|  |
| --- |
| **SEVERE ACCIDENT ANALYSIS** |
| **Doc. Type** | ONR Technical Assessment Guide (TAG) |
| **Unique Doc. ID:**  | NS-TAST-GD-007 | **Issue No.:** | 5.1 |
| **Record Reference:** | 2022/22547 |
| **Date Issued:** | Dec-22 | **Next Major Review Date:** | Aug-27 |
| **Prepared by:** |  | Inspector, Nuclear safety |
| **Approved by:** |  | Professional Lead – Fault Analysis |
| **Professional Lead:** |  | Professional Lead – Fault Analysis |
| **Revision Commentary:** | Major update to scope and technical contentIssue 5.1 - Minor update to remove extant URLs from the document to mitigate potential configuration control issues arising because of changes to third-party web domains. |

**Table of Contents**

[1. Introduction 3](#_Toc110327417)

[2. Purpose and Scope 4](#_Toc110327418)

[3. Relationship to Licence and other Relevant Legislation 6](#_Toc110327419)

[3.1. Licence Conditions 6](#_Toc110327420)

[4. Relationship to SAPs, WENRA Reference Levels and IAEA Safety Standards 8](#_Toc110327421)

[4.1. SAPs and Interfacing TAGs 8](#_Toc110327422)

[4.2. IAEA Standards 12](#_Toc110327423)

[4.3. WENRA Safety Objectives and Reference Levels 15](#_Toc110327424)

[5. Advice to Inspectors 17](#_Toc110327425)

[5.1. Characteristics of Severe Accidents 17](#_Toc110327426)

[5.2. Purpose and Use of SAA 19](#_Toc110327427)

[5.3. Identification of Severe Accident Phenomena 22](#_Toc110327428)

[5.4. Selection of Severe Accident States and Sequences 24](#_Toc110327429)

[5.5. Severe Accident Safety Measures 26](#_Toc110327430)

[5.6. Analysis Techniques 33](#_Toc110327431)

[5.7. Severe Accident Management 38](#_Toc110327432)

[5.8. ALARP 40](#_Toc110327433)

[5.9. Practical Elimination 41](#_Toc110327434)

[5.10. Fukushima Lessons Learned 47](#_Toc110327435)

[6. References 49](#_Toc110327436)

[Glossary and Abbreviations 53](#_Toc110327437)

# Introduction

1. ONR has established its Safety Assessment Principles (SAPs) [1] which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other duty-holders. 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 primary aim of this document is to provide guidance to ONR inspectors in support of the SAPs, so that the adequacy of licensee[[1]](#footnote-1) safety cases can be assessed more effectively and efficiently, and to guide inspectors in the exercise of their regulatory judgement. Consistent with the scope of the SAPs (in particular paragraph 6), the TAG is intended to be technology-neutral. It is not intended to provide prescriptive instructions to licensees on how to design their facilities, undertake their activities or write their safety cases.
2. Consistent with the principle of defence of depth, ONR has an expectation (SAPs paragraph 610) that events beyond those considered as part of Design Basis Analysis (DBA) are managed through the provision of equipment and procedures that can prevent progression of accidents or mitigate the consequences. These events, where the potential consequences may be more severe, should be considered in the safety case. ONR refers to such events as ‘severe accidents’.
3. The SAPs (paragraph 664) define severe accidents as those fault sequences that could lead either to radiological consequences off-site exceeding 100 mSv, or to an unintended relocation of a substantial quantity of radioactive material within the facility which places a demand on the integrity of the remaining physical barriers. For power reactors a severe accident is often associated with significant core degradation, but ONR’s definition encompasses other types of facility where radiological hazards are high.
4. This TAG contains guidance to advise and inform ONR staff in the exercise of their regulatory judgment. It provides guidance on expectations for the analysis of severe accidents, referred to here and in the SAPs as severe accident analysis (SAA). Undertaking SAA may not be applicable, or be proportionate, for all types of facility. However, for facilities presenting the highest hazards SAA is beneficial and should be an integral part of the licensee’s demonstration of defence in depth.
5. The SAPs define the principle aims of SAA to be to:
* assist in the identification of any further reasonably practicable preventative or mitigating measures beyond those derived from other forms of analysis;
* form a suitable basis for accident management strategies and procedures;
* support the preparation of emergency plans for the protection of people; and
* support the probabilistic safety analysis (PSA) of the facility’s design and operation.
1. SAA is predominately focused on deterministic analysis of events which are more severe than those considered as part of the DBA. Wider consideration of severe accidents in the safety case may also include probabilistic analysis, particularly for power reactors and other complex facilities. Level 2, and where appropriate Level 3, PSA should include consideration of the probabilistic aspects of severe accidents. Guidance on these complimentary methods of fault analysis is covered in other ONR TAGs.
2. The licensee’s SAA should support the design of severe accident safety measures such as containment structures and support the qualification of equipment by defining severe accident environmental conditions. The analysis should also support the development of accident management strategies and guidance. Although closely related to SAA, guidance on the assessment of these aspects of the safety case is outside the scope of this TAG.
3. ONR seeks to ensure that its guidance to inspectors reflects international safety standards produced by organisations such as the International Atomic Energy Agency (IAEA) and Western European Nuclear Regulators Association (WENRA). Building on the lessons learned from the accident at Fukushima Daichi, there is an established international consensus on the need to consider severe accidents in the design of new facilities and to identify reasonably practicable improvements for existing facilities. In this context, this TAG includes guidance on interpretation of international expectations for consideration of ‘design extension conditions’ (DEC) and for the ‘practical elimination’ of early or large releases of radioactivity. For Nuclear Power Plants (NPPs) the international definitions of DEC refer to two types of conditions depending on the level of fuel damage; this TAG focuses on DEC with core melting/severe fuel damage and which is termed ‘DEC B’ by WENRA. As described in this TAG, the expectations for analyses and demonstrations covered by such international standards are underpinned by, and are compatible with, ONR's Fault Analysis SAPs.

# Relationship to Licence and other Relevant Legislation

## Licence Conditions

1. The nuclear site Licence Conditions (LCs) place legal requirements on the licensee to make and implement arrangements to ensure that safety is being managed adequately. The licence conditions provide a legal framework which can be drawn on in assessment. The following are of particular relevance in the context of SAA:
* Licence Condition 11 – Emergency Arrangements: “…the licensee shall make and implement adequate arrangements for dealing with any accident or emergency arising on the site and their effects.”
* Licence Condition 15 - Periodic Review: “The licensee shall make and implement adequate arrangements for the periodic and systematic review and reassessment of safety cases”.
* Licence Condition 23 - Operating Rules: “The licensee shall, in respect of any operation that may affect safety, produce an adequate safety case to demonstrate the safety of that operation and to identify the conditions and limits necessary in the interests of safety. Such conditions and limits shall hereinafter be referred to as operating rules”.
* LC28 Licence Condition 28 - Examination, Inspection, Maintenance and Testing: “The licensee shall make and implement adequate arrangements for the regular and systematic examination, inspection, maintenance and testing of all plant which may affect safety”.
1. Licence Condition 23 requires that an adequate safety case should be produced by the licensee, which should be in accordance with its arrangements under Licence Condition 14: Safety documentation. Where there is the potential for a severe accident, there is an expectation that the safety case should include and be informed by severe accident analysis. Consideration of conditions and limits should not be confined to those aspects derived from the licensee’s DBA. For some types of facility there may be practical measures that can be implemented to prevent the escalation of severe accidents and/or mitigate the consequences. In such cases there should be consideration of ‘operating rules’ across all levels of defence in depth. For example, this could include controls on the availability of equipment required for severe accidents, or conditions on when to deploy, actuate and terminate severe accident measures.
2. LC11, and the similar duties introduced by the Radiation (Emergency Preparedness and Public Information) Regulations 2019 (REPPIR), set expectations on the scope and extent of the licensee’s emergency arrangements. The arrangements should address all events that might lead to a radiation emergency, including those considered to be ‘beyond design basis’; this might include events which meet ONR’s definition of a severe accident. The operator’s emergency arrangements should ensure that plans are scalable for these severe events and that any capabilities that are required in addition to, or instead of, those provided for lesser events can be adequately resourced and implemented in the event of such an emergency. SAA may be used to inform the licensee’s arrangements for emergency planning and also the hazard evaluation and consequence assessments required by REPPIR to inform detailed and outline off-site planning.
3. The licensee’s SAA may demonstrate the benefit of having additional safety measures, beyond those identified as part of its DBA. In this case the relevant safety functions should be categorised and any measures which deliver these functions (such as structures, systems and components) should be classified using the licensee’s own schemes. Whilst these additional features might be assigned a lower classification than DBA measures based on significance for delivering a safety function, they should still be recognised as making a contribution to nuclear safety as part of defence in depth. As such, any identified features should be subject to maintenance (or otherwise demonstrated to be able to perform the required function) through the life of the facility, commensurate with the nuclear safety significance.
4. The legal requirement of LC15 is that the licensee must carry out periodic reviews of its safety cases. This is necessary, as facilities may degrade over time, or be progressively modified in some way, or be used in a way not conceived of in the original design. Legacy nuclear facilities may not have been originally designed with the same level of analytical and engineering rigour that would be used if those same facilities were to be designed today. The licensee may benefit from improved understanding of the behaviour of plants in accident conditions and from learning from past accidents. ONR’s guidance to inspectors on periodic review [2] expects that all nuclear facilities consider their SAA and the analysis techniques when performing periodic reviews to ensure that they remain appropriate. ONR’s guidance reflects international good practice [3] which is that periodic review should include an evaluation of the supporting analyses for design extension conditions, that the arrangements aimed at preventing or mitigating severe accidents continue to be sufficient and whether any improvements are reasonable and practicable.

