need to contain PSA as well as deterministic analysis.
* **LC 15 - periodic review** - sets out the requirements for periodic review and reassessment of safety cases. The periodic reviews carried out under these arrangements include those for updating/extending the PSA (or producing one, if none previously exists, and comparison with relevant good practice) and using it to support the arguments for continuing operation during the period until the next review. It is ONR’s expectation that where licensees have established living PSA programmes all relevant files and records will be maintained for the life of the facility.
* **LC 17 - management systems** - sets out the requirement for quality assurance (QA) arrangements for all matters that affect safety. In this respect dutyholders are expected to establish an adequate QA process that is effectively applied during all phases of the PSA and its application.
* **LC 20 - modification to design of plant under construction** –   
  Where available, PSA should be used to risk inform modifications while facilities are being constructed. The earlier PSA is utilised in this process the greater the chance of any associated risks being reduced ALARP. PSA is a powerful tool for improving reliability and avoiding dependencies between SSCs. PSA is the only tool available that can quantitatively characterise the relative importance of SSCs and proposed design modifications as a whole. As such, PSA fills a gap when making ALARP arguments that cannot be covered by other analysis approaches.
* **LC 22 - modification or experiment on existing plant** – Similarly to LC 20, use of PSA should be considered when modifications are being planned on existing plant.
* **LC 23 - operating rules** - requires the licensee to produce an adequate safety case. This should be done in line with the licensee’s safety case production arrangements required by LC 14. For complex and high hazard facilities the safety case should utilise both PSA and deterministic aspects. PSA can also be effectively used to demonstrate the risk benefits of safety mechanisms, devices and circuits, as required by LC 27 where applicable.
* **LC 24 - operating instructions** - requires the licensee to ensure that all operating instructions which may affect safety are written down and complete. This expectation links with the claimed operator actions modelled in the PSA and the operating instructions. Therefore, ONR expects the PSA to be well documented with potential errors operators could make when following operating instructions modelled with high fidelity.
* **LC 28 – Examination, inspection, maintenance and testing (EIMT)** - The licensee shall make and implement adequate arrangements for regular and systematic EIMT. Where available the PSA should be used to risk inform the maintenance schedules and testing regimes based on the significance of systems to safety.

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

## Safety Assessment Principles

1. This guide interprets ONR’s use of the PSA related SAPs,FA.1, FA.10 and FA.14 [1]. Numerical targets five, six, seven, eight and nine related to PSA are also discussed in this guide. A detailed discussion on numerical targets and their basis is explained in Annex 2 of the SAPs. FA.11 (validity of PSA), FA.12 (scope and extent) and FA.13 (adequate representation) are also highly relevant to PSA. [2] discusses these SAPs in more detail.

### FA.1 - Fault Analysis: General Design Basis Analysis, PSA and Severe Accident Analysis

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

1. This principle outlines the inter-relationship between the three types of fault analysis, design basis analysis (DBA), PSA and SAA and how in combination they address the range of potential initiating events (IEs) with nuclear safety significance. As with DBA and SAA, the scope of PSA should be suitable and sufficient and used along with the other two fault analysis approaches to help demonstrate that risks are ALARP and to address SAPs numerical targets five, six, seven, eight and nine. The SAPs establish the expectation that safety cases for power reactors, or where there is significant complexity, or where the numerical targets may be challenged should include PSA.

### FA.10 - Fault Analysis: PSA – Need for PSA

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

1. This principle sets the framework and requirements for a PSA study. PSA should assist designers in achieving a balanced and optimised design so that no particular class of accident or feature of the facility makes a disproportionate contribution to the overall risk. PSA is used by dutyholders to enable risk informed judgements on the safety of the facility, the risk profile, the risk importance of safety systems etc. The overriding aim of ONR conducting assessment of the PSA is to assist regulatory judgements on the safety of the facility and whether the risks of its operation are being made ALARP. In this context ‘suitable and sufficient’ means that the PSA should be of a broad enough scope to capture the risk from a facility, and detailed enough to contribute to the demonstration that the risk is ALARP.

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

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

1. The aim of this principle is to establish the expectations on what uses the dutyholders should make of the PSA to support decision-making and on how the supporting analyses should be undertaken.
2. PSA can be used by dutyholders in several ways including:

* designing the facility
* risk informing modifications to design or operation
* supporting the demonstration that risks are tolerable and ALARP
* informing the selection of safety function categories or the safety class of structures, systems and components
* setting operating rules
* informing arrangements for examination, maintenance inspection and testing (for example the frequencies of these activities)
* plant configuration control (including maintenance planning), which for power reactors is normally through the use of risk monitors
* developing and changing operating procedures and associated training programmes for managing faults and accidents (including severe accidents)
* helping to determine initiating event frequencies for DBA
* providing an input to SAA, support demonstration of practical elimination and to analyses performed under the Radiation (Emergency Preparedness and Public Information) Regulations (REPPIR)
* demonstration of understanding of overall facility risk profile and comparison against numerical targets
* contributing to periodic safety reviews

1. PSA can be used by ONR in several ways including:

* event analysis and investigating significant incidents and events
* understanding the safety significance of issues and inspection findings
* targeting inspections on aspects of the facility with the highest safety significance

1. Further details on all these aspects are covered in Section ‎5.

## WENRA Reference Levels

1. The reactor harmonization working group of the Western European Nuclear Regulators Association (WENRA) published reactor safety reference levels (RLs) in January 2007 and revised versions in January 2008 and most recently February 2021 [5]. They reflect expected practices to be implemented in the WENRA countries. As the WENRA members have different responsibilities, the emphasis of the RLs has been on nuclear safety, primarily focusing on the main safety functions for ensuring the integrity of the reactor core and spent fuel. Issue O of the reference levels refers to PSA. This TAG is consistent with Issue O of the WENRA reference levels. [Appendix 3](#_Appendix_3_–) presents the mapping between Issue O of the RLs and this TAG.

## IAEA Safety Standards and Guides

1. The general safety requirements (GSR) Part 4, ‘Safety assessment for facilities and activities’, states:

“The main factor to be taken into consideration in the application of a graded approach is that the safety assessment shall be consistent with the magnitude of the possible radiation risks arising from the facility or activity. The approach also takes into account any releases of radioactive material in normal operation, the potential consequences of anticipated operational occurrences and possible accident conditions, and the possibility of the occurrence of very low probability events with potentially high consequences.” [6]

1. PSA is particularly valuable for the study of the last two parts of the paragraph above, i.e. consequences from anticipated operational occurrences and analysing the possibility of the occurrence of very low probability events with potentially high consequences. GSR Part 4 also states:

“The safety assessment shall include a safety analysis, which consists of a set of different quantitative analyses for evaluating and assessing challenges to safety by means of deterministic and also probabilistic methods.” [6]

1. Sitting aside the general safety requirements in the International Atomic Energy Agency (IAEA) document hierarchy are the specific safety requirements (SSR). SSR 2/1, which focusses on design of nuclear power plants, states:

“5.76. The design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and for all plant states, including shutdown, with particular reference to:

(a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;

(b) Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented;

c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.” [7]

1. SSR 2/2, which focusses on commissioning and operational, states:

“If a probabilistic assessment of risk is to be used for decision making purposes, the operating organization shall ensure that the risk analysis is of appropriate quality and scope for decision making purposes. The risk analysis shall be performed by appropriately skilled analysts and shall be used in a manner that complements the deterministic approach to decision making, in compliance with applicable regulations and plant licence conditions.” [8]

1. There are various other SSRs published by the IAEA, for example SSR-3 relates to research reactors [9] and SSR-4 relates to safety of nuclear fuel cycle facilities [10].
2. Sitting below the GSR and SSR documents in the IAEA hierarchy are the general and specific safety guides which provide guidance on how to meet the requirements of GSR Part 4 and the SSRs and present international good practice. The IAEA safety guides that are most relevant to PSA are IAEA specific safety guide (SSG) 3 related to level 1 PSA [11] and SSG-4 related to level 2 PSA [12]. The IAEA Safety Series report on conducting level 3 PSA has also recently been re-instated [13]. These guides are aimed at PSA practitioners and provide more detail than necessary for someone looking to gain an overview of PSA. These guides have been used to inform the production of this TAG, and [2].

## American Society of Mechanical Engineers

1. The American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS) jointly publish a range of PSA standards[[1]](#footnote-2):

* Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications [14]
* Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs) [15]
* Standard for Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications [16]
* Requirements for Low Power and Shutdown Probabilistic Risk Assessment [17]
* Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants [18]

1. ONR assessments have recognised some of these standards as a source of relevant good practice for nuclear reactor facility PSA. ONR has not conducted a comprehensive review of the standards, and not all have been used to support PSAs assessed by ONR, however they are used by a wide range of vendors, designers and operators worldwide. Therefore they are likely to be a good source of relevant good practice and help inspectors understand the standards commonly applied to develop PSAs internationally.

