Office for Nuclear Regulation

ONR GUIDE			
Severe Accident Analysis			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-007 Revision 4		
Date Issued:	September 2017	**Review Date:**	September 2020
Approved by:	Robert Moscrop	Professional Lead, Fault Analysis	
Record Reference:	TRIM Folder 1.1.3.776. (2018/394424)		
Revision commentary:	Minor update to reference the Ionising Radiation Regulations 2017. Updated November 2018.		

TABLE OF CONTENTS

Published 09/17

1. INTRODUCTION

1.1 Office for Nuclear Regulation (ONR) has established a set of Safety Assessment Principles (SAPs) [1], which apply to the assessment by ONR 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 inspectors in their technical assessment work and hence in making regulatory judgements and decisions. This Technical Assessment Guide (TAG) is one of these guides.

1.2 TAGs are intended to provide guidance to inspectors for carrying out their regulatory duties. They also help to demonstrate how ONR meets the Western European Nuclear Regulators Association (WENRA) Reference Levels (RLs) and how ONR guidance is linked to that contained in International Atomic Energy Authority (IAEA) safety standards. TAGs are not written for duty holders, and although they may be used as a source of guidance or good practice, duty holders should not take them as a prescriptive set of legal requirements.

1.3 This severe accident TAG is intended to be used in conjunction with TAGs on "Deterministic Safety Analysis and the Use of Engineering Principles in Safety Assessment" [2]; "Transient Analysis for Design Basis Accidents in Nuclear Reactors" [3] and "Probabilistic Safety Analysis" [4].

2. PURPOSE AND SCOPE

2.1 The SAPs [1] provide a framework to guide regulatory decision making in the nuclear permissioning process. SAPs are supported by TAGs, which further aid ONR's decision making process with guidance intended to advise and inform inspectors in the exercise of their professional regulatory judgment. This TAG has been produced to aid inspectors when assessing those aspects of a safety case in respect of Severe Accident Analysis (SAA).

2.2 The 2014 SAPs (paragraph 664) define 'severe accidents' to be:

> *"'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.*"

The highest off-site radiological BSL dose in Target 4 is 100 mSv off-site (via conservative calculations); while a substantial quantity of radioactive material is defined to be "*one which if released could result in the consequences specified in the societal risk Target 9").* An event that could reasonably exceed any of these numerical targets is potentially a severe accident and should be considered in the safety case.

2.3 The types of events that should be considered as part of a SAA are set out in the following sections. Broadly speaking, SAA is less concerned with the details of the sequences that could lead to the severe accident, but instead focuses on potential adverse states that the facility could be in, and then analyses the options open to the licensee to bring the position back under control. The severe adverse situations and states considered within SAA include those beyond the design basis of the facility, or initiated by a security incident, or those for which design basis provisions have not been successful in bringing a fault back under control.

2.4 SAA is an established worldwide concept for nuclear power plants but less so for other nuclear facilities. The principles developed for nuclear power plants can however be readily transferred to other types of nuclear facilities where there is a comparable level

of hazard. For a nuclear power plant, a severe accident is generally taken to be one where core melt or significant degradation of the fuel occurs. However, in light of the Fukushima accident in 2011, the international consensus has been to extend the scope to include significant damage to fuel stored in spent fuel ponds etc. For other nuclear facilities such as fuel cycle plants, there is greater variety in the type of event that could lead to a severe accident since the processes and technologies involved are much more wide-ranging. However, due to the nature of the processes involved, there is a lower degree of uncertainty associated with physical and chemical properties of the material that could be released.

2.5 The SAPs therefore seek that SAA is considered as part of a complementary approach to fault analysis for cases where there is a very large hazard. DBA and PSA should already have been applied to ensure the analysed risks are acceptably low. SAA should then be applied to cater for possibilities such as the analysis being incorrect or incomplete; the initiating event being out of scope; or the measures put in place being circumvented or failing in some way. SAA is therefore based primarily on hazard rather than risk, and is focussed on states and situations that might theoretically arise (termed scenarios from now on), rather than fault sequences leading to a particular state. It thus requires different ways of thinking compared to DBA and PSA.

2.6 The essential underlying principle is that, although extreme scenarios have a very low frequency of occurrence, the duty holder is required to consider, in advance, the necessary actions in the event of a major accident occurring, and to make adequate provisions which may include engineering measures, where reasonably practicable, emergency plans and procedures. It is expected that the safety functions to be delivered by these systems should be analysed and justified in the safety case and be consistent with the site's emergency preparedness and accident response arrangements (see Principle AM.1).