# Relationship to SAPs, WENRA Reference Levels and IAEA Safety Standards

## SAPs and Interfacing TAGs

1. As part of producing a complete safety case (SAP SC.4, paragraph 101(f)), licensees with responsibility for high hazard nuclear facilities are expected to analyse severe accidents as part of the overall demonstration that risks are ALARP. Deterministic SAA will form one part of the licensee’s wider safety case for severe accidents, which will need to consider other areas of engineering and analysis.
2. SAPs FA.1, FA.2 & FA.3 provide general expectations for fault analysis for all nuclear facilities. There is an expectation (FA.1) that where hazards are high the licensee’s approach should include SAA, alongside other complimentary analysis techniques such as DBA and PSA. FA.2 expects that all initiating faults, including those with the potential to cause a severe accident, should be identified. FA.3 states that the consequences of faults (including severe accidents) should be analysed for both release of radioactive material and for exposure to direct radiation.
3. SAPs FA.15, FA.16 & FA.25 and the associated paragraphs, 663-677, provide the high level guidance to inspectors on SAA. This TAG provides more detailed guidance to inspectors on these SAPs:
* FA.15 - Scope of severe accident analysis: Fault states, scenarios and sequences beyond the design basis that have the potential to lead to a severe accident should be analysed.
* FA.16 - Use of severe accident analysis: Severe accident analysis should be used in the consideration of further risk-reducing measures.
* FA.25 - Relationship to DBA and PSA: The severe accident analysis should be performed in a manner complementary to the DBA and PSA, so that each type of analysis informs the others in a mutually consistent manner within the facility’s safety case.
1. In accordance with SAPs FA.1 and FA.3, it is expected that radiological consequence analysis of severe accidents sequences should be carried out and the associated risks assessed as part of the facility PSA. One of the purposes of the PSA (SAP FA.14 and paragraph 661(k))) is to provide an input to SAA, for example to identify fault sequences that should be subject to SAA. The SAA may also support the PSA; in particular, for nuclear power plants this would be expected to include inputs to Level 2 and Level 3 PSA such as information on accident progression, plant conditions and source terms. The numerical targets in the SAPs (NT.1) are used by inspectors as an aid to judgement when considering whether radiological hazards are being adequately controlled and risks reduced to As Low As Reasonably Practicable (ALARP). Severe accidents may need to be considered in any evaluations by the licensee against its risk criteria and reviewed by the inspector against Targets 5 to 9.
2. SAP EKP.3, consistent with IAEA Safety Requirements [4],[5], states that nuclear facilities should be designed and operated with defence in depth against potentially significant faults or failures through the provision of multiple independent barriers. Using the IAEA definitions of levels of defence in depth [4] and also paragraph 152 and Table 1 of the SAPs, severe accidents are plant states arising from the absence, bypass or failure of measures at Level 3 (and lower) in the defence in depth hierarchy. Severe accident analysis informs consideration of measures at Levels 4 and 5. Measures at Level 4 should protect against fault escalation and mitigate the consequences of accidents, whereas those at Level 5 should provide for emergency management and on- and off-site emergency response.
3. A number of other SAPs are closely associated with severe accidents, either explicitly or in a general sense in that in principle they apply to all faults and accidents. The inspector should be cognisant of the links to other aspects of the licensee’s wider severe accident safety case and how these aspects are informed by SAA. With this in mind, the inspector should be aware of the expectations of the following SAPs:
* ECS series – categorisation of safety functions and classification of safety measures
* EKP series – key engineering principles
* ESS series – safety systems
* ESR series – control and instrumentation of safety-related systems
* ECE series – civil engineering, particularly containments
* EQU.1 – equipment qualification for severe accident conditions
* ECV series – containment systems
* ECM.1 – testing of severe accident equipment during commissioning
* EHF series – human factors consideration of operator actions in severe accidents
* EHA series – external and internal hazards as initiators of a severe accident
* AM.1 - accident management and emergency preparedness
1. A number of ONR TAGs provide guidance to inspectors on aspects that form part of SAA, or interface directly with it. The following TAGs are referred to in the detailed guidance provided in Section 5 of this document:
* NS-TAST-GD-005: Guidance on the Demonstration of ALARP [6]
* NS-TAST-GD-006: Design Basis Analysis [7]
* NS-TAST-GD-013: External Hazards [8]
* NS-TAST-GD-014: Internal Hazards [9]
* NS-TAST-GD-030: Probabilistic Safety Analysis [10]
* NS-TAST-GD-045: Radiological Analysis for Fault Conditions [11]
* NS-TAST-GD-042: Validation of Computer Codes and Calculation Methods [12]
* NS-TAST-GD-063: Human Reliability Analysis [13]
* NS-TAST-GD-089: Chemistry Assessment [14]
1. There are many other documents that provide guidance to inspectors on matters related to the licensee’s wider safety case for severe accidents. Those likely to be of most relevance are:
* NS-TAST-GD-003: Safety Systems [15]
* NS-TAST-GD-020: Civil Engineering Containments for Reactor Plants [16]
* NS-TAST-GD-021: Containment – Chemical Plants [17]
* NS-TAST-GD-031: Safety Related Systems and Instrumentation [18]
* NS-TAST-GD-035: The Limits and Conditions for Nuclear Safety (Operating Rules) [19]
* NS-TAST-GD-051: The Purpose, Scope, and Content of Safety Cases [20]
* NS-TAST-GD-059: Human Machine Interface [21]
* NS-TAST-GD-094: Categorisation of Safety Functions and Classification of Structures, Systems and Components [22]
* NS-TAST-GD-103: Emergency Power Generation [23]
* NS-INSP-GD-011: LC 11 and REPPIR– Operator’s Emergency Arrangements [24]
* Approved Code of Practice and guidance for the Radiation (Emergency Preparedness and Public Information) Regulations 2019 [25]

## IAEA Standards

1. The IAEA Safety Standards (Requirements and Guides) are used to benchmark the SAPs and are recognised by ONR as relevant good practice. They should therefore be consulted, where relevant, by inspectors as complementary guidance to the SAPs and TAGs.
2. A key IAEA Safety Standard of relevance is the Specific Safety Requirements SSR-2/1 ‘Safety of Nuclear Power Plants: Design’ [4]. This refers to application of the concept of ‘defence in depth’ to provide consecutive and independent levels of protection against faults and accidents. The purpose of the fourth level of defence is to prevent the progression of accidents that occur from failures at lower levels and to mitigate the consequences if these develop to a severe accident. SSR-2/1 also introduces the key expectation that plant states (for both the reactor and any spent fuel pool) that could lead to an early radioactive release or a large radioactive release[[2]](#footnote-2) shall be ‘practically eliminated’[[3]](#footnote-3). Further guidance to inspectors on this topic is provided in Section 5.
3. To support the demonstration of defence in depth, SSR-2/1 Requirement 20 states that ‘design extension conditions’ shall be derived and analysed for new designs. IAEA has plans to publish more detailed guidance on defence in depth in relation to design extension conditions and on practical elimination. ONR has worked with international partners during the drafting and review of this additional guidance to ensure compatibility with this TAG.
4. SSR-2/1 recognises that it might not be practicable to apply these requirements to NPPs that are already in operation or under construction. However, IAEA’s expectation is that these requirements would be a relevant consideration for a periodic review of an existing plant, to determine whether there could be reasonably practicable safety improvements.
5. Consistent with the expectations in SSR-2/1, contracting parties to the Convention on Nuclear Safety have agreed ‘The Vienna Declaration on Nuclear Safety’ [26]. Principle 1 requires that “new nuclear power plants are to be designed, sited, and constructed, consistent with the objective of preventing accidents in the commissioning and operation and, should an accident occur, mitigating possible releases of radionuclides causing long-term off site contamination and avoiding early radioactive releases or radioactive releases large enough to require long-term protective measures and actions.”. For existing plants Principle 2 requires that reasonably practicable or achievable safety improvements are to be implemented in a timely manner. As a contracting party, the UK is committed to setting expectations to address these objectives, taking into account the relevant IAEA Safety Standards.
6. SSR-4 ‘Safety of Nuclear Fuel Cycle Facilities’ [5] sets similar expectations to those in SSR-2/1. IAEA’s expectation is that safety requirements established in this publication are to be applied for new nuclear fuel cycle facilities and also to existing facilities to the extent practicable. SSR-4 has a broader scope of applicability beyond NPPs and includes nuclear fuel cycle facilities in which nuclear material and radioactive material are processed, handled, stored and prepared for disposal. However, the fundamental objective for consideration of design extension conditions is the same, which is to prevent accident conditions which are more severe that those considered in DBA, or to mitigate their consequences, as far as is reasonably achievable. IAEA has also provided practical information for safety re-assessment of nuclear fuel cycle facilities in light of the accident at the Fukushima Daiichi nuclear power plant [27].
7. SSG-2 ‘Deterministic Safety Analysis for Nuclear Power Plants’ [28] includes guidance on the analysis of design extension conditions, including in support of a demonstration of practical elimination. In relation to severe accidents, the guidance includes analysis of plant states with core melting. Although specifically targeted at NPPs, many of the principles on identification of events, acceptance criteria, use of computer codes and levels of conservatism should provide the inspector with useful guidance on deterministic SAA for all types of facility.
8. Other IAEA guidance of particular relevance to severe accidents includes:
* SSG-4: Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants [29] – This explains how SAA should support the PSA.
* SSR-2/2: Safety of Nuclear Power Plants: Commissioning and Operation [30] – Requirement 19 covers the preparatory measures, procedures and guidelines, and equipment that are necessary for preventing the progression of accidents, including severe accidents.
* SSG-53: Design of the Reactor Containment and Associated Systems for Nuclear Power Plants [31] – Provides supporting guidance to SSR-2/1 in relation to containment. Application of the guidance to existing nuclear power plants is provided in an Appendix. This should provide useful background to the inspector on a key defence in depth measure for many modern designs of NPP.
* SSG-54: Accident Management Programmes for Nuclear Power Plants [32] - Provides guidance on setting up a severe accident management programme, from the conceptual stage to the development of a complete set of procedures and guidelines.
* SSG-64: Protection against Internal Hazards in the Design of Nuclear Power Plants [33] – Expects that safety features for design extension conditions should be designed or protected against applicable internal hazards.

## WENRA Safety Objectives and Reference Levels

1. WENRA has produced standards for different types of facilities, including new and existing power reactors, research reactors, spent fuel storage and waste treatment facilities. In relation to design extension conditions, the main source of guidance is that produced for reactors, however the principles discussed are often more widely applicable. Inspectors are thus encouraged to use the reference levels for reactors as sources of good practice when assessing licensees’ submissions for all types of nuclear facilities. Inspectors should however be mindful that the intent of these guides can often be met through a wide range of effective measures and practices and the approach for reactors may not necessarily translate directly.

### Safety Objectives for New Nuclear Power Plants

1. The WENRA Reactor Harmonization Working Group has developed safety objectives for new NPPs [34]. Whilst the objectives address new civil NPP projects, the intention is that they should also be used as a reference to help identify reasonably practical safety improvements for existing designs.
2. Of particular relevance to severe accidents is Objective O3 ‘Accidents with Core Melt’. This concerns the potential for radioactive release from accidents with core melt from either the reactor or the spent fuel pool. This states that accidents which could lead to early or large releases have to be practically eliminated, or where this cannot be achieved design provisions have to be taken so that only limited protective measures in area and time are needed for the public and that sufficient time is available to implement these measures. Taking into account lessons from the Fukushima Daiichi accident, WENRA has also produced common positions on selected key safety issues [35]. In relation to Objective 3 these include:
* Position 4 - Provisions to mitigate core melt and radiological consequences
* Position 5 - Practical elimination.
1. Reflecting the expectations of the Nuclear Safety Directive of the European Union [36], and the Vienna Declaration on Nuclear Safety [26], WENRA has provided further guidance [37] on the key elements and expectations for the demonstration of practical elimination for new NPPs.

### Reference Levels for Existing Nuclear Power Plants

1. Section 4 of NS-TAST-GD-005 [6] identifies the WENRA Safety Reference Levels as relevant good practice (RGP) for existing civil NPPs. The Safety Reference Levels were re-issued in 2021 [38]. Those directly related to the scope of this TAG are primarily included within ‘Issue F’ (Design Extension of Existing Reactors). Similar expectations have been set out for existing research reactors [39].
2. The Safety Reference Levels for ‘Issue LM’ (Emergency Operating Procedures and Severe Accident Management Guidelines) and ‘Issue R’ (On-site Emergency Preparedness) are also relevant to the extent that SAA informs development of such plans and procedures. Guidance is also provided on consideration of external hazards more severe than those assumed for DBA (refer to Issue TU6); such extreme hazards could be potential initiators of severe accidents and could affect the success of measures to prevent accident progression and mitigate consequences.
3. The guidance on SAA contained in Section 5 of this TAG has been reviewed against, and aligned with, the relevant SRLs.