## 

## Numerical targets

1. The numerical targets relevant to PSA are discussed in detail in Section ‎5.9. This section provides a summary of the main targets relevant to PSA.   
   These five targets have been selected for this TAG as PSA is often used by dutyholders to provide comparisons of risk from a facility against these targets. The targets quantify ONR’s risk policy and have been set to assist us in making proportionate regulatory decisions and targeting our resources to where the risks and hazards are greatest. More specifically, the targets are guides to inspectors to indicate where additional safety measures may need to be considered and, in the case of permissioning decisions, to help judge whether risks are tolerable. The targets are based on the basic safety level (BSL) and basic safety objective (BSO).
2. It is ONR policy that a new facility or activity should at least meet the BSLs.   
   It is possible that older facilities may exceed one of more of the BSLs. While some BSLs are a legal limit which must be met, the BSLs of targets five to nine are not legally binding. However, ONR’s policy is that the level of gross disproportion in ALARP consideration should be very high and so inspectors should assume that it is highly likely that additional improvements to safety will prove reasonably practicable.
3. The BSOs form benchmarks that reflect modern safety standards and expectations. The BSOs also recognise that there is a level beyond which further consideration of the safety case would not be a reasonable use of ONR resources, compared with the benefit of applying these resources to areas of higher risk. Inspectors therefore need not seek further improvements from the designer/dutyholder but can confine themselves to assessing the validity of the arguments presented. The dutyholder, however, is not given the option of stopping at this level. ALARP considerations may be such that the dutyholder is justified in stopping before reaching the BSO, but if it is reasonably practicable to provide a higher standard of safety, then the dutyholder must do so by law.

|  |  |
| --- | --- |
| **Individual risk of death from accidents – any person on the site** | **Target 5** |
| The targets for the individual risk of death to a person on the site, from accidents at the site resulting in exposure to ionising radiation, are:  BSL: 1 × 10-4 pa  BSO: 1 × 10-6 pa | |

|  |  |
| --- | --- |
| **Frequency dose targets for any single accident – any person on the site** | **Target 6** |
| The targets for the predicted frequency of any single accident in the facility, which could give doses to a person on the site, are:  **Effective dose, mSv Predicted frequency per annum**  **BSL BSO**  2–20 1 × 10-1 1 × 10-3  20–200 1 × 10-2 1 × 10-4  200–2000 1 × 10-3 1 × 10-5  > 2000 1 × 10-4 1 × 10-6 | |
| **Individual risk to people off the site from accidents** | **Target 7** |
| The targets for the individual risk of death to a person off the site, from accidents at the site resulting in exposure to ionising radiation, are:  BSL: 1 × 10-4 pa  BSO: 1 × 10-6 pa | |
| **Frequency dose targets for accidents on an individual facility – any person off the site** | **Target 8** |
| The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site are:  **Effective dose, mSv Total predicted frequency per annum**  **BSL BSO**  0.1–1 1 1 × 10-2  1–10 1 × 10-1 1 × 10-3  10–100 1 × 10-2 1 × 10-4  100–1000 1 × 10-3 1 × 10-5  >1000 1 × 10-4 1 × 10-6 | |
| **Total risk of 100 or more fatalities** | **Target 9** |
| The targets for the total risk of 100 or more fatalities, either immediate or eventual, from accidents at the site resulting in exposure to ionising radiation, are:  BSL: 1 × 10-5 pa  BSO: 1 × 10-7 pa | |

# Advice to Inspectors

## Introduction

1. This section aims to provide guidance to all inspectors on the use of PSA and probabilistic insights. This guidance has been written for non-PSA specialists, to provide improved understanding of what PSA and QRA can reveal about risk, where ONR expects PSA to be performed, how PSA can be used by dutyholders to risk inform decision making and reduce risks ALARP, and how PSA and QRA can be used by ONR inspectors to aid risk informed regulatory decision making.
2. The following topics are covered:

* Section ‎5.2 – Overview of PSA
* Section ‎5.3 – What facilities should have PSA?
* Section ‎5.4 – Scope of PSA
* Section ‎5.5 – Interfaces with Other
* Section ‎5.6 – Use of PSA
* Section ‎5.7 – Limitations and uncertainty of PSA
* Section ‎5.8 – Quantification/presentation of results
* Section ‎5.9 – Comparison with numerical targets
* Section ‎5.10 – Probabilistic insights
* Section ‎5.11 – Applications for PSA insights in ONR

## Overview of PSA

1. At a high level, PSA is used to assess nuclear safety risks arising from initiating events and hazards. PSA is not usually used to produce security assessments or to analyse human-induced security threats such as sabotage or terrorism. However, the use of PSA to support security assessments is currently an area of research.
2. PSA is developed on a best-estimate basis. This means that the various inputs to the PSA, such as initiating event frequencies and failure probabilities of components and operators are selected to be as realistic as possible. Conservatism and optimism should be avoided if a PSA is to be used to inform decisions since conservatively evaluated contributors may mask the items that are really contributing to total risk. Avoiding conservatisms is also particularly important when the PSA is used to evaluate trade-offs. This is a different approach to DBA which often uses conservative assumptions to demonstrate the fault tolerance of a facility and the effectiveness of safety measures. DBA and PSA can often lead to different risk insights. A good safety case should combine the outputs from both PSA and DBA to demonstrate that risks are ALARP. Further information on DBA can be found in the DBA TAG [19].
3. PSA standards will commonly refer to level 1, level 2 and level 3 PSA.   
   These terms are typically defined in a light water reactor context, but other facilities can use similar concepts to define boundaries between different aspects of accident sequences if this is useful:

* Level 1 PSA refers to the part of the model which starts with initiating events and models accident sequences leading to core or fuel damage. Level 1 PSA ends with a set of plant damage states;
* Level 2 PSA starts with plant damage states and models the containment and the phenomena that occur following fuel damage. Level 2 PSA ends with a set of release categories/source terms.   
  For some reactor designs there may not be a clear dividing line between level 1 and level 2 PSA;
* Level 3 PSA starts with source terms and models the release of radioactivity into the environment and the effects of the radioactivity on humans and the environment.

1. Two significant aspects of PSA models are fault trees and event trees.   
   Fault trees are used to logically model safety functions, identifying the various combinations of failure modes (including operator actions) which lead to failure of the function. Fault tree development relies upon a good understanding of system design and operation, often informed by techniques such as Failure Modes and Effects Analysis (FMEA).
2. Event trees are used to logically model accident sequences, considering success or failure of all possible combinations of safety functions.   
   Typically the headings in an event tree are ordered chronologically, but this may not always be the case. The event tree logic is developed based on the effects on the overall facility after each safety function succeeds or fails.   
   The fault trees and event trees can be linked together so that dependencies between systems are accounted for when the PSA model is analysed. Further details can be found in the systems analysis section of SSG-3 [11].
3. QRA is often a simpler approach to assessing risk than PSA, typically utilising fault trees or event trees but not integrating the two together.   
   Fault tree analysis or event tree analysis may be carried out as part of a QRA. QRA does not typically consider aspects like uncertainties, common cause failures or human reliability to the same level of detail as PSA and does not typically cover the whole scope of plant, operating modes, hazards or initiating events.
4. For further details on the attributes of an adequate PSA refer to [2].

## What facilities should have PSA?

1. Figure 1 from the SAPs shows the frequency and consequence range where PSA can apply. It shows that PSA applies for all consequence and frequency ranges.

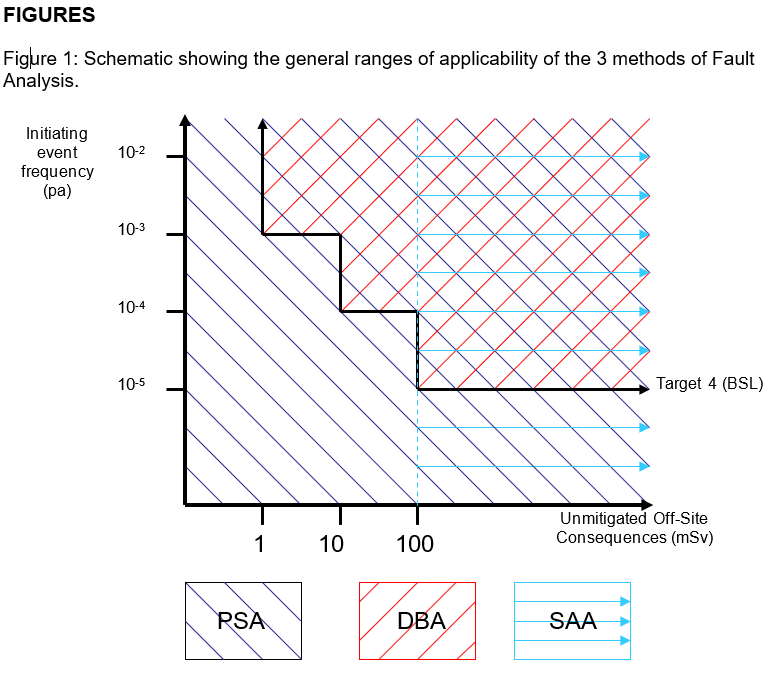


Figure 1: Ranges of applicability of methods of fault analysis.

1. The SAPs state the following three cases where a PSA should be provided:

* safety cases for power reactors
* where there is significant complexity
* where the numerical targets may be challenged

1. Safety cases for power reactors have been expected to provide PSA for many years, as power reactors are inherently complex with high potential consequences. For a power reactor, PSA is often the only technique that can identify complex dependencies between different initiating events, hazards, SSCs, operator actions and support systems.
2. The second bullet above refers to the complexity of the facility. For complex, high hazard facilities a combination of deterministic and probabilistic methods should be followed by the dutyholder (and reported in the safety case) to demonstrate the extent and effectiveness of the defence in depth provision included within a nuclear facility to ensure fault tolerance.
3. Other non-reactor facilities can also present significant complexity.   
   An inspector should consider whether typical DBA techniques are able to capture the dependencies between different initiating events, hazards, SSCs, operator actions and support systems. If it is doubtful that DBA is adequately capturing this information then the inspector should ask to see the PSA or QRA.
4. The third bullet above refers to potential for the risk from a facility to exceed the numerical targets in the SAPs. For non-reactor facilities which are unlikely to challenge the numerical targets, the development of a PSA is unlikely to be a proportionate expectation. This may be the case for facilities with small radiological inventories or simple passive storage of radioactive materials. Whilst dutyholders are free to develop a PSA if they wish to risk inform operation and decision making, it should not be a focus of regulatory attention. In the case of PSA this refers to numerical targets five to nine. Further guidance on numerical targets is provided in Section ‎5.9.
5. Some non-reactor facilities may not be amenable to PSA. For example, if the hazard is difficult to characterise due to significant uncertainty in the fault progression, then a PSA may not be able to provide a meaningful analysis. This may be the case for legacy storage facilities where the contents of the facility are unknown. In this case a dutyholder may wish to produce a bounding or screening analysis to highlight areas of uncertainty which may be able to be reduced through further research or analysis. Conversely even a simple QRA and associated sensitivity analysis can be used to identify risk significant aspects of a facility. Even unquantified fault trees can benefit dutyholders by improving understanding of systems and helping to identify vulnerabilities.
6. Facilities which do not meet any of the three criteria above and choose not to develop a PSA model may still choose to develop QRA or individual probabilistic arguments based on best-estimate data. This analysis can be used by licensees to provide a more realistic view of the risks from a specific fault or the best estimate reliability of a safety function or SSC. This can be helpful, for example when deterministic requirements have not been fully met, to support an argument that risks are ALARP or to identify proportionate improvements. Note however that these probabilistic arguments do not remove the requirement for adequate DBA. Inspectors can apply the guidance in the following sections in a proportionate manner to assess whether the probabilistic analysis has been produced in line with relevant guidance. Section ‎5.10 provides further guidance on use of probabilistic insights when a PSA model is not available.