2.7 In general, the aims of SAA are to ensure that high hazard nuclear facilities are designed and operated so that, should a severe accident occur, the facility can be returned to an appropriately safe and stable condition with the radiological consequences mitigated subject to As Low As Reasonably Practicable (ALARP). This involves determining the potential progression of the accident, the magnitude and characteristics of the consequences and any cliff edges. This information should then be applied, as per Para 672 of the SAPs, 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 Principle AM.1);
- support the preparation of emergency plans for the protection of people (see Principle AM.1); and
- support the PSA of the facility's design and operation.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 SAFETY ASSESSMENT PRINCIPLES

3.1 The SAPs [1] that provide the regulatory basis for the application of this guide by inspectors are principally FA.15 and FA.16 as:

FA.15 - Scope of severe accident analysis, states that:

> *"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, states that:

> *"Severe accident analysis should be used in the consideration of further risk-reducing measures."*

3.2 Principles FA.15 and FA.16, and their supporting paragraphs (663 – 673), provide specific guidance on SAA in safety cases. Paragraph 663 notes that rigorous application of DBA and PSA should ensure that the predicted risks from fault sequences leading to significant radiological consequences are very low. Nevertheless suitable and sufficient SAA is required to ensure that risks are reduced So Far As Is Reasonably Practicable (SFAIRP) – commonly termed "ALARP".

3.3 In addition, there are other Principles and supporting guidance from the SAPs that are particularly relevant to SAA. These are described in the following paragraphs.

3.4 Paragraph 101 f) indicates that, where appropriate, SAA should form part of the facility's safety case in order to demonstrate that the control of hazards and the risk beyond the design basis is ALARP. Paragraphs 605 to 611 explain the complementary inter-relationship of the three forms of fault analysis described in the SAPs (DBA, PSA and SAA), and the need for these to be mutually consistent is indicated in paragraph 620.

3.5 Paragraph 610 highlights the importance of a defence in depth approach to safety. The approach is described in detail under Principle EKP.3, which states:

> *"Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression."*

3.6 In particular, Para 151 d) states that defence in depth should be applied so that there are additional measures to mitigate the consequences of severe accidents. IAEA Safety Standard Series SSR-2/1 [5] defines defence in depth in terms of five "Levels" of protection. Beyond the design basis, Level 4 is of key relevance to SAA. Although Level 5 (emergency control and emergency response on and off site) will be important too, as the results from SAA should inform emergency response activities and planning, (see Principle AM.1).

3.7 Level 4 of the SAPs defence in depth hierarchy seeks the provision of additional measures and procedures to prevent or mitigate fault progression, and for accident management. Modern commercial facilities, especially power plants, incorporate design features to enhance their resilience to accidents leading to significant inventory redistribution (e.g. fuel degradation and relocation). These design features represent defence in depth in the sense that they provide protection against fault sequences that are Beyond Design Basis (BDB). SAA therefore informs what is reasonable in this regard; often through comparison with relevant good practice adopted at similar facilities in other nations or facilities of a different design that demonstrate a similar level of hazard potential.

3.8 Equipment qualification is an important aspect of SAA. SAPs relevant to this include EQU.1, which states:

> *"Qualification procedures should be applied to confirm that structures, systems and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives."*

3.9 In particular Paragraph 175 states that equipment qualification procedures should, where appropriate, address severe accident conditions. The key point here is that where equipment needs to perform safety functions in severe accident conditions, it should be qualified to do so. This requires consideration of post-accident conditions (e.g. high pressures, temperatures, humidity and radiation fields; and in nuclear chemical plants, the highly corrosive environments likely to be present in a severe accident).

3.10 The provision of suitable and sufficient control and instrumentation for severe accident conditions is similarly vital to the viability of the severe accident response. This is reflected in SAP ESR.1, which states:

> *"Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate secondary control or monitoring locations."*

3.11 Paragraph 430 states the equipment provision should encompass severe accidents. Paras 453 to 456 highlight the need for human interface aspects to be considered in this provision. In a severe accident context, "compatibility with human psychological and physical characteristics" means that the adverse working environments likely following a severe event should be considered explicitly by a human factors specialist.