# Advice to Inspectors

## Characteristics of Severe Accidents

1. Paragraph 609 of the SAPs identifies the need to plan for events with more severe consequences than those allowed for in DBA. Such events may involve low frequency events for which the measures identified as part of DBA would be ineffective, or where measures are assumed to fail. Where consequences are high, it is considered reasonable for the licensee to carry out SAA to address how severe events would be managed and to identify the plant, equipment and procedures that would be needed to control or mitigate the consequences. Paragraph 666 of the SAPs states that SAA is not normally concerned with the sequence of events leading to the accident, but instead SAA should be focussed on preventing progression of the resulting severe accidents and/or mitigating the consequences. A severe accident may arise from a range of internal and/or external causes, including security-related initiators (paragraph 39 of the SAPs refers). The expectation is that the application of SAA should be considered for any nuclear facility where there is the potential for a severe accident. The purpose of this section is to provide guidance to the inspector on what should be considered as a severe accident, based on ONR’s definition in the SAPs and on international definitions for design extension conditions.
2. The SAPs paragraph 664 defines severe accidents as:

“those fault sequences that could lead either to consequences exceeding the highest off-site radiological doses given in the BSLs of Numerical Target 4 (i.e. 100 mSv, conservatively assessed) or to an unintended relocation of a substantial quantity of radioactive material within the facility which places a demand on the integrity of the remaining physical barriers. A substantial quantity of radioactive material is one which if released could result in the consequences specified in the societal risk Target 9.”

1. An event that could reasonably meet these criteria should be considered as a severe accident. For nuclear power plants it is expected that events involving degraded core states with fuel melt and relocation of material, for example within containments, would be candidates for consideration as severe accidents, even if by design there are no (or at least limited) off-site radiological consequences. More generally a major release of radioactivity from any facility, from whatever cause, would be considered a severe accident if the off-site dose could exceed 100 mSv. At fuel processing sites this might include certain releases arising from containment failure of hazardous liquors. Similarly, accidents resulting in exposure to high levels of direct radiation off-site might also satisfy the definition. However, the interpretation of this definition is likely to be facility and technology dependent. The inspector should be aware that what is appropriate for one facility may not necessarily read directly across to others.
2. To support the demonstration of defence in depth, SSR-2/1 Requirement 20 [4] expects that an analysis of ‘design extension conditions’ be performed for new designs:

“A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant’s capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.”

1. For NPPs, the IAEA definition of DEC includes “conditions in events with core melting”. Similarly, WENRA also considers DEC to include events “with postulated severe fuel damage” and refers to these as ‘DEC B’ [38]. Both of these situations meet ONR’s definition of a severe accident and are therefore within the scope of this TAG.
2. Consistent with paragraph 628 of the SAPs, ONR’s guidance to inspectors on DBA (NS-TAST-GD-006, [7]) identifies a class of very low frequency events where design basis safety measures are assumed to fail or be ineffective, but where best-estimate deterministic approaches show that other plant features are effective in preventing high consequences (typically by preventing fuel degradation). Such events should be analysed to demonstrate that there are no cliff-edge effects associated with faults just beyond the cut-off frequency for accidents considered using DBA. IAEA SSR-2/1 refers to these as DEC without significant fuel degradation. In the context of existing NPPs, WENRA [38] refers to such events as ‘DEC A’. If prevention of fuel damage can be demonstrated, then these events would not be expected to satisfy ONR’s definition of a severe accident and their consideration is outside of the scope of this TAG. However, ‘DEC A’ events should be considered as part of the licensee’s wider approach to fault analysis to demonstrate defence in depth. Further guidance on the assessment of ‘DEC A’ events is provided in NS-TAST-GD-006.
3. From a practical perspective, the inspector should take a pragmatic approach to interpreting a licensee’s terminology, demarcations and safety case presentation, and focus on outcomes and consistency with RGP.
4. For other types of facilities such as those associated with the nuclear fuel cycle, Requirement 21 of SSR-4 [5] sets expectations for the analysis of DEC that are either more severe than design basis accidents or that involve additional failures. In accordance with Requirement 11, this requirement should be applied in a graded way, taking into account the level of risk and magnitude of the hazard. However, an event which meets ONR’s definition of a severe accident should normally be subject to SAA using analysis techniques appropriate to the facility and the hazards.

## Purpose and Use of SAA

1. Section 5.1 defines those states which meet ONR’s definition of a severe accident and should guide inspectors on when it would be proportionate to expect SAA. Having established whether there is an expectation for some level of SAA, this section provides guidance to the inspector on the purpose and objectives of the analysis. Subsequent sections then provide guidance on assessing the licensee’s approach to SAA and how the analysis is being used to inform the wider safety case.
2. FA.16 of the SAPs states that SAA should be used in the consideration of further risk-reducing measures. This aim is consistent with international expectations for the analysis of DEC. Paragraph 672 of the SAPs sets out ONR’s wider expectations for SAA, which should be to provide information to:
* assist in the identification of any further reasonably practicable preventative or mitigating measures beyond those derived from engineering analysis, DBA and PSA;
* form a suitable basis for accident management strategies and procedures (see SAP AM.1);
* support the preparation of emergency plans for the protection of people (see SAP AM.1); and
* support the PSA of the facility’s design and operation.
1. The safety case should identify the key claims made in relation to severe accidents and the SAA should provide the supporting evidence to substantiate these claims. In accordance with IAEA SSG-2 [28], this could include claims that:
* The facility can be brought into a state where the containment functions can be maintained in the long term.
* The SSCs and procedures are capable of preventing a large radioactive release or an early radioactive release, including containment bypass (as part of demonstrating practical elimination).
* Control locations remain habitable to allow performance of required staff actions.
* Planned severe accident management measures are effective.
1. Relevant safety functions should be identified, reflecting the circumstances of the accident and the prevailing conditions. The SAA should use deterministic methods to demonstrate that the safety functions are achieved by features implemented in the design, combined with measures that can be implemented through human actions and administrative controls described in procedures and/or accident management guidelines. Paragraph 673 of the SAPs recognises that the analysis does not necessarily need to follow the same conservative engineering practices that would be expected for measures identified as part of DBA. A realistic or best-estimate approach may also be preferable for defining accident management strategies. Despite the application of less conservative practices, the licensee should still be using a process for categorising safety functions and classifying the relevant safety measures based on importance to safety; this should be informing the appropriateness of engineering standards and the robustness of operator claims.
2. The outputs from the analysis should allow the characteristics of severe accidents to be defined in terms of:
* the chronological progression of postulated accident sequences and timing of key events;
* changes in plant conditions during the accident;
* physical, chemical and radiation conditions affecting SSCs, including where necessary any relevant dynamic, local or indirect loads and effects [9];
* the timescales, quantities and compositions of radiological releases and also the associated radiological consequences; and
* the levels of direct radiation.
1. The effectiveness of any safety measures will need to be demonstrated against suitable acceptance criteria, which will need to be established by the licensee. The international expectation in SSG-2 [28] is that this should include radiological criteria, which might be expressed in terms of activity levels or radiological doses. Relevant technical criteria should also be set in terms of the integrity of barriers against releases of radioactive material, including avoidance of unacceptable challenges to the containment. Whilst ONR does not stipulate any regulatory criteria for severe accidents, the numerical targets in NT.1 of the SAPs (in particular Targets 8 and 9) do provide a framework to allow inspectors to judge the significance of the risks from severe accidents.
2. As stated in FA.25 of the SAPs, SAA should not be carried out in isolation from the other types of fault analysis (DBA and PSA). DBA will define the boundary of faults which can be shown to be prevented and protected by robust, conservatively designed safety measures. Beyond this point, consideration of design extension conditions should be used to demonstrate that there would still be resilience to less likely/more severe faults than considered in the DBA, with no cliff edge effects. In accordance with SAPs paragraphs 667, EHA.18 & EHA.7, this should include faults and accidents initiated by external and internal hazards which are more severe than those assumed in the DBA.
3. Where conditions for a severe accident are met, SAA should consider, normally using a realistic or best-estimate approach, whether there are further reasonably practical measures that would be beneficial in preventing escalation of the accident and/or mitigating the consequences. Any such measures need to be designed or protected against applicable internal and/or external hazards. Any internal hazards arising from operation of the severe accident measures should also be considered.
4. Modern PSA models as applied to NPPs should allow risk-informed judgements to be made in support of the design and operation of a facility. Separate guidance on assessment of the PSA is provided in FA.10-FA.14 of the SAPs and NS-TAST-GD-30 [10]. SAP paragraph 676 expects that the PSA should include relevant severe accident states, which in accordance with SAP FA.12 should cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults. For a NPP it is expected that SAA will support the Level 2 PSA modelling by providing deterministic analysis of severe accident sequences.
5. The SAPs (AM.1) provide guidance to ONR inspectors on assessment of the licensee’s arrangements for accident management and emergency preparedness. The expectations are relevant to all types of high hazard facilities and should be informed by SAA. This is an aspect that the inspector should be considering for a new facility and also as part of an assessment of the licensee’s periodic safety review. The licensee should have strategies and plans to deal with severe accidents and the relevant arrangements should be designed to ensure that the consequences of severe accidents will be mitigated as far as reasonably practicable. SAA should be used by the licensee to identify required operator actions and inform the development of procedures such as accident management guidelines. The SAA should be used to identify plant, equipment and supplies needed to support the accident management strategy and to inform requirements for robustness of plant and equipment to withstand accident conditions. Requirements for off-site emergency planning under REPPIR [25] include a requirement that all events be considered, irrespective of frequency, and so this is expected to include low frequency events which are severe accidents. These aspects are considered further in Section 5.7.

## Identification of Severe Accident Phenomena

1. SAA should be based on an adequate understanding of severe accident phenomena (SAPs paragraph 671); these are likely to be specific to the type of facility and in the case of NPPs to the reactor technology employed. The inspector should be looking for the safety case to identify and describe the relevant phenomena in terms of the nuclear, chemical and physical processes involved and the circumstances under which the phenomena could occur. The purpose of identifying severe accidents phenomena is to understand what needs to be mitigated, controlled or prevented; this should then allow suitable severe accident measures to be identified and, through analysis, the measures shown to be effective against the phenomena.
2. For light water reactors (LWRs) and other established reactor designs the licensee will be able to refer to the substantial body of information from international publications and guidance such as IAEA SSG-2 [28]. The key phenomena are expected to involve challenges to the containment and are likely to be drawn from the following:
* In-vessel fuel degradation, melting, relocation and interactions
* In-vessel steam explosions from molten fuel/water interactions
* Direct containment heating from high pressure ejection of fuel materials
* Ex-vessel steam explosions from molten fuel/coolant interactions
* Generation and dispersion of flammable gases such as hydrogen and carbon monoxide within the containment and the potential for combustion, deflagration and detonation
* Ex-vessel molten core-concrete interactions
* Criticality (and re-criticality) due to relocation/reconfiguration of fuel and core materials
1. For novel types of reactor the licensee will be expected to demonstrate that the list of phenomena is complete and where necessary the understanding of these is supported by relevant research and experimental evidence.
2. For other types of nuclear facility the severe accident phenomena may be less complex than for reactors and in many cases (such as physical relocation and direct radiation) these may be the same phenomena already considered as part of DBA. Examples of phenomena for nuclear fuel cycle facilities (e.g. those covered by the scope of SSR-4 [5]) could include:
* Overheating/boiling of thermogenic radioactive liquors
* Fires in radioactive material handling facilities and waste stores
* Dispersal of radioactive materials due to energetic events
* Criticality accidents
1. For all types of facilities there may still be significant uncertainty about what phenomena could actually be involved. For example, for legacy facilities it may not be possible to determine the initial state of nuclear material. The inspector should be seeking confidence that the licensee understands the types and severity of phenomena that could be involved and has explained the basis for any assumptions made in the SAA.
2. Many of the severe accident phenomena involve complex physico-chemical processes which can play a significant part in the progression and radiological consequences of accidents. NS-TAST-GD-089 provides guidance on chemistry in general and Appendix 2 therein considers some of the key accident phenomena for LWRs designs. The types, quantities and properties of the radioactive materials, both within the plant and those that could be released, will define source terms for consequence modelling. For core melt scenarios the grouping of radionuclides based on chemical and physical properties will provide a key input for SAA codes which will model the behaviour of the materials within the plant. Similarly, the transport and mass transfer of radionuclides within a reactor and more widely within the containment will be influenced by chemistry, as will the design of severe accident mitigation measures such as filters and systems for controlling hydrogen. For reactors and also some fuel cycle facilities, consideration of accident chemistry is therefore likely to be a significant factor affecting the progression and consequences of severe accidents. The ONR assessment of a licensee’s submission should include an appropriate input from ONR’s Chemistry specialism to ensure that the relevant phenomena have been adequately considered.
3. Some phenomena may be claimed to be physically impossible or that their likelihood of occurrence is very low such that no further consideration as part of SAA is warranted; the licensee should substantiate such assertions with appropriate analysis, discussion and where necessary reference to experimental and research evidence.