## Scope of PSA

1. The scope of PSA should be appropriate for the facility and how the PSA is being used. For example, if the PSA model does not have adequate coverage of the aspects of the facility affected by a design change, then the insights obtained from it may be misleading. In this case, additional coverage should be added to the PSA model to ensure it covers the relevant parts of the facility. If this is not possible (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 or using a simpler quantified approach.
2. The scope of the PSA should be broad enough so that the results allow a meaningful comparison of risk from different aspects of the facility. If the scope is incomplete there is a risk that the insights from PSA will be skewed towards addressing aspects that have been modelled, at the expense of aspects which have not.
3. Complex new build facilities should aim to develop a full scope PSA in sufficient detail to risk inform the design and operation of the facility.   
   The scope and/or level of detail may be lower for existing facilities if they can argue that the effort to provide more detail would be disproportionate to the benefits obtained. Inspectors should satisfy themselves that any limitations in scope or detail are soundly based upon the hazard and complexity of the facility and the balance between the benefits of performing additional analysis and the cost of doing so.
4. When considering the scope and detail of PSA an inspector may consider the following. Although a non-PSA specialist may not be able to assess all these aspects by themselves, they should approach the PSA team for support where aspects such as these are under consideration:
5. In cases where there is currently no PSA, whether producing one would be worthwhile;
6. In cases where there is a PSA, whether the scope of the PSA model is adequate to inform the analysis being produced. The initiating events, hazards, SSCs, operator actions and support systems should be modelled in sufficient detail for the PSA results to be meaningful;
7. Whether the scope of the PSA is appropriate for the stage of the project. Expectations for the scope and level of detail of a PSA will increase as a project moves from GDA to licensing, permissioning and operation;
8. Whether the scope of the PSA covers all the sources of radioactivity on the facility. For a reactor site this should include the reactor core, fuel ponds, fuel handling facilities, waste storage tanks, etc;
9. Whether the scope of the PSA allows a meaningful comparison to be made with the numerical targets of the SAPs. Further information on numerical targets is provided in Section ‎5.9.
10. Whether the scope of the PSA covers all classes of initiating events and hazards. The range of frequencies of initiating events should be wider than that used for DBA (as low as 1 × 10-9 per year if the potential radiological consequences are high), so the inspector should confirm that initiating events and hazards are not being screened out based on a deterministic cutoff;
11. Whether there are different levels of conservatism for the analysis of different initiating events, for example the seismic PSA may be more conservative than the internal events PSA;
12. Whether the scope of the PSA covers all foreseeable operating modes of the facility;
13. 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;
14. Whether there are any multi-unit considerations that should be accounted for in the PSA.
15. While these questions are useful for considering the outputs from a whole PSA, often an inspector will come across a much smaller scope of PSA linked to a single change in operation or a single modification. In this case similar questions are applicable, but the expectations may be reduced compared to those above. For example the scope and detail of the PSA would only need to be adequate to model the systems, dependencies and risks associated with the systems undergoing change or modification.

## 

## Interfaces with other specialisms

1. PSA relies on inputs from many other specialisms, and the outputs from PSA can be useful to other disciplines. Figure 1 from the latest version of SSG‑3 lays out six high level aspects of PSA development [11]. These are shown in Table 1, along with examples of ONR specialisms that interface with PSA when these aspects of a PSA are assessed.

Table 1: Interfaces between PSA and other disciplines

| IAEA analysis area | ONR specialisms involved | Comments |
| --- | --- | --- |
| Initiating Event Analysis | Fault Studies  Internal Hazards  External Hazards  Fuel and Core/ Radiation Protection/ Criticality | Fault studies may support assessment for many initiating events.  Hazards may support assessment of internal and external hazards that can lead to initiating events occurring within the facility.  Fault studies/fuel and core/radiation protection and criticality may assess the likelihood of core mis-loading and criticality faults. |
| Human Factors | Human factors may support assessment of type A and B human error probabilities which may cause initiating events (refer to Section ‎5.6.9) |
| Electrical Control & Instrumentation (EC&I) | Control & instrumentation may assess spurious initiation of C&I systems  Electrical may support assessment of faults related to loss of offsite power and onsite power supplies |
| Mechanical Engineering | Mechanical engineering may support assessment of mechanical handling faults such as dropped loads |
| Accident Sequence Analysis  Supporting Analyses | Fault Studies | Fault Studies assess transient analysis that informs level 1 PSA, though it is often conservative if used for DBA. If the same analysis is used for DBA and PSA, ONR should ensure the analysis is not overly conservative for PSA purposes.  Fault Studies may support assessment of severe accident analysis which is an input to Level 2 PSA analysis |
| Radiological Consequences | Radiological consequences may support assessment of level 3 PSA analysis |
| Radiological Protection | Radiological protection may support assessment of worker risk analysis if it is produced |
| Human Factors | Human factors may support assessment of claims made on operators to respond to faults.  Human factors carry out task and error analysis to determine what tasks are needed and how they may fail.  The use of emergency operating procedures and severe accident management guidelines are assessed by human factors inspectors. |
| Internal Hazards  External Hazards | Internal and external hazards assess the potential for events to escalate as a result of the impact of hazards on lines of protection. |
| System analysis (including passive systems and computer-based systems) | Fault Studies  Mechanical Engineering | Fault studies and mechanical engineering are often involved with assessment of active and passive systems, especially the thermal-hydraulic analysis of cooling systems.  Fault studies may support assessment of systems designed to mitigate severe accidents |
| Control & Instrumentation (C&I) | C&I may assist with assessments of C&I systems, especially where claims are made on software reliability. |
| Internal Hazards  External Hazards | Internal and external hazards are often involved in the characterisation of hazards and the impact of those hazards on active and passive systems. |
| Human Reliability Analysis | Human Factors | Human factors will assess the qualitative aspects of task analysis, while PSA will focus on the quantitative aspects.  Human factors carry out task analysis to identify potential errors and performance shaping factors. They use these to estimate the reliability of human based safety claims that are modelled in the PSA. |
| Data and Common Cause Failure Analysis | Mechanical Engineering  Electrical Engineering  Control & Instrumentation (C&I) | Data can be sourced from generic industry sources, fleet data or station specific data. Mechanical, Electrical and C&I may support assessment of data sources. |

## Use of PSA

1. Dutyholders may use the information and insights from their PSA models to risk inform many of their decisions. The following sections provide an overview of how PSA may be used by a dutyholder, and the aspects inspectors should expect to see.

### Design/modifications

1. SAP FA.14 states that PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities [1]. PSA should be used from as early in the design/modification process as possible. PSA can be used to optimise the design of systems and modifications during the design process. Where optioneering is taking place, PSA can be used to provide an input to the process by quantifying reliability, sensitivity and risk from the modification. For example PSA can be used to understand:

* the risk profile of the plant being designed
* the risk impact of a modification
* which SSCs are most risk significant
* which SSCs become risk significant or risk insignificant if input data or assumptions change (for example, change in classification or design specification)
* whether an SSC has the correct classification from a radiological risk perspective
* whether severe accidents have been practically eliminated on a frequency basis
* the effectiveness of severe accident mitigation measures such as containment venting
* the effectiveness of off-site countermeasures

1. 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.
2. The level of detail in the PSA model should be consistent with the design information available. If the design is in an early development phase the PSA can be high level and simplified to mirror the information available and to allow for iterations of the PSA to be quick to produce to risk inform the design as it is developed. When more detail is available the PSA should be updated. This can lead to an iterative process which results in the PSA model being sufficiently realistic to inform the decisions required of it.
3. The quantification and presentation of results from the PSA allow dutyholders and inspectors to gain a risk-informed view of a design or modification. Further details on quantification and presentation of results are found in Section ‎5.8.
4. ONR’s TAG on PSA provides additional guidance on the technical adequacy of PSA applications [2]. SSG-3 provides guidance on the use of PSA for design evaluation [11].

### Safety case and ALARP

1. The SAPs state that the risks from a facility should be balanced, such that no single class of accident makes a disproportionate contribution to the overall risk [1]. The guidance in the SAPs is aimed at new facilities and applied to existing facilities on a proportionate basis.
2. There are two places in the SAPs which refer to balancing risk and the use of factors of one-tenth of total risk. Paragraph 646 states:

“PSA should assist the designers in achieving a balanced and optimised design, so that no particular class of accident or feature of the facility makes a disproportionate contribution to the overall risk, e.g. of the order of one tenth or greater. PSA should enable a judgement to be made of the acceptability or otherwise of the overall risks against numerical targets 5 to 9 and should help to demonstrate that the risks are, and remain, ALARP.” [1]

1. In this context a class of accident may be ‘electrical faults’ or ‘reactivity faults’. Typically there may be approximately ten classes of accident for a facility. The use of one tenth in this paragraph is intended to provide an example of using PSA to balance the risks from the design. This is not a requirement. Inspectors should use the results of the PSA to understand if the design is balanced and risks have been reduced ALARP, and if not they should ask the dutyholder to justify why their design is acceptable.
2. PSA can be used to help demonstrate this based on charts such as Figure 2. Typically some classes of faults will be more risk significant than others. Inspectors should focus more effort on faults that contribute a greater amount of risk and seek to understand if there are any practicable means to reduce these risks.

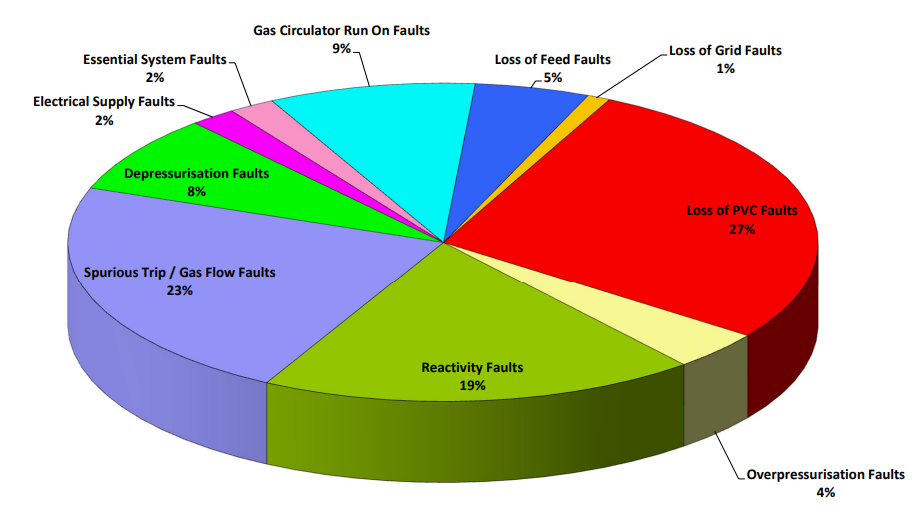


Figure 2: Example of balance of risk of failure to trip from fault groups for an advanced gas-cooled reactor (AGR).

1. Paragraph 749 of the SAPs, linked to target 8, states:

“The risks from the facility should be balanced; that is, no single class of accident should make a disproportionate contribution to the overall risk, e.g. of the order of one tenth of the frequency targets for each dose band.” [1]

1. In this case the frequency target referred to is the BSL associated with target 8. This is relevant to PSA, but also for any other analysis used to compare risk against target 8. This prompt to demonstrate that no class of accident contributes greater than one tenth of the BSL is most relevant to legacy facilities which can present higher risks than a typical new build facility. Inspectors should pay extra regulatory attention to facilities where a single accident group is contributing greater than one tenth of the BSL as it could indicate that risks are not well controlled.
2. When a dutyholder makes an ALARP argument they are stating that the time, trouble and money to reduce risks further are grossly disproportionate to the benefits gained from the risk averted. PSA can be used to inform these arguments by quantifying the overall level of risk and the change in risk from potential modifications.
3. Deterministic, engineering, operational and other factors also need to be considered. The PSA may identify an option as being the one that reduces risk the most, but if it has other drawbacks such as being difficult to commission or operate, would take longer to realise the risk benefit, rely on novel or untested technologies etc. then another option which the PSA shows is second best may be the better choice.
4. Dutyholders should not use artificial limits in a PSA, such as a limited claim on the reliability of a C&I system in line with its classification or a Common Cause Failure cutoff, as a justification for not implementing risk reduction measures because no benefit would be seen in the PSA results.
5. PSA cannot be used to argue that risks have been reduced ALARP in isolation. The question of whether any reasonably practicable improvements could be made still stands It is not sufficient for a dutyholder to state that the PSA shows the risk is low, or below a target such as the BSO, and therefore ALARP. However, inspectors may choose to focus less regulatory attention on risks that are below the BSO.
6. ONR have produced TAG 5 on ALARP [20]. The TAG recommends that PSA is produced for systems with significant hazards or complexity, as outlined in Section ‎5.3 of this TAG. It provides further details on the different factors to weigh up when considering arguments that risks are ALARP. There is also discussion of cost-benefit analysis, which PSA is uniquely placed to support by quantifying the risk side of the equation. Arguments that risks are ALARP need to consider all types of risk, not just nuclear/radiological ones, so PSA may not be able to contribute to all aspects of an ALARP argument.

### Living PSA

1. The PSA model should be kept ‘living’. This means the PSA should be kept up to date with modifications to the plant, and the data in the model should be based on the operating experience from the real facility. The PSA should also be updated during periodic reviews of safety to provide an overview of the risk from the facility. The IAEA have produced a document reflecting best practice for keeping a PSA living [21]. The IAEA define a living PSA as follows:

“A ‘living PSA’ (LPSA) can be defined as a PSA of the plant, which is updated as necessary to reflect the current design and operational features, and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysts’ assumptions in the absence of such information.” [21]

### Risk monitors

1. Once a facility has a good quality PSA, the dutyholder can use it to develop a risk monitor. A risk monitor allows the operator of a facility to calculate the risk for the exact configuration that the plant is in, considering the operating mode and any equipment that is out of service. While the normal result from a PSA is an annual risk averaged over the full range of plant states, the risk calculated with a risk monitor is the point in time risk based on the plant configuration at the time. This means that normal time at risk factors, for example the plant operating at power for 90% of the time, are removed from a risk monitor. Weather conditions and other activities can be accounted for in the risk monitor model to indicate an increase of certain initiating events, such as risk of trip due to loss of grid, or seawater intake blockage.
2. The status of the plant in the risk monitor is kept live based on the component availability on the real facility. High level overview screens are available within the risk monitor which can quickly show operators the current plant status. The risk monitor interface can also display the status of the deterministic defence in depth levels of protection, relating to key safety functions.
3. Risk monitors can be used to support outage and maintenance planning. The risk level associated with the different plant configurations can be viewed ahead of time and the risk peaks smoothed out by altering the outage configurations. The information derived from the risk monitor should be supported by deterministic considerations of risk to obtain a risk profile that is ALARP.
4. Not all components are modelled in PSA models. In these cases, a representative component will be selected in the PSA model to ensure the availability of a system reflects the plant state.
5. Inspectors who are presented with outputs from risk monitors should consider the following:

* is the operating mode of the reactor adequately modelled in the underlying PSA for the risk monitor to be accurate?
* Are all required configurations captured, for example, interconnectors?
* are the procedures at the station clear on where the risk monitor can and cannot be used?
* are the procedures at station clear on actions required following the risk monitor evaluation?
* how are the risk thresholds derived?

1. At Heysham 2, Torness and Sizewell B the risk monitor is used in the day to day running of the station. The two main applications are instantaneous configuration risk management by control room staff, and long, medium- and short-term forward planning of maintenance activities to smooth out avoidable risk peaks and reduce risks ALARP. The current risk level as shown by the risk monitor is additionally used to provide site-wide awareness, for example, in daily briefings.

### Classification and categorisation

1. Categorisation and classification is primarily a deterministic process, with guidance provided in ONR’s TAG on the categorisation of safety functions and classification of structures [22] and IAEA safety guide, SSG-30 [23]. PSA can provide additional insights and an alternative point of view to review whether the categorisation and classification scheme at a facility has produced a consistent and appropriate outcome. By reviewing the results from the PSA against the classification of the components a dutyholder can see if there are components that may have been under or over classified on a risk informed basis.
2. PSA should model all the systems that would be used following a fault on a realistic basis. This includes lower classified and non-classified systems.   
   The PSA results can be used to compare risk insights to classification.
3. For example, if the results from the PSA show that a lower classified or non-classified system is risk significant, then the classification of that system should be reviewed to establish if increasing the classification would provide a risk benefit (for example, by increasing the overall quality of installation, commissioning, examination, maintenance, testing and inspection (EIMT)).
4. PSA can also be used to challenge over-classification. For example, if a system has been defined as a class 1 system, but the PSA indicates the risk significance of the system is low, then the inspector may want to confirm that effort is being expended in the correct area. PSA sensitivity studies can be used to show the risk level if the reliability of the system were an order of magnitude better or worse, or if the system was unavailable. Refer to Section ‎5.8 for more details of results and sensitivity studies.

### Off-site planning and radiological consequences

1. ONR’s TAG on radiological analysis provides information on assessment of radiological consequences [24]. It notes that there are large sources of uncertainty related to the calculation of radiological releases. Where the calculation is being used to support PSA, the assumptions made should be best estimate rather than conservative.
2. The PSA can be used to inform the likelihood and level of harm from a facility. This information can be used as inputs into the REPPIR process detailed in the REPPIR Approved Code of Practice (ACOP) [25]. Where a level 2 PSA is available the source term of different accidents will be developed. Where a level 3 PSA is available this can provide details of the effects of radiological releases on the population and environment around a facility and inform the development of emergency planning zones. The level 3 PSA can show the effects of countermeasures (such as sheltering and evacuation) on the expected consequences to the population.

### Examination, inspection, maintenance and testing (EIMT) optimisation

1. PSA can inform updates to EIMT schedules. The PSA should be of appropriate quality and be suitable for the application. The PSA owner should go through a process of assuring that the PSA has suitable quality and realism for situations that may arise in the proposed application.   
   The ASME/ANS Level 1 standard provides further discussion on this [14]. When reviewing EIMT updates based on PSA an inspector should consider:

* has the dutyholder demonstrated an adequate understanding of the risk profile of their plant, including the relative importance of individual systems/components?
* does the time, trouble and cost associated with the EIMT of each system align with its relative importance?
* is there a recognition that PSAs generally use a simple model, where the component unavailability is calculated by multiplying a failure rate by the time since last test, resulting in a sawtooth shape for the unavailability as a function of time[[2]](#footnote-3)? The results should be interpreted with this in mind.
* is the modelling of components adequate to allow valid conclusions to be drawn?
* is the component failure data of the components under consideration based on representative station data or generic data?
* has the impact on Common Cause Failures been considered?
* have the totality of the proposed changes been considered, as opposed to “salami-slicing” of risk by considering each adjustment individually?
* Has the dutyholder adequately considered other (non-probabilistic) factors when making updates to the maintenance schedule, including:
  + statutory requirements
  + manufacturer recommendations (which may not be best-estimate or may be affected by commercial considerations)
  + Impact of the changes on test regime of linked plant components
  + operational experience held for plant items – are they prone to failure or considered to be reliable and potentially over tested?
  + is there confidence that reduced test intervals will not significantly reduce the overall reliability of the system?
  + Impact on plant of stop/starting
  + Maintenance induced errors.