## Selection of Severe Accident States and Sequences

1. SAPs FA.15 expects that accident states, scenarios and sequences which are more severe than those considered as part of DBA should be subject to SAA. The PSA may provide a basis for identifying candidates for consideration as part of SAA. States and scenarios should not be dismissed from the analysis simply on frequency grounds alone (paragraph 666 of the SAPs); the inspector will need to make judgements on the adequacy of the scope of the analysis on a case-by-case basis and informed by risk. Furthermore, a state or scenario considered to be practically eliminated may still require SAA as part of any demonstration (see Section 5.9). The focus of the analysis should be on how severe accident states or scenarios would be controlled and/or mitigated, not on the sequence of internal or external events that may have led up to the accident. In accordance with paragraph 609 of the SAPs, the inspector should be looking for evidence that the selection includes:
* high consequence events of very low frequency for which the design safety measures may be ineffective; and
* design basis events where, conservatively, the safety provisions are assumed to fail.
1. Paragraph 663 of the SAPs also recognises that the severity of an initiating event included in the DBA may in reality exceed that assumed in the analysis. In the case of external and internal hazards, EHA.7 and paragraph 248 of the SAPs expect that the identification and analysis of severe accidents should be informed by the potential for cliff edge effects (at a hazard severity just beyond that considered in the DBA and which places a demand on severe accident measures).
2. The accident states to be considered should be those which give rise to, or could give rise to, a severe accident as defined in the SAPs (see Section 5.1 of this document). ONR’s intention is that this definition should encompass IAEA’s expectation for consideration of design extension conditions with core melt (also referred to as DEC-B by WENRA).
3. It is not expected that the licensee should analyse every possible severe accident state and sequence in detail, however all operating modes and containment states should be covered, e.g. by identifying a set of bounding fault sequences and grouping each individual sequence with one of the bounding set. Where states are grouped the inspector should expect to see a clear rationale which takes into account factors such as the initial conditions for the accident state (including radioactive source terms), the expected sequence progression and the roles of the measures that are needed to mitigate the severe accident phenomena.
4. FA.16 of the SAPs expects that SAA should be used in the consideration of further risk-reducing measures. Relevant accident states and sequences should be selected to provide the basis for:
* The identification of options for preventing progression and/or mitigation of accidents and to demonstrate the effectiveness of severe accident measures against the identified phenomena.
* Providing information on accident progression, such as on event timings, required operator actions, releases and consequences, and for informing accident management strategies and emergency plans.
* Providing deterministic analysis of accident sequences (both mitigated or unmitigated) where necessary to support Level 2 and Level 3 PSA.
1. To support these purposes, the licensee may need to analyse the progression of unmitigated accidents, i.e. those where conditions have reached a severe accident state, but subsequently where no credit is then taken for Level 4 defence in depth measures. The objective would then be to re-analyse the accidents to show the effectiveness of any measures (where these exist) that would help to control accident progression and/or mitigate any consequences. To support development of accident management strategies and procedures, the SAA may additionally need to consider more realistic scenarios to reflect where operator actions are able to influence the progression of the accident.
2. For a NPP, accident states and sequences with the potential to challenge the containment, resulting in a risk of an early release or a large release, should be subject to particular attention (see also discussion in relation to practical elimination in Section 5.9). For this purpose the selection of sequences should therefore include the following accident categories:
* Prompt reactor core damage and consequent early containment failure, such as from failure of a large pressure-retaining component or uncontrolled reactivity accidents.
* Early containment failure, such as highly energetic direct containment heating, large steam explosion or explosion of combustible gases.
* Late containment failure such as base-mat penetration or containment bypass during molten core concrete interaction, long term loss of containment heat removal or explosion of combustible gases.
* Containment bypass due to leakage, consequential failures or open containment states.
* Significant fuel degradation in a storage fuel pool and uncontrolled releases.
1. For other types of facility the accident states and sequences may be more limited in scope and complexity, but (subject to meeting the criteria in paragraph 664 of the SAPs) may potentially include:
* Release of radioactive materials from places of confinement.
* Unshielded radioactive materials.
* Uncontrolled criticality events.

## Severe Accident Safety Measures

1. The use of the term ‘severe accident safety measures’ here is intended to include SSCs and associated human actions, which either individually or in combination, prevent escalation of severe accidents and/or mitigate the consequences. These form part of measures which deliver safety at Level 4 defence in depth (as defined in SAPs paragraph 152). SSCs may include permanent engineered features and mobile equipment under the control of the licensee. The IAEA uses the term ‘safety feature’ to refer to plant and equipment that is intended to provide a safety function for design extension conditions (including severe accidents); such features fall within the wider scope of severe accident safety measures which is the subject of this section.

### Identification of Safety Measures

1. Regardless of events leading to a plant/fuel degraded state, the international expectations and those of ONR are that a modern nuclear facility should have design provisions for severe accidents such that radiological consequences are mitigated and that the risks are reduced ALARP. The provisions need to consider the fundamental safety functions of reactivity control, cooling and confinement of material/shielding. These should be appropriate to the type of facility and the hazards that exist.
2. The safety functions may involve preventing further progression of a severe accident (for example by restoring cooling), and/or by mitigating the accident consequences (for example by providing filtered venting to minimise containment overpressure or by providing shielding). Depending on type and age of the facility, safety functions are likely to be delivered through some combination of:
* passive design measures;
* active design measures (either automatic or manually initiated) which are permanent and fixed;
* mobile plant and equipment kept either on-site, or at some remote off-site location under the control of the licensee; and/or
* human actions that support the delivery of any active measures and mobile equipment.
1. The expectations of EKP.5 for the preferred hierarchy of the measures do apply, but the inspector should consider each facility and severe accident scenario on its merits. The rate of accident progression is likely to be a key factor in determining which type of measures are needed. For example, a high consequence criticality accident (due to failure of measures identified from DBA) is likely to be sudden and passive measures such as shielding may provide an important means of mitigating the consequences. For other situations there may be significant grace times before accidents escalate; in these scenarios there may be time for systems to be activated by the operator, or even for dedicated mobile equipment to be brought into use.
2. For new reactor designs, the safety measures included for severe accidents could potentially vary greatly from one reactor technology to another. The reactor technologies presented to ONR for Generic Design Assessment (GDA) have adopted different approaches, for example on the extent of claims made on active or passive SSCs, or permanent and mobile equipment. Use of mobile equipment may be one way of demonstrating additional defence in depth at Level 4, for example for longer term sequences to support restoration of cooling. Any claims for mobile equipment, for example on deployment times and equipment survivability, need to be justified and demonstrated through use of analysis and regular exercising.
3. For existing facilities that are not designed to modern standards, back-fitting of fixed engineering measures may not be reasonably practicable. For some facilities, provision of mobile equipment specified to deliver the same functions may provide an adequate alternative. However, the licensee should justify through use of analysis that equipment can be deployed and deliver the required safety function within sufficient time to be effective. Any requirements should inform the licensee’s accident management arrangements.
4. Where identified safety measures include the use of mobile equipment, international expectations [4],[38] are that there should be permanent connecting points. Where such equipment forms part of the accident management strategy, any connecting points should be accessible under the relevant accident conditions. This may include any physical conditions, for example due to extreme hazards where these are initiators of the severe accident, and also radiological conditions.
5. At some types of facility, measures beneficial in a severe accident may have multiple purposes. This may include standard equipment and supplies that have wider day to day uses, for example pumps, generators and supplies for effecting repairs. If specific items are required to deliver the licensee’s accident strategy, then the expectation is that these should be identified as items important to safety in a similar manner to fixed equipment. However, it may not be proportionate to identify all equipment in this way if this just provides a supporting role and can be sourced from multiple locations.
6. The licensee may also choose to consider how other mobile equipment could be used, such as that made available by off-site agencies or under mutual aid arrangements. Such equipment may support part of a ‘best-endeavours’ approach where the licensee’s own equipment has failed or cannot be deployed, or it may provide a supplementary capability. Whilst this may compliment the licensee’s approach to defence in depth, this should not be considered as a replacement for provisions which are under the control of the licensee.

### Performance and Characteristics

1. The performance and characteristics of the identified SSCs should be sufficient to deliver the identified safety function(s). The requirements should be informed by the licensee’s analysis of the identified severe accident scenarios and reflecting the phenomena that need to be prevented or mitigated. For a new design this may involve an iterative process to arrive at a final set of performance characteristics that meet safety objectives. For an existing plant the analysis may be required to demonstrate that the installed provisions will deliver the safety objectives, or identify improvements that need to be made to ensure that these objectives can be met.
2. The licensee’s analysis should also inform an understanding of the timescales for deployment (when does the SSC need to be available) and mission time (how long will the SSC be required to operate).
3. The inspector should be looking for evidence that the key performance requirements have been articulated and that these are supported by the licensee’s analysis. There should be evidence that the requirements are sufficiently flexible to deal with uncertainties and limitations in the analysis. For most nuclear facilities, one or more of the following are likely to be of interest to the inspector:
* consideration and capability of passive heat loss;
* shielding capability;
* cooling system capacities (e.g. pumping rates and available volumes);
* efficiency and capacity of containment sprays;
* measures for controlling chemistry (e.g. pH in the containment);
* containment performance;
* relief and venting capacities;
* filter performance and efficiency;
* performance of other passive devices, such as passive autocatalytic recombiners; and
* equipment for monitoring plant conditions.
1. Any human resources and operator actions required to support delivery of the safety functions should be identified by the licensee (SAP EHF.3). The performance expectations, for example taking into account timescales and any adverse working conditions, should be informed by the licensee’s severe accident analysis. Further assessment may be carried out by a Human Factors inspector against NS-TAST-GD-063 and the wider EHF SAPs, for example to consider whether any human actions are identified and whether tasks have been subject to proportionate analysis and substantiation. The level of attention by the inspector should be informed by factors such as the risk importance and novelty/complexity of the task.
2. There should be evidence that the severe accident mitigations/recovery provisions will be robust against any hazards such as seismic events, flooding and extreme weather conditions which are identified as pre-cursors to the severe accident. Consideration of the identification and severity of the relevant hazards will be a matter for an External Hazards inspector in accordance with expectations in NS-TAST-GD-013.
3. Engineering substantiation of individual SSCs against performance requirements will be of interest to the wider inspector community, in particular the engineering disciplines, but this is outside the scope of this guidance. For this, the various engineering SAPs and TAGs will be the relevant source of reference.