### Technical specifications

1. Complex facilities, such as nuclear power plants, often use technical specifications to control plant availability in different states. The PSA can be used to inform and maintain the technical specifications, for example by:

* determining their plant availability requirements during different operating states
* informing the time allowed with reduced plant availability (often called action completion times) to inform technical specifications
* optimising technical specifications developed on a deterministic basis by reviewing the risks associated with unavailability of systems in different configurations
* using PSA or risk monitor results to differentiate between high risk and low risk states and allow for different action completion times depending upon the risk levels
* using PSA to risk inform the response to rare or unexpected plant states, for example amending the technical specifications to reflect long term plant item unavailability

### 

### Claims on operators

1. As noted in ONR’s TAG on human reliability analysis [26] there are three types of operator action:

* Type A human actions (pre-initiator human error). These are human actions performed during EIMT activities, including calibration, where human error can result in an SSC being unavailable to perform its safety function on demand, or with significantly reduced capability;
* Type B human actions (initiating event human errors). These are human actions performed during normal operations or maintenance where human error can lead to the initiation of a fault sequence;
* Type C human actions (post-initiator human errors). These are human actions performed to prevent, protect against or mitigate the consequences arising from an initiating event. Post initiator human errors can result in an operator action failing to achieve the required safety function.

1. PSA models may include all three types of operator actions. By analysing the PSA, the relative significance of operator actions can be determined. This information should be used by the dutyholder to inform safety case updates and operations.
2. When reviewing risk information related to claims on operators inspectors should consider:

* does the safety case documentation highlight the importance of specific operator actions?
* are risk significant operator actions adequately supported by human factors task analysis, both qualitatively and quantitatively?
* has there been adequate communication with the training department to check that the risk significant actions are understood by facility staff and are trained accordingly?
* are risk significant operator actions highlighted in station operating procedures and labelled as claimed actions and are they adequately clear?

## Limitations and uncertainty of PSA

1. All PSA models will have limitations and conservatisms, such as in scope, depth or detail. Inspectors should be aware of any limitations when using PSA to risk inform their activities or understand how PSA has been used to risk inform dutyholder activities.
2. The limitations associated with PSAs can affect interpretation and use of insights from the PSA. Where PSAs have significant limitations, interpretation of their results and their use in the decision-making process should be done in a cautious way. Inspectors should approach the PSA team for advice as required.
3. Some examples of common limitations in PSA models include:

* only modelling specific operating states – for example, ‘at power’ only
* Not including all sources of radioactivity – for example, Fuel Route
* scope of initiating events – for example, some PSAs focus on ‘internal events’ and have limited consideration of internal or external hazards
* not considering fault progression beyond a certain timeframe –   
  for example, if a fault allows over 24 hours for operators to respond, this may be screened out of some PSAs
* simplistic system modelling – for example, not all systems may be modelled to the same level of detail. This is particularly common when comparing C&I systems to mechanical systems
* asymmetric modelling – whereby all faults of a particular type are assumed to occur in a single division, for example all boiler tube leaks occur in quadrant A
* inclusion of maintenance states – for example, some PSAs model ‘all plant available’ and optimistically ignore any unavailability caused by routine maintenance
* operator errors – for example, some PSAs contain limited consideration of operator induced errors that cause a fault or affect response to a fault, such as incorrect system alignment following maintenance which can produce a latent error which is only revealed when that system is demanded later
* repairs are often not modelled due to uncertainty over how long repairs would take following a fault. This is a source of conservatism in most PSA models
* component failure data – this is often based on generic or fleet-based data which may not take into account specific aspects such as the age or novelty of a component
* underlying transient analysis – this may be based on the transient analysis used to support the DBA with conservative initial conditions used. This can be difficult for inspectors to identify without access to the underlying analysis

1. PSA is also subject to uncertainty. It is important for an inspector to understand the sources of uncertainty that may be present in a PSA. WENRA produced an explanatory note on PSA which provides an overview of the different types of uncertainty in PSA [3] which is summarised in this section.
2. Within a typical PSA each probability parameter assigned to the various components will have an associated uncertainty. The PSA software can then carry out Monte Carlo simulations to calculate the uncertainty of the overall result. Inspectors should remain aware that this uncertainty only represents one contribution to the total uncertainty in a model.
3. Major sources of uncertainty related to the way the PSA is modelled (which may or may not be quantified include):

* how initiating events are grouped
* the choices of scenarios and models for the supporting thermohydraulic and neutronics calculations
* the uncertainties related to knowledge of the phenomena
* the uncertainties related to the modelling of human actions
* the uncertainties related to the simplified modelling and the estimation of software reliability
* the uncertainties related to the estimation of the reliability of equipment operating beyond its qualification conditions
* the uncertainties related to the choice of probabilistic methods (for example how the PSA model is assembled and analysed)

1. It is expected that the owner of the PSA should systematically record the uncertainties related to each PSA task. The overall aim is that model developer should have a good understanding of uncertainties and limitations and what model elements they might affect to be in a good position to assess suitability for a particular application.
2. The PSA often makes visible the uncertainties and limitations that otherwise would be hidden behind deterministic assumptions. Therefore, it is important that all possible contributions from different kinds of safety analysis can be integrated into a consistent overall picture.

## 

## Quantification/presentation of results

1. Whilst a PSA inspector may be comfortable accessing the PSA models of a dutyholder to directly quantify and extract the PSA results, it is not expected that other inspectors will require this level of access or familiarity with PSA software. In order to present the results of a PSA to a wider audience dutyholders should write reports that are accessible and understandable by non-PSA specialists. This section provides an overview of the results that may be presented within a typical PSA report. It is not expected that a non-PSA specialist would use these in detail, but by providing this overview it allows non-PSA specialists to recognise these terms and ask for support from PSA specialists where required.
2. There are many types of results that can be presented in a PSA report, for example:

* minimal cutsets (MCS)
* dominant sequence reviews (DSR)
* fault tree analysis (FTA)
* event tree sequence analysis
* consequence analysis
* importance listings
* graphs and charts
* doseband staircase comparison with target 8

### Minimal cutsets

1. MCS are the minimum number of failures required to lead to a consequence. There are three main ways that MCS are produced in PSA:

* In fault trees MCS represent the combinations of failures that cause failure of the top gate;
* In event trees MCS represent the underlying failures of components (feeding in from contributing fault trees) which lead to a specific consequence in the tree following a certain initiating event;
* Event Tree sequences with the same consequence can be combined to form a consequence analysis. The individual MCS lists are merged.

1. For example, following a loss of offsite power the minimal cutset leading to an offsite release may be as follows:

|  |  |  |
| --- | --- | --- |
| Loss of Offsite Power without recovery | Failure of Main Diesel Generators | Failure of Backup Diesel Generators |

1. PSA reports will often include MCS listings as appendices, but these can be hard to interpret unless the reader is familiar with the PSA model in question. Authors of PSA reports should assist their readers by writing discussion of the top MCS in prose. This is also a good place to discuss any limitations or assumptions that are contributing to the results.

### Dominant Sequence Reviews (DSRs)

1. A DSR is an output from a PSA where the event tree sequences leading to a particular consequence are ordered by frequency. This approach may also be referred to as a review of risk significant sequences. Typically, this is done for significant sequences leading to core damage or offsite release.   
   For each sequence there is then a discussion where any optimisms or conservatisms are noted. This can also form part of a review where suggestions for measures to reduce the risk to ALARP can be noted on a sequence-by-sequence basis. These reduced risks can be quantified by hand calculation or by modifying the PSA model. A similar approach can be used to look at the dominant minimal cutsets for a given consequence.

### Fault Tree Analysis (FTA)

1. FTA refers to the practice of taking the fault trees from part of a PSA model (for example, a system, safety function or support system) and reviewing them in isolation to gain insights about the system. FTA is typically found in PSA reports relating to modifications. During the design and optioneering stage of modifications the PSA can be used to identify the risk significant failure modes of a system. These results are typically presented as MCS and importance listings. The overall failure probability of the system is also quantified. Any limitations in the PSA model should be accounted for by the dutyholder when carrying out FTA.

### Importance analysis

1. The PSA model can be quantified to produce importance listings for a particular fault tree, event tree sequence or consequence. There are multiple types of importance analysis. These are typically generated for basic events. A basic event is the simplest building block of fault trees in a PSA model. They are typically used to represent failure modes of components, operator actions, initiating events and maintenance states. With some additional processing, importance listings can be produced for operator actions   
   (in order of importance), the most important systems or the most significant faults. The following are some types of risk importance measures that may be found in PSA results:

* Fussell Vesely (FV) – This is a ratio of the risk contribution from MCS that contain a given basic event divided by the total risk. For example, if the MCS associated with loss of grid contribute 60% of total risk, the FV importance measure would be 0.6. Fractional Contribution is a similar importance measure to FV which typically has a similar numerical value. These can be used to highlight systems where an increase in reliability would be most valuable;
* Risk increase factor (RIF) – This importance measure is assigned to basic events. It presents a factor of increase in the overall risk if the basic event of interest was always failed. For example, if a particular valve was completely unreliable (i.e. failure probability of 1) and this led to a doubling of core damage frequency (CDF) the RIF would be 2. This factor is also known as Risk Achievement Worth. These can be used to highlight systems/ components which already have high reliability, but the consequence of failure is very significant;
* Risk decrease factor (RDF) - This importance measure is assigned to basic events. It presents a factor of decrease in the overall risk if the basic event of interest was always available. For example, if a particular initiating event was designed out so that it could not occur (failure probability of 0), and this led to a halving of CDF the RDF would be 2. RDF is proportional to FV, so it does not typically lead to additional insights being gained from the PSA;
* Sensitivity high and low – These importance measures show the overall risk if a given basic event failed ten times more frequently or ten times less frequently. This can provide feedback on which aspects of a system are particularly sensitive to the reliability values assigned to them.

### Charts

1. Charts can be used to provide visual summaries of PSA results.   
   Examples include pie charts to show the different contributors to different consequences and comparisons against numerical target 8 using a ‘doseband staircase’. These can provide a visual comparison against the BSO and BSL for target 8. Inspectors should seek to focus more attention on risks that are above the BSO rather than below it. Refer to Section ‎5.9.3 for details of target 8 and doseband staircases.

### Metrics

1. PSA Results are often related to metrics which are set within a dutyholder’s arrangements. For example, CDF or fuel damage frequency (FDF) are typically quantified by a level 1 PSA. Some dutyholders will specify a target for CDF/FDF that their design should meet.
2. A level 2 PSA can calculate a large release frequency (LRF) and a large early release frequency (LERF). Targets are often set around these metrics by dutyholders, typically one or two magnitudes lower than their CDF target. ‘Early’ typically refers to accidents which happen fast enough that off-site countermeasures such as sheltering and evacuation are not possible.
3. Some dutyholders use ‘dosebands’ to describe the radiological consequences of accident sequences, for example from the advanced gas-cooled reactor (AGR) power stations. A doseband is based on the dose received offsite by a member of the public and is calculated separately, outside the PSA. The use of dosebands means that the AGR PSAs have a pseudo level 1/2/3 PSA within a single event tree. The dosebands align to the bands in numerical target 8 as follows:

Table 2: AGR dosebands

|  |  |
| --- | --- |
| Doseband | Offsite dose (mSv) |
| 0 | <0.1 |
| 1 | 0.1-1 |
| 2 | 1-10 |
| 3 | 10-100 |
| 4 | 100-1000 |
| 5 | >1000 |

## Comparison with numerical targets

1. PSA can be used by dutyholders to calculate different results such as system reliability, sequence frequency, CDF etc. that can be used to risk inform design and operation. However, another important use of PSA is to compare the risk levels from a facility against the numerical targets in the SAPs.
2. Some dutyholders choose their PSA outputs to align with the numerical targets from the SAPs. However not all duty holders do this and some dutyholders only produce PSA results that can be compared to a particular target, so some additional analysis or interpretation may be necessary to compare against other targets. However the PSA results should be presented in a way to allow comparison with the numerical targets as noted in [2].
3. Assessors should take a proportionate approach to assessment based on the level of risk presented by a site. If the risk is near to or above the BSL then more attention should be paid to the site. The level of attention paid to the PSA and the assumptions and uncertainties that underpin it will also require more attention. If the risk is below the BSO then less attention may be able to be paid. Attention should be paid to the scope and limitations of the PSA when making this judgement.
4. The numerical targets relevant to PSA are based upon radiological consequences. Whilst not unique, this is relatively uncommon internationally. Many other regulatory regimes have a CDF or LRF target, therefore PSAs developed internationally or applying international codes and standards may present results for CDF and LRF. This does not align directly to any of the ONR targets but can provide a useful point of comparison with other assessments. A CDF target of 1 × 10-5 per reactor year is applied in many other regulatory regimes [27]. A LRF target of 1 × 10-6 per reactor year is also typical.

### Targets 5 and 6

|  |  |
| --- | --- |
| **Individual risk of death from accidents – any person on the site** | **Target 5** |
| The targets for the individual risk of death to a person on the site, from accidents at the site resulting in exposure to ionising radiation, are:  BSL: 1 × 10-4 pa  BSO: 1 × 10-6 pa | |
| **Frequency dose targets for any single accident – any person on the site** | **Target 6** |
| The targets for the predicted frequency of any single accident in the facility, which could give doses to a person on the site, are:  **Effective dose, mSv Predicted frequency per annum**  **BSL BSO**  2–20 1 × 10-1 1 × 10-3  20–200 1 × 10-2 1 × 10-4  200–2000 1 × 10-3 1 × 10-5  > 2000 1 × 10-4 1 × 10-6 | |

1. Targets 5 and 6 are written to assess worker dose. PSA can be an input to support assessments of submissions related to target 5 and 6 but PSA is not usually the basis of the submission. PSA can be used by dutyholders to identify the operator actions that may be required following faults. Targets 5 and 6 are typically assessed by radiological protection specialists, with support from PSA specialists where necessary. The radiological protection TAG provides more information [24].
2. Some dutyholders have made the argument that for facilities with low core damage frequencies a simple assumption may be made that the probability of a fatality following core damage is one. If the CDF is low enough the BSO may be met, even with this conservative assumption. The requirement on dutyholders to reduce risks ALARP remains even where the BSO is met.

### Target 7

|  |  |
| --- | --- |
| **Individual risk to people off the site from accidents** | **Target 7** |
| The targets for the individual risk of death to a person off the site, from accidents at the site resulting in exposure to ionising radiation, are:  BSL: 1 × 10-4 pa  BSO: 1 × 10-6 pa | |

1. Numerical target 7 relates to site-wide risk, and therefore assessment against this target should include consideration of all facilities on the site.   
   A complete best-estimate comparison against target 7 requires a level 1, 2 and 3 PSA to be produced for all relevant facilities. However, most dutyholders for existing facilities will not provide this level of information and will make conservative assessments based on bounding cases. Often a comprehensive level 3 PSA is not available, and licensees will show results against target 8 instead. Best-estimate level 3 PSA is expected for complex new build facilities such as new build NPPs.

### Target 8

|  |  |
| --- | --- |
| **Frequency dose targets for accidents on an individual facility – any person off the site** | **Target 8** |
| The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site are:  **Effective dose, mSv Total predicted frequency per annum**  **BSL BSO**  0.1–1 1 1 × 10-2  1–10 1 × 10-1 1 × 10-3  10–100 1 × 10-2 1 × 10-4  100–1000 1 × 10-3 1 × 10-5  >1000 1 × 10-4 1 × 10-6 | |

1. The SAPs note that “the risks from the facility should be balanced; that is, no single class of accident should make a disproportionate contribution to the overall risk, for example, of the order of one tenth of the frequency targets for each dose band”. As discussed in Section ‎5.6.2 this refers to the BSL rather than the BSO.
2. As shown in Figure 3, target 8 forms a staircase, often known as a doseband staircase. Licensees such as the AGR power stations may combine their radiological consequences with their level 1 PSA to produce a frequency for each doseband which they display on the doseband staircase. This can provide a clear view of where risks are most in excess of the BSO/BSL. Assessors should consider focussing more effort on these areas.   
   Inspectors should note where multiple accident frequencies are assigned to the same dose level on the staircase, for example the risk from fuel route and reactor operations may be shown as separate points on the staircase. The risks from these should be combined to compare with the target, although inspectors should consider the information in the TECDOC from IAEA on risk aggregation [28].

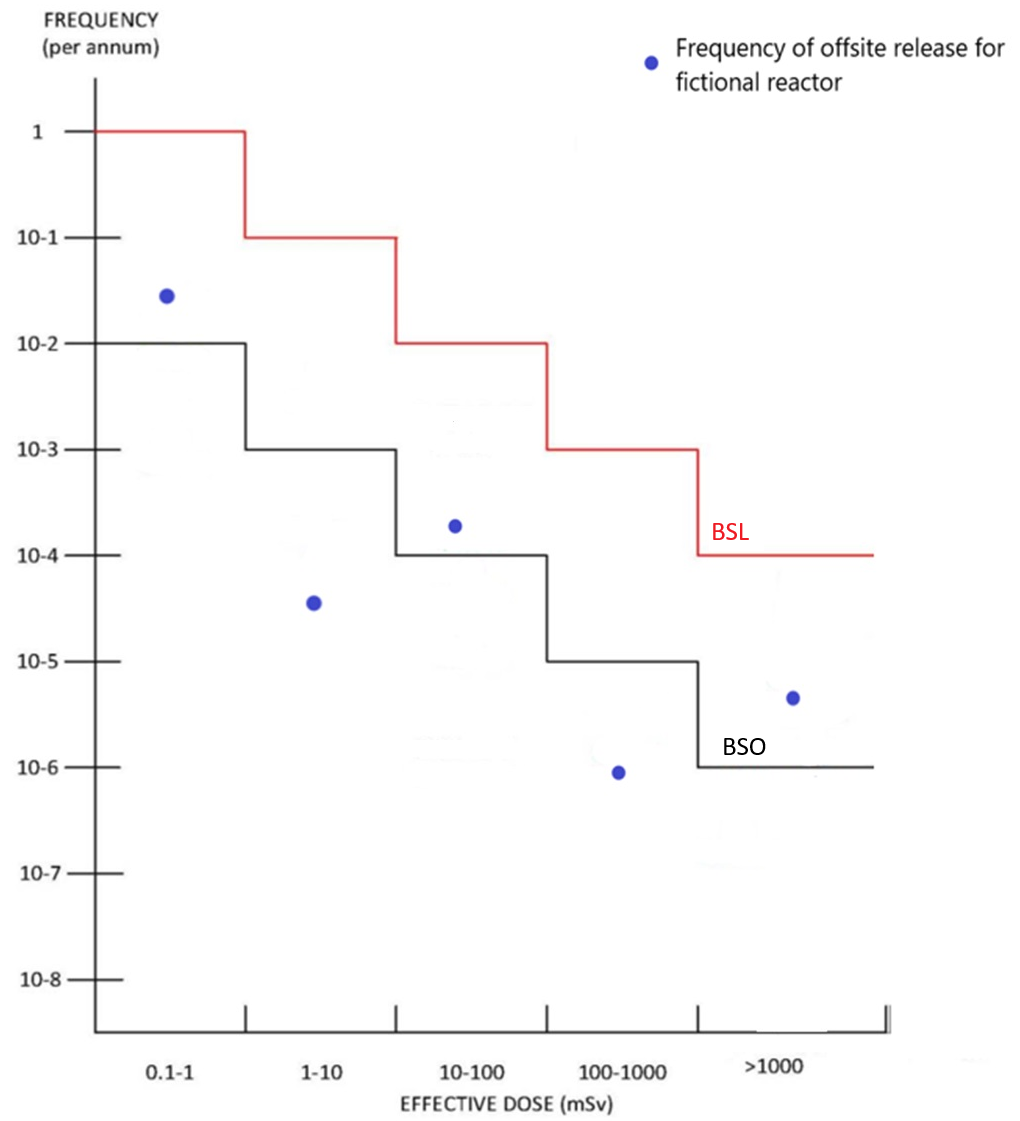


Figure 3: Target 8 doseband staircase

1. The BSL and BSO represent ONR policy and are used to focus regulatory attention on areas where risks are least well controlled. The requirement for risk to be ALARP is a legal requirement that applies everywhere on the doseband staircase.
2. While the expectation is for PSA to be best estimate throughout levels one, two and three, there may be deterministic requirements to produce a more conservative analysis for comparison with target 8. For example the expectation in the SAPs that the person should be assumed to remain directly downwind of the release point for the duration of the release is a conservative approach.