### Support Systems and Supplies

1. The support systems needed to initiate and maintain the operation of the SSCs should be identified. Common examples of support systems are likely to be:
* control and instrumentation;
* electrical power;
* cooling systems and heat sinks, and
* HVAC.
1. The licensee’s safety case should include evidence to demonstrate that the requirements for provision of adequate on-site supplies of consumables to support the identified SSCs over an initial period of operation have been considered. This could include supplies of fuel, lubricants, water, compressed gases and chemicals, etc. Consideration should be given to the vulnerability of storage locations to any hazards which could be the cause of the accident. There should be an understanding of how consumables would be re-supplied from off-site over a longer period to support the objective of achieving a safe, stable state.
2. Key learning from Fukushima Daiichi accident was the need to be able to support the welfare of operators/responders over a prolonged period of time, potentially in the absence of normal regional or national infrastructure. Where necessary there should be consideration of any requirements for accommodation, food & water, sanitation, medical supplies, etc.

### Independence and Defence in Depth

1. A key engineering principle in the SAPs (EKP.3) is that nuclear facilities should be designed and operated such that defence in depth is achieved by the provision of multiple independent barriers to fault progression. Using the scheme in SAPs paragraph 152, this means that severe accidents measures at Level 4 of defence should normally be independent from those at Levels 1, 2 and 3. Success of the defence in depth approach hinges on independence between the levels and not (ordinarily) claiming earlier levels in the response of later ones without very good reason. By definition, a severe accident state will normally have occurred due to failure of measures earlier in the fault progression, where such measures have been bypassed, or where conditions exceed those assumed for SSCs identified as part of DBA.
2. The expectation is therefore that the licensee’s SAA will normally assume that the safety measures identified for Level 3 protection are unavailable, although the inspector should be aware of any potential for partial success of Level 3 measures to make the situation worse. The purpose of the analysis should be to determine the additional safety measures required to regain control of the accident. There may however be exceptions to rules for independence; for example, in cases where multiple independent safety measures exist at Level 3 an argument could be made that adequate Level 4 protection / mitigation is provided by Level 3 plant and equipment. There may also be scenarios where success or failure of equipment at Level 3 does not influence the progression to the severe accident and so this equipment may provide a benefit at Level 4. Arguments of this type need to be considered on their individual merits, taking account of aspects such as the degree of redundancy / diversity within the Level 3 measures and the extent of vulnerabilities to common cause failures. In certain situations it may also be appropriate to consider the potential for recovery or partial recovery of Level 3 measures where timescales and conditions allow.
3. An effective way of achieving independence between levels of defence in depth is by provision of diverse and segregated measures at each level. The inspector should be looking for consideration of diversity, particularly where there are challenges to the independence between measures at Levels 3 and 4, for example due to common mode and common cause failures.
4. Human error is one type of common cause vulnerability that could be a challenge to the independence of the Level 4 safety measures from preceding levels. Where reliance is placed on human actions, consideration should be given to potential dependencies between human actions required by the DBA and actions required by SAA. Further guidance on consideration of dependency can be found in NS-TAST-GD-063 Human Reliability Analysis [13]. Appropriate ONR Human Factors specialist advice should be sought if this is expected to be a significant consideration in the assessment.
5. Severe accident measures should be resilient against adverse conditions that may arise as a consequence of the accident sequence. Level 3 defence in depth measures may not be available in the case of hazards which exceed the severity assumed for DBA. The licensee should demonstrate that independent measures at Level 4 can still deliver the required safety function with a sufficient margin beyond the DBA hazard level.

### Redundancy

1. The safety case should explain any assumptions made about the availability of severe accident SSCs and supporting human actions. Consistent with international expectations [28], the unavailability of a severe accident system or system component due to maintenance does not need to be assumed and there is no requirement for the single failure criterion to be applied in the SAA to demonstrate delivery of the safety function. Subject to constraints defined in its safety case, the licensee may identify a need to take severe accident systems out of service for maintenance; this may be needed for statutory reasons or to justify reliability assumptions made in the PSA. This needs to be supported by an appropriate justification, which may involve probabilistic considerations of the benefits and risks.

### Multi-facility Sites

1. Where a site comprises multiple facilities, the inspector should look for evidence that the licensee has identified any requirements for managing severe accidents concurrently across facilities. For example, a severe external event (such as an earthquake or a site flood) could cause common loss of site services (e.g. loss of off-site power) affecting multiple facilities at the same time. There may also be multiple events across a site, which when taken in totality, warrant consideration as a severe accident. Any potential for an accident at one site to escalate to another, or for interactions between sites, should also be identified. For these situations the licensee should be able to demonstrate that there are adequate safety provisions in terms of the types and quantities of equipment and supplies to ensure a coordinated response and that the requirements for human resources have been considered.

### Classification of Safety Measures

1. Categorisation of safety functions and safety classification of safety measures should not be limited to Levels 1, 2 & 3 of defence in depth. The scheme in NS-TAST-GD-094 provides an example of how safety functions might be categorised for high consequences events which fall outside of DBA. Where there is high hazard potential, the expectation is that the licensee’s own scheme should include provision for categorising safety functions which are required to prevent escalation of accident conditions or mitigate the consequences of severe accidents. Classification should then follow using the licensee’s scheme for determining the safety significance of SSCs and human actions. The inspector should expect to see categorisation and classification applied at Level 4 defence in depth, but this may not be appropriate for non-engineered provisions which will likely dominate at Level 5.
2. Using such approaches, SSCs for severe accidents are likely to have lower classifications than those measures identified in the DBA as the principal means of delivering safety. As such, the plant and equipment required for severe accidents, need not necessarily be substantiated to deliver their required safety functions to the same level of confidence as DBA measures. However, this needs to be considered on a case-by-case basis taking into account the importance of the safety function and level of robustness required (SAPs paragraph 673).
3. Where the licensee’s SAA identifies a need for severe accident measures, or where these are identified as having a benefit, the expectation is that these should be assigned an appropriate classification. Severe accident SSCs should be subject to through-life maintenance, testing and inspection commensurate with the safety classification (ECS.3). This should include non-permanent SSCs which should be maintained commensurate with their safety classification. Expectations on classification should not necessarily preclude the use of other (non-classified) equipment on a best-endeavours basis if those managing accident response on the day consider that this would provide a safety benefit.
4. There is an expectation that human actions that deliver safety functions should be identified for all conditions, including for severe accidents (EHF.3) and that, in accordance with paragraph 164 of the SAPs these should be subject to safety classification analogous to that for SSCs.

### Input to Equipment Qualification

1. Paragraph 175 of the SAPs and EQU.1 sets the expectation that equipment qualification procedures should, where appropriate, address severe accident conditions. This should include the severe accident measures, any essential support systems and the instrumentation and control that would be used for monitoring as part of the accident management. Whilst the level of confidence expected from qualification procedures may be lower than for design basis measures, it should be recognised that equipment may be exposed to more challenging conditions.
2. Regulatory judgements on the adequacy on equipment qualification will primarily be a matter for specialist inspectors from engineering disciplines. However, severe accident analysis should be used to identify expected extremes of physical, chemical and radiation conditions to inform requirements for equipment qualification.

## Analysis Techniques

1. The main purpose of deterministic safety analysis should be to confirm that safety measures delivering plant safety functions are sufficiently effective for postulated faults and accidents. For reactors, deterministic analysis performed as part of SAA typically involves the use of specialised and often complex theoretical or empirical methods, normally implemented as computer codes. For spent fuel pools and other types of facility, modelling may involve the use of more simplistic codes, or an extension of codes used for DBA. The AV series of SAPs, together with ONR’s TAG on the Validation of Computer Codes and Calculation Methods NS-TAST-GD-042 [12] provide relevant guidance for the inspector on judging the adequacy and application of the methods and codes, including those used for SAA.
2. SSG-2 [28] provides relevant international guidance on deterministic safety analysis for NPPs, with specific guidance for DEC with core melting in paragraphs 7.56-7.67. The inspector should consider the general principles in this guidance to be relevant good practice for SAA carried out for all types of facility.

### Methods, Codes and Model Development

1. Mature severe accident system codes such as MAAP, MELCOR and ASTEC have been used extensively by licensees to substantiate the claims made for LWRs. These codes and the underpinning methods have been the subject of significant development to accommodate new reactor design features relating to aspects such as in-vessel melt retention and ex-vessel core catcher strategies. There has also been increasing use of codes to model accidents involving spent fuel pools and some have also been developed for application to novel reactor technologies.
2. The licensee may also need to supplement its use of system codes with other codes which look at specific phenomena. These may be stand-alone or coupled with system codes. General Computational Fluid Dynamics (CFD) codes which have application beyond SAA may also be used. Appendix 1 of NS-TAST-GD-042 provides further guidance on the assessment of CFD simulations in safety cases.
3. For non-reactor facilities the licensee’s SAA may involve the use of standard nuclear industry methods and codes to analyse aspects such as criticality accidents, shielding, release and dispersion. In many cases these could be an extension of the methods used for DBA, albeit with different assumptions compatible with SAA requirements, and so the licensee and the inspector may be able to draw on evidence already presented in other parts of the safety case.
4. Whatever approaches are used, the licensee should present a clear rationale and justification for its selection of codes for use in SAA. The underlying methods should be capable of representing the relevant severe accident phenomena and be suitably validated for the circumstances (AV.2 & AV.3 of the SAPs). Licensees should be taking credit for the research, experiments and benchmarking that have been utilised in the development of the methods and codes. The accidents at the Fukushima Daiichi plants have provided significant data that are helping to better understand key accident phenomena and help reduce the uncertainties. The inspector should be looking for evidence that the methods are cognisant of the latest available knowledge, but should be wary of the use of novel approaches based on weak validation evidence or approaches where there is insufficient consensus from the severe accident community.
5. Using its choice of code(s), the licensee should develop a model which represents the relevant features of the plant (AV.1 of the SAPs). This should include an adequate level of detail to support the aims of the SAA (SAPs paragraph 672). It should be confirmed that codes are being used within the limits of applicability, or justification provided accordingly.
6. The licensee should be able to demonstrate that it has an effective process for ensuring all aspects of quality control governing the use of the codes (AV.4 of the SAPs). Whilst the quality management expectations for SAA may be less onerous than for analysis which supports DBA, the licensee should still be able to demonstrate that it has suitable controls in place.
7. ONR’s guidance on calculational methods in NS-TAST-GD-042 provides general guidance on user effects. The inspector may be able to gain confidence of the licensee’s arrangements for ensuring user proficiency from consideration of its other analyses, such as DBA. However, the inspector should be mindful that the greater complexity of severe accident modelling and the scarcity of experimental data may require specific consideration.
8. In accordance with AV.5 of the SAPs, the licensee should be able to produce documentation which supports the use of the methods and codes, such as code user guides, validation reports, uncertainty studies and input decks.