### Target 9

|  |  |
| --- | --- |
| **Total risk of 100 or more fatalities** | **Target 9** |
| The targets for the total risk of 100 or more fatalities, either immediate or eventual, from accidents at the site resulting in exposure to ionising radiation, are:  BSL: 1 × 10-5 pa  BSO: 1 × 10-7 pa | |

1. The results of a level 3 PSA can be used to estimate the frequency of accidents leading to 100 or more fatalities. This may be formed from a mixture of stochastic and prompt deaths. For complex new build facilities, level 3 PSA is expected and considered to be relevant good practice. Previously some requesting parties have made a simplifying assumption that any large releases will lead to >100 fatalities and shown that the target is met due to a low large release frequency. This may be proportionate for designs that do not have a site identified or where risks are low.
2. Level 3 PSAs are often produced for light water reactors where the dedicated containment building can lead to different releases to the environment depending on the propagation of the initial fault through core damage and containment failure. Simpler approaches that combine level 1 PSA with radiological consequences may be suitable for facilities without dedicated containment.
3. Level 3 PSA is not always carried out by licensees operating existing facilities. Where this is the case, an inspector should expect an equivalent calculation that quantifies the harm to off-site populations if a level 3 PSA is absent.
4. For nuclear facilities with small inventories of material, or which present low risks, it may be simple for dutyholders to demonstrate that targets 7 and 9 are met, even with conservative assumptions. A detailed PSA model may not be required for this. However, target 8 includes a range of consequence levels from 0.1mSv up to >1000mSv. Many nuclear facilities are likely to have faults within this range. However, the work required to develop a PSA may still be considered disproportionate if the target 8 risks are expected to be below the BSO. Section ‎5.3 discusses what facilities should have a PSA.

## Probabilistic insights from quantitative analysis

1. Non-reactor facilities may not have full scope PSA models available.   
   This may be because they are legacy facilities which were constructed prior to the development of PSA techniques or because they are simple facilities where it would not be proportionate to develop a full PSA.
2. It is expected that quantitative analysis will have been carried out to support the design and operation of these facilities. The same information that is used to support PSA modelling can also be used for simpler techniques such as reliability modelling. Much of the guidance from this TAG is still applicable to quantitative analysis.
3. The guidance in the sections above is applicable to many aspects of quantitative analysis. Where quantitative analysis has been produced for a facility inspectors should consider:

* on what basis has the analysis been produced – conservative or best-estimate
* how appropriate the data sources are where data has been used to support the calculations
* how the quantitative analysis has supported the design process or modification process
* whether the quantitative analysis provides inputs to an argument that risks are ALARP
* how any uncertainties and limitations have been treated in the analysis
* how the analysis has been used to compare against numerical targets

1. Some licensees use deterministic safety cases as their main demonstration that hazards are managed and risks have been reduced ALARP. PSA can be used to complement the deterministic analysis by reducing conservatisms in the analysis and showing a more realistic view of fault progression to help demonstrate that risks have been reduced ALARP.

## Applications for PSA insights in ONR

1. PSA can provide useful information for inspectors from non-PSA disciplines. The PSA team within ONR are available to assist inspectors to understand how PSA can benefit their assessment as described in the following sections.

### PSA event analysis

1. ONR hold copies of the PSA models for all operating and under construction civil reactors in the UK. When an incident is reported via the ONR incident reporting system as a nuclear safety incident notification form (INF1) this is reviewed by the ONR PSA team. PSA event analysis can be performed to identify the risk associated with a nuclear safety event and the sensitivity of any further failures that could have occurred.
2. Events are screened to establish if the initiating events or SSCs that were affected are within the scope of the PSA. Events that are considered are those that led to loss of protective measures, reduced or challenged defence in depth or caused a reactor trip with loss of safety systems.
3. The PSA model is then modified to take account of the initiating event that occurred and any failures of SSCs. The model is analysed, and the results are categorised based on the following table.

Table 3: PSA event analysis categories

| Category | Conditional Core Damage Probability or increase in Core Damage Probability | Conditional probability of >1Sv offsite release or increase in frequency of >1Sv offsite release |
| --- | --- | --- |
| High Safety Significance | >1×10-04 | >1×10-05 |
| Moderate Safety Significance | 1×10-04 to 1×10-05 | 1×10-05 to 1×10-06 |
| Minor Safety Significance | 1×10-05 to 1×10-06 | 1×10-06 to 1×10-07 |
| Low Safety Significance | < 1×10-06 | < 1×10-07 |

1. Inspectors can use PSA event analysis to gain a better understanding of the risk significance of events that have happened. This information can be used to risk inform future inspections and to identify trends. It can also be used to inform the level of regulatory attention required when following up incidents.

### ‘PSA on a page’

1. PSA on a page is a recent initiative by the ONR PSA team to improve the visibility of PSA results for the wider organisation. ONR hold the PSA models for each of the operating nuclear power stations and those that have entered GDA in the UK.
2. PSA on a page provides a simple overview of the most risk significant initiating events, common cause failures, operator actions and fault sequences for a reactor. The risks from fuel route and hazards are also covered where these have been analysed in the PSA.
3. References to PSAs on a page are not included within this TAG as they are routinely updated by the PSA team and any references are likely to become out of date prior to revision of this TAG.
4. Inspectors should approach the PSA team to obtain the most recent versions.

### PSA support to inspections and assessments

1. PSA results can be used to inform the selection of systems and faults that require more attention during inspections. Using PSA can help inspectors to be proportionate and targeted in their selections. PSA on a page and PSA event analysis can also provide information on where inspectors may wish to focus their attention.
2. For example, PSA insights may help risk inform the scope of a systems-based inspection (SBI), or target attention on specific claims or SSCs during assessment of a safety case. Important operator actions can be considered during LC 10 or LC 24 inspections, or as part of SBIs.
3. PSA can help to characterise the safety significance of assessment findings and shortfalls during inspections. Similar approaches to those described in PSA event analysis can be used to establish the risk associated with various faults and systems.
4. As discussed in Section ‎5.7, PSA models often contain limitations, assumptions and uncertainties. Advice should be sought from the PSA team where the limitations of the PSA may impact the insights being used.
5. It is important to recognise that PSA only provides one view of risk and so should only act as one input to decision making alongside deterministic analysis, good engineering principles and other techniques.

# Appendix 1 – Examples of use of PSA

A1.1 - Example of use of PSA by industry

1. An example of a PSA-informed modification was recently assessed by ONR. An operating facility was changing its operating mode due to approaching end of life. This meant that the PSA model that had previously been used to assess risks during operation had to be modified to represent the operating mode supporting end of life. This new operating mode put additional demands on various systems such as fuel handling cranes. The PSA identified that some of the cranes were presenting a relatively high risk.   
   The dutyholder compared this risk against the time and cost of implementing improvements and concluded the risk was not ALARP. The dutyholder used this information to propose some changes to the cranes and once these modifications were in place the dutyholder was able to make an argument that the risks had been reduced ALARP.

A1.2 - Examples of use of PSA by regulators

### PSA event analysis

1. This is an anonymised example of PSA event analysis. Inspectors should contact the PSA team if they wish to discuss the example in more detail.
2. A facility suffered from multiple failures in the offsite electrical grid supplies. This led to unplanned shutdowns of the facility and some plant failures.   
   The facility PSA included a Loss of Offsite Power fault with an initiating event frequency based on the normal frequency of loss of offsite power across that type of facility.
3. ONR analysed the PSA model with an increased Loss of Grid Frequency to represent the multiple grid failures. The PSA analysis results indicated that the increase in risk was of a high safety significance. The PSA inspector presented the results to the relevant site and specialist inspectors and this information was used to inform ONR engagement with the dutyholder on their response to the offsite failures.

## A1.3 - Use of PSA to inform on-site inspections

1. ONR regularly utilise information from the PSA to inform inspection planning and scoping for System-Based-Inspections (SBIs). PSA Inspectors use the PSA to determine the risk contribution from different systems and hazards on a station and to also identify high importance components and operator actions related to specific systems and hazards. ONR site and specialist inspectors then use this information to identify focus areas for their inspections and inform inspection scope and planning.

## A1.4 - Other examples

1. There are many examples of dutyholders and ONR using PSA to risk inform design and operation of nuclear facilities. This ranges from using PSA to inform concept design, improve maintenance practices, justify continuing operation, and target system modifications and improvements over the lifecycle of a facility. However due to commercial sensitivity this has been redacted and is stored for internal reference only and is made available to Inspectors via ONR’s electronic document and record management system [29].

# Appendix 2 – Mapping between Issue O WENRA Reference Levels

| WENRA Reactor Safety Reference Levels | Section in this document |
| --- | --- |
| O1.1 - For each plant design, a specific PSA shall be developed for level 1 and level 2, considering all relevant operational states, covering fuel in the core and in the spent fuel storage and all relevant internal and external initiating events. External hazards shall be included in the PSA for level 1 and level 2 as far as practicable, taking into account the current state of science and technology. If not practicable, other justified methodologies shall be used to evaluate the contribution of external hazards to the overall risk profile of the plant. | ‎5.4 Scope of PSA |
| O3.1 - PSA shall be used to support safety management. The role of PSA in the decision-making process shall be defined | ‎5.6 Use of PSA |
| O3.2 - PSA shall be used (on a continuous basis) 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. | ‎5.6 Use of PSA |
| O3.3 - 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". | ‎5.6 Use of PSA  5.9 Comparison with numerical targets |
| O3.4 - PSA shall be used to assess the adequacy of plant modifications, changes to operational limits and conditions and procedures and to assess the significance of operational occurrences. | ‎5.6 Use of PSA |
| O3.5 - 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. | ‎5.6 Use of PSA |
| O3.6 - 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. | ‎5.6 Use of PSA |
| O4.1 - 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 | ‎5.7 Limitations and uncertainty of PSA |
| O4.2 - 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. | ‎5.6 Use of PSA |
| O4.3 - 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. | ‎5.6 Use of PSA |

# Appendix 3 – A brief overview of the development of nuclear power plant PSA in the UK

1. This appendix sets out a brief overview of the development of PSA for the civil reactor fleet in the UK. It is provided for context and information only and is not intended to be comprehensive or definitive.
2. The first nuclear power stations in the UK to develop PSA models were the AGRs. The first five to be built (Dungeness B, Hinkley Point B, Hunterston B, Hartlepool and Heysham 1) had a deterministic safety case but did not have a PSA during the design and construction phase. PSA models were produced following the start of operation. Some aspects of these PSA models are strongly linked to the deterministic safety case that underpins the design of these stations, especially for hazards initiating events.
3. The last two AGRs to be built (Heysham 2 and Torness) were developed using insights from an at-power PSA during the design and construction phase. This led to some improvements in their design, including improved separation and segregation of SSCs to improve resilience to hazards. These two stations have a risk monitor called ESOP. See section ‎5.6.3 for more guidance on risk monitors. The risk monitor is only used for at-power operation and limited start-up and shutdown states as none of the AGR PSAs model operation during reactor shutdown.
4. The last station to be commissioned in the UK was SZB which has a broad scope PSA including shutdown states and a probabilistic assessment of hazards. This station also has a risk monitor using RiskWatcher software. SZB has a full scope PSA which is used for a variety of purposes including:

* maintenance planning (Riskwatcher)
* outage planning (Riskwatcher)
* point in time risk levels (Riskwatcher)
* risk studies (PSA model)
* plant modifications
* emergent safety justifications
* operational assessments
* safety reviews
* data changes
* MITS changes
* procedural changes
* claims on operators
* tech spec changes
* tech spec action completion times
* tech spec extended completion times

1. New power station developments since SZB have included PSAs, for example recent GDA submissions that have achieved a Design Acceptance Certificate have included broad scope PSA models including internal events, hazards, fuel storage and fuel handling, in all plant operating states. The level of detail for each area can vary depending on the risk significance of the faults in each area.
2. The PSA for Hinkley Point C has been developed over a number of years. The original PSA model presented at GDA was replaced by a new fully symmetric PSA model. This model was built using a semi-automated fault tree tool known as KB3. This allowed for detailed fault tree models to be built based on the piping and instrumentation diagrams. The HPC PSA has recently been updated to include detailed modelling of internal fire, internal flood and seismic hazard PSA models. An updated level 2 PSA and a level 3 PSA have also been produced.

# References

|  |  |
| --- | --- |
| [1] | ONR, “Safety Assessment Principles (SAPs) for Nuclear Facilities - 2014 Edition (Revision 1),” 2020. |
| [2] | ONR, “NS-TAST-GD-030 - Probabilistic Safety Analysis”. |
| [3] | WENRA, “PSA Explanatory Note,” March 2007. [Online]. Available: https://www.wenra.eu/sites/default/files/publications/rhwg\_psa\_explanatory\_note\_march07.pdf. [Accessed 24 February 2023]. |
| [4] | ONR, “Licence Condition Handbook,” 2017. [Online]. Available: https://www.onr.org.uk/media/gixbe2br/licence-condition-handbook.pdf. |
| [5] | WENRA, “Safety Reference Levels for Existing Reactors 2020,” 2021. [Online]. Available: https://www.wenra.eu/sites/default/files/publications/wenra\_safety\_reference\_level\_for\_existing\_reactors\_2020.pdf. |
| [6] | IAEA, “Safety Standards Series No. GSR Part 4 (Rev. 1) - Safety Assessment for Facilities and Activities,” 2016. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1714web-7976998.pdf. |
| [7] | IAEA, “Specific Safety Requirements SSR 2/1 (Rev. 1) - Safety of Nuclear Power Plant: Design,” 2016. [Online]. Available: https://www-pub.iaea.org/MTCD/publications/PDF/Pub1715web-46541668.pdf. |
| [8] | IAEA, “Specific Safety Requirements SSR 2/2 (Rev. 1) - Safety of Nuclear Power Plant: Comissioning and Operation,” 2016. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1716web-18398071.pdf. |
| [9] | IAEA, “Specific Safety Requirements SSR-3 - Safety of Research Reactors,” 2016. [Online]. Available: https://www-pub.iaea.org/MTCD/publications/PDF/P1751\_web.pdf. |
| [10] | IAEA, “Safety Standards Series No. SSR-4 - Safety of Nuclear Fuel Cycle Facilities,” 2017. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1791\_web.pdf. |
| [11] | IAEA, “Safety Standards Series No. SSG-3 (Rev. 1) - Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants,” 2010. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1430\_web.pdf. |
| [12] | IAEA, “Specific Safety Guide No. SSG-4 - Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants,” 2010. [Online]. Available: https://www-pub.iaea.org/mtcd/publications/pdf/pub1443\_web.pdf. |
| [13] | IAEA, “Safety Series No. 50-P-12 - Procedures for Conducting PSA of Nuclear Power Plants (Level 3): Off-site Consequences and Estimation of Risks to the Public,” 1996. [Online]. Available: https://gnssn.iaea.org/Superseded%20Safety%20Standards/Safety\_Series\_050-P-12\_1996.pdf. |
| [14] | ANS, “ANS/ASME RA-S-1.1-2024 - Standard for Level 1/Large Early Release Frequency Probabilisitic Risk Assessment for Nuclear Power Plant Applications,” 15 March 2024. [Online]. Available: https://store.accuristech.com/ans/standards/ans-ra-s-1-1-2024?product\_id=2582888. |
| [15] | ANS, “ANS RA-S-1.2-2024 - Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs),” 17 June 2024. [Online]. Available: https://store.accuristech.com/ans/standards/ans-ra-s-1-2-2024?product\_id=2907249. |
| [16] | ANS, “ANS RA-S-1.3-2017 - Standard for Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications (Trial Use Standard),” 13 July 2017. [Online]. Available: https://store.accuristech.com/ans/standards/ans-ra-s-1-3-2017?product\_id=2019591. |
| [17] | ANS, “ANS/ASME-58.22-2014 - Requirements for Low Power and Shutdown Probabilistic Risk Assessment,” 25 March 2015. [Online]. Available: https://store.accuristech.com/ans/standards/ans-58-22-2014?product\_id=1903278. |
| [18] | ANS, “ANSI/ASME/ANS RA-S-1.4-2021 - Probabilistic Risk Assessment for Advanced Non-Light Water Reactor Nuclear Power Plants,” 1 January 2021. [Online]. Available: https://store.accuristech.com/ans/standards/ans-ra-s-1-4-2021?product\_id=2207481. |
| [19] | ONR, “NS-TAST-GD-006 - Design Basis Analysis”. |
| [20] | ONR, “NS-TAST-GD-005 - Regulating duties to reduce risks to ALARP”. |
| [21] | IAEA, “TECDOC-1106 - Living Probabilistic Safety Assessment (LPSA),” 1999. [Online]. Available: https://www-pub.iaea.org/MTCD/publications/PDF/te\_1106\_prn.pdf. |
| [22] | ONR, “NS-TAST-GD-094 - Categorisation of Safety Functions and Classification of Structures”. |
| [23] | IAEA, “Specific Safety Guide No. SSG-30 - Safety Classification of Structures, Systems and Components in Nuclear Power Plants,” 2014. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1639\_web.pdf. |
| [24] | ONR, “NS-TAST-GD-045 - Radiological Analysis - Fault Conditions”. |
| [25] | ONR and HSE, “The Radiation (Emergency Preparedness and Public Information) Regulations 2019 - Approved Code of Practice and Guidance,” 2020. [Online]. Available: https://www.onr.org.uk/media/zamdzwr1/reppir-2019-acop.pdf. |
| [26] | ONR, “NS-TAST-GD-063 - Human Reliability Analysis”. |
| [27] | NEA, “NEA/CSNI/R(2019)10 - Use and Development of Probabilistic Safety Assessments at Nuclear Facilities,” 25 January 2022. [Online]. Available: https://www.oecd-nea.org/jcms/pl\_51523/use-and-development-of-probabilistic-safety-assessments-at-nuclear-facilities?details=true. |
| [28] | IAEA, “TECDOC-1983 - Risk Aggregation for Nuclear Installations,” 2021. [Online]. Available: https://www-pub.iaea.org/MTCD/publications/PDF/TE-1983web.pdf. |
| [29] | ONR, “Examples of ONR using PSA to risk inform design and operation of nuclear facilities (Available via CM at 2024/3298)”. |

# Glossary and abbreviations

ACOP Approved Code of Practice

ALARP As Low as Reasonably Practicable

ASME American Society of Mechanical Engineers

BSL Basic Safety Level

BSO Basic Safety Objective

CCF Common Cause Failure

CDF Core Damage Frequency

DBA Design Basis Analysis

DSR Dominant Sequence Reviews

EIMT Examination Inspection Maintenance Testing

FDF Fuel Damage Frequency

FMEA Failure Modes and Effects Analysis

FTA Fault Tree Analysis

FV Fussell Vesely

GDA Generic Design Assessment

GSR General Safety Requirements (IAEA)

IAEA International Atomic Energy Agency

INF1 Incident Notification Form

LC Licence Condition

LERF Large Early Release Frequency

LRF Large Release Frequency

LWR Light Water Reactor

MCS Minimal Cutset

PRA Probabilistic Risk Analysis

PSA Probabilistic Safety Analysis

QRA Quantitative Risk Assessment

RDF Risk Decrease Factor

REPPIR Radiation (Emergency Preparedness and Public Information) Regulations

RIF Risk Increase Factor

SAA Severe Accident Analysis

SAP Safety Assessment Principle(s)

SBI Systems Based Inspection

SSC Structure, System, Component

SSG Specific Safety Guide (IAEA)

SSR Specific Safety Requirement (IAEA)

TAG Technical Assessment Guide(s)

WENRA Western European Nuclear Regulators’ Association

1. In the United States, PSA is referred to as Probabilistic Risk Analysis (PRA). [↑](#footnote-ref-2)
2. A more complex model, which is less commonly used, adds in a fixed on-demand failure contribution and gives a gentler slope to the sawtooth function. [↑](#footnote-ref-3)