### Conservatism, Sensitivities and Treatment of Uncertainties

1. The licensee should include a consideration of areas of optimism, uncertainty and conservatism in its safety case (SAPs SC.5). The importance of this is recognised in ONR’s ‘Risk informed regulatory decision making’ [40]. SAA inherently involves more uncertainty than other forms of analysis and so the inspector’s regulatory decision-making will need to be informed by a thorough understanding of any uncertainties.
2. In line with paragraph 669 of the SAPs and the international guidance on analysis of design extension conditions [28], a best-estimate approach should normally be followed for SAA. For the purpose of informing accident management strategies and emergency planning, SAA should be approached with the intention of evaluating the progression of events in as realistic a manner as possible. However, this may not be appropriate when designing a severe accident safety measure (or group of measures) to deliver a safety function. In this case the inspector should consider the assumptions made by the licensee on the operation of other systems which provide mitigation earlier in the accident sequence and consider whether these are consistent with the licensee’s arguments for defence in depth. For example, the design of in-vessel retention for a reactor should be on the basis that efforts to prevent core relocation have failed. The inspector should be satisfied that appropriate initial conditions have been chosen, noting that these may be different depending on the phenomenon and the system being considered. Having determined the initial conditions, the expectation is that adequacy of the safety measures should then be demonstrated on a best-estimate basis.
3. The inspector should also be wary of conservatism because severe accident phenomena are often diverse, complex and potentially counter intuitive. This leads to situations in which a ‘conservative’ assumption in one area can potentially produce a non-conservative outcome in another. Indeed, what is ‘conservative’ in DBA may potentially become ‘non-conservative’ in severe accident conditions. The inspector should also be aware of the use of overly conservative assumptions to drive perverse outcomes, such as an incorrect conclusion that no further reasonably practicable measures can be implemented.
4. The challenge of correctly and accurately predicting severe accident phenomena is considerable and limited direct experimental evidence is available to validate the methods in an integrated manner. Where there is major uncertainty in the physical phenomena, it is appropriate to consider the level and impact of this uncertainty as discussed below.
5. The licensee is expected to describe any assumptions, simplifications and areas of uncertainty in the methods. It is also expected that sensitivity studies will be performed to understand such effects and determine the significance of these (AV.6 of the SAPs). A key uncertainty in the SAA will often be the manner in which the accident progresses. There will often be several accident paths, for example at Fukushima Daiichi different scenarios developed on the different units. This can be strongly affected by the type and timing of operator interventions and the actual performance of equipment.
6. The uncertainty analysis should attempt to explore the variations to scenarios that could develop as the accident progresses and the factors that determine which accident path will be followed. Sensitivity analyses should be used to check that there are no sudden escalations (‘cliff edges’) in consequences just beyond the analysed conditions, and for example that assumptions of equipment sizing remain valid. Where uncertainties are such that realistic analysis cannot be performed with confidence, a more conservative approach may be needed. In such cases the licensee will need to consider the extent to which predictions from SAA can still be used to inform accident management.
7. In view of the variety of potential applications of SAA, no general rules for the analysis of uncertainties have been included in this TAG. This is an ongoing area of research within the international community. The general message to inspectors is to seek an approach where licensees are clear about any uncertainties and any conservatism applied in the SAA and are in a position to understand their effects.
8. Where the uncertainties are large, and in line with SAPs paragraph 671, inspectors should be seeking confidence that the licensee is doing all that is reasonable to underpin the assumptions and simplifications in their SAA. In general, the licensee should be able to demonstrate they are up to date regarding relevant areas of research and the current international consensus, are being proactive in learning from accidents and that where necessary are supporting further work in areas of key uncertainty.
9. It would be beneficial for the inspector to be aware of major research programmes and be informed by current international thinking on severe accident topics. The various publications produced by the OECD’s Nuclear Energy Agency may be one useful reference source for the inspector.

### Independent Confirmatory Analysis

1. To support assessment of novel or complex submissions, inspectors may consider commissioning independent confirmatory analysis to support and inform the overall regulatory judgements and outcome. Undertaking independent confirmatory analysis is a valuable method to gain insights into the licensee’s SAA. The overall objective of ONR’s confirmatory analysis is to gain confidence in the licensee’s analysis and that SSCs will be able to deliver the required safety function. It can reveal the impact of user and code effects and model sensitivities on key claims made in the licensee’s analysis. The ability of the licensee to supply data, boundary conditions and explain modelling assumptions to support independent analysis is a good way to form a view on quality control (AV.4 of the SAPs) and the analysts’ understanding and experience. Regardless of whether ONR chooses to commission its own independent confirmatory analysis, it is important to recognise that it is the licensee that needs to demonstrate the safety of the facility through its own analysis.
2. The independent confirmatory analysis undertaken should be proportionate, with the most likely applications being in limited circumstances where novel applications or complex scenarios are proposed. When such analysis is carried out, the inspector should ensure that there is a clear scope and purpose. Where necessary this may need to involve collaboration with other disciplines (for example chemistry and PSA) to consider common areas of interest and the interfaces with their own work streams. Analysis should always be targeted, for example to judge the adequacy of the licensee’s overall analysis based on a sample of severe accident scenarios, to consider in detail the treatment of a particular complex phenomenon or to better understand key sensitivities.
3. ONR does not prescribe what codes should be used by licensees, nor is it committed to one particular code for its independent confirmatory analysis. Should a submission have used MAAP, the inspector may consider another independent code such as MELCOR, but this is not always essential. Sharing the outcome of confirmatory analyses within the international regulatory community can help provide additional insights, particularly relating to new reactor designs.

## Severe Accident Management

1. This section provides advice to the inspector on how SAA should be used to inform the development of accident management strategies and procedures, and also on preparation of emergency plans for protection of the public (paragraph 672 of the SAPs). These aims of SAA support the requirements of SAPs FP.7 which, reflecting UK law, states that arrangements must be made for emergency preparedness and response in case of nuclear or radiation incidents. Consistent with the REPPIR Approved Code of Practice [25], ONR’s expectation is that these arrangements should, in a suitably graded way, consider all incidents irrespective of frequency, including those which are severe accidents.
2. ONR’s guidance on AM.1 of the SAPs refers to ‘emergency operating procedures’ and ‘accident management guidelines’, although licensees may use other terminology. For NPPs the former (EOPs) typically provide guidance to plant operators on prevention, control and mitigation of design basis events. These should be informed by the licensee’s DBA and are not considered further here. Accident management guidelines, sometimes referred to as severe accident management guidelines (SAMGs), typically extend the guidance to situations where the plant has entered a severe accident state, or where this is judged to be imminent.
3. AM.1 of the SAPs, together with duties covered by the REPPIR regulations, should guide the scope and content of the licensee’s accident guidelines and procedures. A regulatory assessment of the accident guidelines/procedures and the wider set of emergency arrangements implemented by the licensee is likely to require input from a number of ONR disciplines. Such an assessment is covered by other guidance such as NS-INSP-GD-011 [24], but should be informed by ONR’s understanding of the licensee’s SAA.
4. IAEA’s publication on Accident Management Programmes for Nuclear Power Plants, SSG-54 [32] provides useful detailed guidance to inspectors on the factors that should be considered by the licensee in developing accident management strategies and guidelines and how these link to SAA. For existing reactors the WENRA Reference Levels [38] for ‘Issue LM’ (Emergency Operating Procedures and Severe Accident Management Guidelines) and ‘Issue R’ (On-site Emergency Preparedness) are also relevant. Many of the principles are generic and these recommendations may also be applied with judgement to other types of nuclear installation. Whilst these guidance documents provide useful background on how SAA should inform guidelines and procedures, the development of these is not the focus of this TAG.
5. Paragraph 776 of the SAPs states that accident management guidelines should be based on the facility’s SAA. The inspector should be looking for the SAA (supported by aspects of the PSA) to provide the following:
* a representative selection of initial accident states;
* appropriate points for the transition into accident management guidelines (see paragraph 133);
* the symptoms that will allow the operators to identify the true state of the plant;
* alternative scenarios for how accident sequences might progress and an analysis of the likely effectiveness of different strategies for these;
* the plant monitoring functions that are required to support the delivery of the severe accident measures;
* the required plant and equipment (including mobile equipment) and the associated human actions to deploy these;
* the timescales for key operator actions;
* environmental conditions within and around the plant and the effect on deployment of equipment and people;
* defining mission times for plant and equipment and the supply of consumables; and
* expected radiation dose levels on- and off-site.
1. The licensee should explain how it has used the SAA and PSA to arrive at a representative set of accident scenarios covering the most likely accident states and outcomes. Obscure accident sequences may have been considered for the purposes of the PSA, but there may be little benefit in these being the focus for accident management, particularly if the sequence frequency is comparatively low. Any guidelines would be expected to consider all areas of the plant where a severe accident could occur and cover all modes of operation. For example, for a NPP this would also be expected to include the spent fuel pool and reactor shutdown modes.
2. The criteria for entry into the severe accident domain (with an associated change in procedures and guidelines to follow) should be clearly defined and informed by results from the licensee’s SAA. The specific criteria will depend on the nature and design of the facility, but is typically expected to relate to the occurrence of a cliff-edge in hazard or risk. This could be associated with loss of one or more containment barriers or some irreversible change to the state of the plant requiring a shift in emphasis from prevention / control to mitigation. For NPPs this could be linked to the likely onset of fuel degradation and might typically use parameters such as core-outlet temperature (for Pressurised Water Reactors) or water level (for Boiling Water Reactors), together with an increased radiation level in the containment. For other types of facility the transition could simply be linked to a step change in measurable radiation consequences.
3. Radiological consequence analysis carried out for severe accident sequences should provide an input to off-site emergency planning (SAPs paragraph 624), for example to determine the extent of the detailed and outline planning zones required under REPPIR. Where the hazard potential is significant, paragraph 771 of the SAPs states the REPPIR Hazard Evaluation and Consequence Assessment (HECA) should be informed by SAA. Regulatory assessment of a REPPIR duty-holder’s HECA is not covered by this TAG, although any such assessment should be informed by an understanding of any underpinning SAA (and the DBA and PSA).

## ALARP

1. The Health and Safety at Work etc. Act 1974 places a duty on licensees to reduce the risks from their activities ‘so far as is reasonably practicable’ (SFAIRP). ONR uses the term ‘as low as reasonably practicable’ (ALARP) as a convenient means to express this legal duty. General ONR guidance on expectations for ALARP is set out in NS-TAST-GD-005 [6]. A purpose of SAA is to assist in the identification of any reasonably practicable measures which could prevent the progression of a severe accident or mitigate the consequences and therefore has an important role to play in the demonstration of ALARP.
2. By definition, severe accidents should be low frequency events which can only occur when robust measures, for example those identified through DBA, have failed or have been overcome. The nature of severe accidents and the conditions they can generate means that that any additional design features are likely to be expensive. Pure cost-benefit analysis techniques may therefore be of limited value in ALARP decision making.
3. In contrast, RGP has an important role to play in judging the adequacy of severe accident provision, particularly for existing facilities where circumstances are similar or there is the potential to retrofit solutions based on established technologies. However, the inspector should be open minded about alternative ways to achieve the required safety outcomes, even if the design solution is different to that seen elsewhere. The objective should be for the licensee to use SAA to demonstrate the effectiveness of the chosen approach and show that this delivers a comparable level of safety to other examples of RGP.
4. For new plants using novel technologies there may be limited examples of RGP. In the case of new reactor designs, such as those considered in a GDA, the inspector should treat each design on its merits and should not be unduly influenced by ALARP decisions and choices made in earlier GDAs for alternative reactor designs. The ONR assessment objective instead should be to be satisfied that the licensee’s use of SAA supports a conclusion that all reasonably practicable measures have been identified.
5. It is important to recognise that RGP is not fixed and will evolve, sometimes in a significant way, especially after major events such as Three Mile Island, Chernobyl and Fukushima Daiichi. It also should be recognised that what is reasonably practicable when designing a new facility may be grossly disproportionate for an existing facility.
6. The results of the PSA for severe accident scenarios and comparisons against measures such as ‘core damage frequency’, ‘large release frequency’ and Targets 7, 8 and 9 of SAP NT.1 can also provide valuable risk-based contexts for ALARP judgements made by both the licensee and ONR.
7. There may be cases where the licensee argues that the risks associated with severe accidents are below its defined criteria for further consideration via SAA. If the inspector is satisfied by these arguments, perhaps with reference to the ONR’s Basic Safety Objectives (BSOs) in NT.1, it will usually be reasonable not to pursue the lack of SAA further. However, as stated in paragraph 701 of the SAPs, legal duties on the licensee to demonstrate that risks are ALARP do not stop at this level. Safety cases for high hazard facilities should still discuss severe accidents, consider whether the Level 4 defence in depth measures are adequate, and whether it would be grossly disproportionate (if applicable) to provide more design features. Such demonstrations are likely to interface with emergency arrangements, and again, inspectors should be open minded on whether the evidence of adequacy or the demonstration of ALARP sits within part(s) of the safety case covering severe accidents, or if it is contained within LC 11 arrangements (especially on operating facilities).
8. The requirement to demonstrate that risks have been reduced ALARP does not necessarily mean that ONR is demanding grossly disproportionate additional safety measures. Whilst a focus of the analysis is likely to be on the provision of engineered measures, there may still be reasonably practicable improvements that can be implemented, even if these have not been, or cannot be, explicitly accounted for in the SAA. For example, it may still be possible to optimise instrumentation, situational awareness, the ease of deployment of equipment, etc.

## Practical Elimination

### Applicability

1. The concept of practically eliminating early or large radioactive releases in the design of a nuclear facility is an example of where RGP has evolved over time. It is now established in international guidance, however it is only fully expected for new facilities. However, as with all RGP, it should be considered in periodic safety reviews of existing facilities in a proportionate way (i.e. facilities with the potential to have large or early releases, or high radiation doses). For periodic review this should be part of the overall consideration of whether there are any further reasonably practical measures that would reduce risks ALARP (see Section 5.8).
2. The application of practical elimination concepts in IAEA’s SSR-2/1 [4] and WENRA’s guidance [37] is restricted to the design of NPPs, but the latest IAEA guidance in SSR-4 [5] extends the usage of practical elimination to other types of high hazard facilities such as nuclear fuel cycle facilities. Article 8a of the Nuclear Safety Directive of the European Union [36] sets the objective that early or large releases should be avoided following an accident on any nuclear installations with a construction licence after August 2014. The Directive also states that this objective should be considered by relevant licensees as a reference for timely improvements on existing installations, including as part of periodic safety reviews.
3. In the case of new reactor designs considered as part of a GDA, the demonstration of practical elimination is likely to be a matter for the plant designer and undertaken as part of an iterative process to define and justify an acceptable design. In other situations, for example a new facility on an existing site, it will be the responsibility of the operator (licensee) to provide an adequate demonstration of practical elimination for the design being proposed.

### Definitions

1. The term ‘practical elimination’ is introduced in IAEA SSR-2/1 [4]. The requirement (for NPPs) is that:

“The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is ‘practically eliminated’.”

1. The terms ‘early’ and ‘large’ are defined broadly by IAEA in terms of the timing and geographical extent of off-site protective actions that could be implemented as part of Level 5 defence in depth:

“An ‘early radioactive release’ in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A ‘large radioactive release’ is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.”

1. WENRA’s Position 5 on practical elimination [35] is that:

“accidents with core melt which would lead to early or large releases have to be practically eliminated;” and

“for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures.”

1. In the context of nuclear fuel cycle facilities, IAEA SSR-4 [5] sets equivalent expectations:

“…facility states that could lead to high radiation doses, large radioactive releases or associated major chemical consequences are practically eliminated and that there are no facility states with more than minor potential radiological consequences with a significant likelihood of occurrence.”

1. SSR-4 refers to the practical elimination of high radiation doses as well as large releases. Although the aims are slightly different to those for reactors, the principles of producing a demonstration of practical elimination can be taken to be the same. Where applicable, chemical consequences referred to in SSR-4 are assumed to be covered by statutory provisions made under the Health and Safety at Work etc. Act 1974, such as the Control of Major Accident Hazard Regulations - this aspect is not considered further in this TAG.
2. In line with this international guidance, paragraph 611 of the SAPs states that SAA should form part of a demonstration that potential severe accident states have been practically eliminated. Unless justified otherwise by the licensee, the SAPs reference to ‘severe accident states’ should be taken to encompass plant states and conditions that could lead to an early release or large release.

### Demonstration

1. From an ONR perspective, the practical elimination of early or large releases with a high degree of confidence is a holistic safety case claim for the final design which needs to be suitably substantiated. It is not necessarily an additional accident analysis technique in addition those identified in SAP FA.1 (i.e. DBA, PSA and SAA). Rather, it is something that should be possible to demonstrate with reference to existing analysis.
2. Designers looking to improve on an existing design, may create a specific process to identify additional design features to ensure early or large releases are practically eliminated. Whether features identified through this process (and their supporting analysis) remain in a special category or they are subsequently incorporated into the wider Level 4 defence in depth measures and analysed with ‘routine’ SAA may be a consideration for inspectors to explore, pragmatically considering the implications of either approach.
3. Practical elimination is fully consistent with ALARP. In addition to being an example of evolving RGP for severe accidents, practical elimination provides a demonstrable target for what severe accident design measures should achieve whilst also contributing to evidence that further measures are not necessary.
4. ONR does not prescribe any set methodology, format or quantitative criterion for a demonstration of practical elimination. The inspector will need to consider each case on its merits and expectations will need to be guided by the purpose of the demonstration and matters of proportionality.
5. To date there are only limited available examples of how the requirements have been explicitly addressed by industry, and how demonstrations have been considered by regulators. Based on SSR-2/1 requirements, WENRA members have developed a common understanding of the term and the approach to demonstrating practical elimination [37]. This is consistent with ONR’s current thinking on the topic and provides a useful reference for the inspector.
6. There are likely to be several necessary components to any practical elimination demonstration submitted to ONR as part of a wider safety case:
* A definition of what constitutes an early or large release;
* Identification of scenarios, sequences or plant states which have the potential to lead to an early or large release;
* Fit-for-purpose demonstrations that the design, performance and reliability of safety measures are designed to cope with the scenarios which could result in an early or large release.
1. Whether or not a severe accident (as defined in this guidance) results in an early or a large release (or high radiation dose) will be dependent on many factors such as the type of facility, accident progression and the siting of the facility. The inspector should not assume any direct correlation between ONR’s expectation for SAA and need to demonstrate practical elimination; however in many cases the two are likely to be closely linked and such a demonstration is likely to require some form of SAA. To define what constitutes a large or early release, the licensee will need to apply judgement, which is likely to be plant and location specific. For example, for a reactor the licensee may consider that a release from containment of ‘x%’ of the core caesium iodide inventory constitutes a large release, or that a release within ‘y’ hours is an early release. These need to be defined in the context of the need for protective actions such as permanent relocation, emergency evacuation outside the immediate vicinity of the plant, sheltering, long term restrictions in food consumption etc.
2. UK Health Security Agency guidance on public health protection in radiation emergencies [41] establishes dose thresholds for actions in the form of Emergency Reference Levels (ERLs). This may be useful to the inspector in benchmarking criteria applied by an overseas plant designer to a GB context.
3. There are several ways for a licensee to identify scenarios with the potential to cause early or large releases. In most cases, it is expected these will be associated with severe accident scenarios that can cause the failure or bypass of the final confinement barrier (in the case of a LWR, the containment building structure). Both phenomenological (top-down) and sequence-orientated (bottom-up) approaches can be taken to either identify the ways the confinement barrier could fail or what the consequences of individual sequences are. All modes of normal operation should be considered (e.g. full power operation, refuelling and shutdown states, and any modes or activities associated with an open containment building). Similarly, all plant locations and buildings where there is a sufficiently high radiological hazard (typically where irradiated nuclear fuel is present) should be considered.
4. In the case of LWRs, IAEA guidance such as SSG-2 [28] can provide a good baseline list for the inspector to compare the licensee’s identification process against.
5. Those scenarios or phenomena which have been identified as a potential challenge to the final confinement barrier need to be shown in the final design to either be:
* physically impossible, or
* extremely unlikely to occur with a high degree of confidence.
1. Physical impossibility claims for practical elimination, with the emphasis on the inherent safety characteristics of the system or facility, can be credible. ONR inspectors should be supportive of design solutions that remove challenges which may have existed on previous facilities with a need for active management, and which instead result in either a complete absence of unacceptable loads or, due to inherent physical characteristics or static features, a significantly lower load on relevant SSCs than could cause their failure.
2. Significantly, consistent with the wider principle and objectives of practical elimination set out in the international guidance, claims of physical impossibility still need to be demonstrated / substantiated within the safety case, with methods consistent with SAA techniques. In other words, a claim of practical elimination is not an adequate reason for not doing SAA, rather it is something which needs to be substantiated through appropriate SAA.
3. In practice, the physical impossibility approach is likely to be limited on most types of high hazard facilities to a few very specific cases. Examples could be the elimination of hydrogen detonation by use of materials that do not generate hydrogen in accident conditions, or by ensuring sufficient physical separation to prevent propagation of failures between components. For the remaining phenomena and scenarios that cannot be eliminated by the inherent design, practical elimination needs to be demonstrated through a combination of deterministic and probabilistic arguments / analysis showing that early or large releases are extremely unlikely to occur because of the safety measures and features provided in the design (and any supporting operator actions and emergency arrangements).
4. The inspector should consider the following points when assessing arguments that large or early releases are extremely unlikely:
* Both the SAPs and international guidance are clear that demonstrations that early or large releases are extremely unlikely with a high degree of confidence cannot be purely a probabilistic test. PSA has an important role to play, but it should only be one leg of the safety arguments.
* Within that probabilistic leg of the safety arguments, it is for the licensee to propose a suitable numerical risk target for early or large releases that support the case it is making. The risk targets can be benchmarked against ONR’s Targets 8 and 9, as well as international RGP for large release frequency and other practical elimination demonstrations.
* Practical elimination with a high degree of confidence does not mean that deterministic severe accident analysis needs to be undertaken with the levels of conservatism and margins similar to those expected for DBA. Instead, confidence will usually be provided by highlighting the presence of multiple and robust levels of defence in depth, each one of which is appropriately robust and independent from other lines.
* The adequacy of the lines of defence in depth included in the design does need to be substantiated, but not necessarily through bespoke ‘practical elimination’ analysis. Existing analysis done under the auspices of DBA, ‘DEC A’, ‘DEC B’ / SAA and PSA can be referenced to support claims of adequacy, presence of safety margins, lack of cliff-edges, reliability, independence and common cause failure tolerance etc.
* Some extreme faults may be so catastrophic or immediate that early action of lines of defence in depth will not be possible to prevent fault escalation, the defeat of the final confinement barrier and a release to the environment. An example of such a scenario is a catastrophic failure of a reactor pressure vessel. In these scenarios, practical elimination arguments can reference deterministic arguments made elsewhere in the safety case as to why there is a high degree of confidence the vessel will not fail. This can be complemented by PSA which can put its hopefully small contribution to the risk of an early or large release into context with the risks from those faults that are protected by multiple layers of defence in depth.

## Fukushima Lessons Learned

1. The accident at Fukushima Daiichi in 2011 prompted wide-ranging reviews of nuclear safety. Whilst a number of resilience studies were performed by licensees shortly after the accident, ONR placed specific actions on licensees to review their designs against the emerging lessons from national and international reviews. The findings of the reviews were ultimately reported in the HM Chief Inspector of Nuclear Installations Final Report [42], the European Nuclear Safety Regulators Group Stress Tests [43],[44] and the IAEA Director General’s Report [45].
2. Whilst the Chief Inspector’s Final Report concluded that the UK approach for identifying the design basis for internal and external hazards was sound, the circumstances of the accident resulted in a heightened understanding of the importance of considering severe accidents. In relation to the analysis of severe accidents in licensee safety cases (including as part of the PSA), this led to recommendations that:
* The UK nuclear industry should review, and if necessary, extend analysis of accident sequences for long‐term severe accidents. This should identify appropriate repair and recovery strategies to the point at which a stable state is achieved, identifying any enhanced requirements for central stocks of equipment and logistical support.
* The nuclear industry should ensure that adequate Level 2 Probabilistic Safety Analyses (PSA) are provided for all nuclear facilities that could have accidents with significant off‐site consequences and use the results to inform further consideration of severe accident management measures. The PSAs should consider a full range of external events including “beyond design basis” events and extended mission times.
1. In the years since the Fukushima accident, the lessons and recommendations identified have been consolidated into revised ONR and international guidance, as well as industry practice. ONR inspectors should be looking to gain confidence that licensees have recognised the lessons, acted on specific recommendations (where applicable) and have carried out SAA in accordance with RGP.

# References

1. Safety Assessment Principles for Nuclear Facilities. 2014 Edition, Revision 1 January 2020.
<http://www.onr.org.uk/SAPS/saps2014.pdf>
2. Periodic Safety Review (PSR). NS-TAST-GD-050, Revision 8, October 2020.
<https://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-050.pdf>
3. IAEA Safety Standards – Periodic Safety Review for Nuclear Power Plants. Specific Safety Guide No. SSG-25, 2013.
https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1588\_web.pdf
4. IAEA Safety Standards – Safety of Nuclear Power Plants: Design. Specific Safety Requirements No. SSR-2/1, Revision 1, 2016.
<https://www-pub.iaea.org/MTCD/publications/PDF/Pub1715web-46541668.pdf>
5. IAEA Safety Standards – Safety of Nuclear Fuel Cycle Facilities. Specific Safety Requirements SSR-4, Revision 1, 2017.
http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1791\_web.pdf
6. Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable). NS-TAST-GD-005, Revision 11, November 2020.
http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-005.pdf
7. Design Basis Analysis. NS-TAST-GD-006, Revision 5, October 2020.
http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-006.pdf
8. External Hazards. NS-TAST-GD-013, Revision 7, October 2018.
<http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-013.pdf>
9. Internal Hazards. NS-TAST-GD-014, Revision 7, October 2021.
https://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-014.pdf
10. Probabilistic Safety Analysis. NS-TAST-GD-030, Revision 6, June 2019.
<http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-030.pdf>
11. Radiological Analysis for Fault Conditions. NS-TAST-GD-045, Revision 5, July 2019.
<http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-045.pdf>
12. Validation of Computer Codes and Calculation Methods. NS-TAST-GD-042, Revision 4, March 2019.
<http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-042.pdf>
13. Human Reliability Analysis. NS-TAST-GD-063, Revision 5 October 2018.
http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-063.pdf
14. Chemistry Assessment. NS-TAST-GD-089, Revision 1, February 2021.
<http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-089.pdf>
15. Safety Systems. NS-TAST-GD-003, Revision 8, March 2019.
<http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-031.pdf>
16. Civil Engineering Containments for Reactor Plant. NS-TAST-GD-020, Revision 4 December 2017.
http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-020.pdf
17. Containment – Chemical Plants. NS-TAST-GD-021, Revision 5 July 2019.
http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-021.pdf
18. Safety Related Systems & Instrumentation. NS-TAST-GD-031, Revision 6 September 2016.
http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-031.pdf
19. Limits And Conditions For Nuclear Safety (Operating Rules). NS-TAST-GD-035, Revision 6 March 2018.
<https://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-035.pdf>
20. The Purpose, Scope, and Content of Safety Cases. NS-TAST-GD-051, Revision 7, December 2019.
<http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf>
21. Human Machine Interface. NS-TAST-GD-059, Revision 5 November 2019.
http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-059.pdf
22. Categorisation of Safety Functions and Classification of Structures, Systems and Components. NS-TAST-GD-094, Revision 1, July 2019.
<http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-094.pdf>
23. Emergency Power Generation. NS-TAST-GD-103, Revision 1, February 2019.
<http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-103.pdf>
24. LC 11 and REPPIR– Operator’s Emergency Arrangements. NS-INSP-GD-011, Revision 7, August 2020.
http://www.onr.org.uk/operational/tech\_insp\_guides/ns-insp-gd-011.pdf
25. Approved Code of Practice and Guidance for the Radiation (Emergency Preparedness and Public Information) Regulations 2019.
http://www.onr.org.uk/documents/2020/reppir-2019-acop.pdf
26. Vienna Declaration on Nuclear Safety, IAEA INFCIRC/872, February 2015.
https://www.iaea.org/sites/default/files/infcirc872.pdf
27. IAEA Safety Report Series No.90 - Safety Re-assessment for Nuclear Fuel Cycle Facilities in Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, 2016.
https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1726web-49178252.pdf
28. IAEA Safety Standards – Deterministic Safety Analysis for Nuclear Power Plants. Specific Safety Guide SSG-2, Revision 1, 2019.
<https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1851_web.pdf>
29. IAEA Safety Standards – Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants. Specific Safety Guide SSG-4, 2010.
<https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1443_web.pdf>
30. IAEA Safety Standards – Safety of Nuclear Power Plants: Commissioning and Operation. Specific Safety Requirements SSR-2/2, Revision 1, 2016.
<https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1513_web.pdf>
31. IAEA Safety Standards – Design of the Reactor Containment and Associated Systems for Nuclear Power Plants. Specific Safety Guide SSG-53, 2019.
https://www-pub.iaea.org/MTCD/publications/PDF/P1856\_web.pdf
32. IAEA Safety Standards – Accident Management Programmes for Nuclear Power Plants, Specific Safety Guide SSG-54, 2019.
https://www-pub.iaea.org/MTCD/Publications/PDF/P1834\_web.pdf
33. IAEA Safety Standards - Protection against Internal Hazards in the Design of Nuclear Power Plants, Specific Safety Guide SSG-64, 2021.
https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1947\_web.pdf
34. WENRA Statement on Safety Objectives for New Nuclear Power Plants, November 2010.
35. WENRA Safety of new NPP designs (Study by Reactor Harmonization Working Group RHWG), March 2013.
36. Council Directive 2014/879 Euratom of 8 July 2014, amending Directive 2009/71/Euratom establishing a Community framework for the nuclear safety of nuclear installations laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation. Official Journal of the European Union L219/42.
<https://www.onr.org.uk/documents/2017/council-directive-2014-87-euratom.pdf>
37. Practical Elimination Applied to New NPP Designs - Key Elements and Expectations (Reactor Harmonization Working Group Report), September 2019.
38. WENRA Safety Reference Levels for Existing Reactors 2020, February 2021.
WENRA Safety Reference Levels for Existing Research Reactors, November 2020.
39. Risk informed regulatory decision making, Office for Nuclear Regulation, June 2017.
https://www.onr.org.uk/documents/2017/risk-informed-regulatory-decision-making.pdf
40. Public Health Protection in Radiation Emergencies PHE-CRCE-049, GW-430, Public Health England. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805655/Advice_for_Radiation_Emergencies_2019.pdf>
41. Japanese earthquake and tsunami: Implications for the UK nuclear industry - Final Report, HM Chief Inspector of Nuclear Installations.
<https://www.onr.org.uk/fukushima/final-report.pdf>
42. European Council “Stress Tests” for UK nuclear power plants: National Final Report.
https://www.onr.org.uk/fukushima/stress-tests-301211.pdf
43. “Stress Tests” for UK non-Power Generating Nuclear Facilities: Final Report.
https://www.onr.org.uk/fukushima/ngpf-report.pdf
44. IAEA Director General’s Report on the Fukushima Daiichi Accident.
https://www.iaea.org/publications/10962/the-fukushima-daiichi-accident

# Glossary and Abbreviations

ALARP As low as reasonably practicable

BSL Basic Safety Level

BSO Basic Safety Objective

DBA Design Basis Analysis

DEC Design Extension Conditions

EIMT Examination, Inspection, Maintenance and Testing

EOP Emergency Operating Procedure

ERL(s) Emergency Reference Level(s)

GDA Generic Design Assessment

HECA Hazard Evaluation and Consequence Assessment

IAEA International Atomic Energy Agency

LC Licence Condition

LWR Light Water Reactor

NPP Nuclear Power Plant

PSA Probabilistic Safety Analysis

REPPIR The Radiation (Emergency Preparedness and Public Information) Regulations 2019

RGP Relevant Good Practice

SAA Severe Accident Analysis

SAMG Severe Accident Management Guideline

SAP(s) Safety Assessment Principle(s)

SFAIRP So far as is reasonably practicable

SRL(s) Safety Reference Level(s)

SSC(s) Structure, System and Component(s)

TAG(s) Technical Assessment Guide(s)

WENRA Western European Nuclear Regulators’ Association

1. Licensee has been used throughout this TAG as a single term that includes other duty-holders, Requesting Parties participating in a Generic Design Assessment (GDA), and any other organisation or individual involved in the development or application of the safety case. Designer has been used in some cases to give an indication of where in the life cycle of a facility safety case activity should be undertaken. The designer may or may not be the Licensee or Requesting Party and use of the term here is not intended to relate to any legal duties of a ‘designer’ under relevant legislation. [↑](#footnote-ref-1)
2. An ‘early radioactive release’ in this context is a radioactive release for which off-site

protective actions would be necessary but would be unlikely to be fully effective in due time.

A ‘large radioactive release’ is a radioactive release for which off-site protective actions, that

are limited in terms of lengths of time and areas of application, would be insufficient for the

protection of people and of the environment. [↑](#footnote-ref-2)
3. The possibility of certain conditions arising may be considered to have been ‘practically eliminated’ if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.” [↑](#footnote-ref-3)