3.12 Also of relevance is SAP ECV.3, which states:

> *"The primary means of confining radioactive materials should be through the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components."*

3.13 Particularly paragraph 525 c) states that the containment design should include performance requirements in the event of a severe accident, including its structural integrity and stability, in order to minimise any uncontrolled release of radioactivity into the environment. The final containment, where in place, is expected to maintain its integrity if a severe accident has resulted in a large release of energy and radioactive material, leading to an increase in containment pressure. The Fukushima accident highlighted the importance of the containment overpressure protection system in a severe accident and highlighted that, where reasonably practicable, defence in depth should be used to account for potential unforeseen events.

3.14 Mitigation measures to ensure a robust and independent means of protecting the containment against overpressure should be considered as part of the design where appropriate. In addition, the capability to mitigate containment over pressure without off-site support and without challenge to the period required for restoration of containment should also be considered. The SAA should provide a deterministic prediction of the maximum containment pressure for such conditions.

3.15 On the basis that the containment is designed to limit the spread of activity, the containment should be able to control the pressure by passive means SFAIRP such that the containment structure rides out the pressure transient, potentially without any active systems, noting that such a facility should not be detrimental to the overall safety of the plant.

3.16 Finally, SAPs fundamental principle FP.7 seeks arrangements for emergency preparedness and response in the case of nuclear and radiological incidents, specifically stating:

> *"Arrangements must be made for emergency preparedness and response in case of nuclear or radiation incidents."*

3.17 Further details are provided in paragraphs 768 ff. (Accident Management and Emergency Preparedness). As already noted, where the hazard potential is high, these arrangements should be informed by suitable and sufficient SAA.

3.2 SITE LICENCE CONDITIONS

3.18 The Licence Conditions (LCs) [6] providing the regulatory basis for the application of this guide by inspectors are principally:

- LC23 - Operating Rules;
- LC14 - Safety Documentation; and
- LC11 - Emergency Arrangements.

3.19 LC23 requires licensees to:

> *"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".*
>
> *LC23(1) calls such conditions and limits "operating rules".*

It is important to note that the licensee's duties under LC23 apply to any operation that may affect safety and so the Operating Rules (OR) coverage, like that of the safety case, needs to be complete, i.e. address all important aspects of the facility's operation, from normal operations through to dealing with emergencies. This means that the licensee's safety case should adopt a defence in depth approach to safety, leading to the provision of several layers of protection against potentially significant faults or failures. Such an approach should lead to development of limits and conditions for response to accidents (Level 4) and emergencies (Level 5). These latter two Levels should be informed by the licensee's severe accident analysis. Detailed guidance on this is provided in TAG T/AST/035 [7].

3.20 Related to this, under LC14, licensees are required to:

> *"make and implement adequate arrangements for the production and assessment of safety cases*"

As already noted, where the hazard potential is great enough, the safety case should include SAA. The licensee's LC14 arrangements should therefore make provision for identifying where SAA is needed and the methods of analysis to be used.

3.21 In addition, the SAA should inform emergency planning (defence in depth Level 5). Here, LC11 requires licensees to:

> *"make and implement adequate arrangements for dealing with any accident or emergency arising on the site and their effects*."

LC11 also requires the licensee to consult with all other relevant persons or organisations where their assistance or co-operation is needed. In practice, this includes the relevant Local Authorities (LAs), the emergency services and operators of adjacent hazardous installations. LC11 puts a requirement on the licensee to rehearse its emergency arrangements, preparedness and response at appropriate intervals and to ensure that all employees of the licensee who have emergency arrangement duties

are properly trained. The SAA in the safety case should be used to inform all these aspects.

3.3 THE RADIATION (EMERGENCY PREPAREDNESS AND PUBLIC INFORMATION) REGULATIONS

3.22 The Radiation (Emergency Preparedness and Public Information) Regulations 2001 (REPPIR) [8], implement in Great Britain the articles on intervention in cases of radiation (radiological) emergency as defined in Section 1 of the Council Directive 96/29/Euratom (BSS96 Directive) [9]. A "radiation emergency", as defined in REPPIR, is an event that is likely to result in a member of the public receiving an effective dose in excess of 5 mSv during the year immediately following the event. REPPIR presents the legal framework for protection of the public through emergency preparedness for radiation accidents.

3.23 Under REPPIR, relevant duty holders[1] are required to undertake and submit to the ONR a Report of Assessment (RoA) that contains the particulars specified in REPPIR Schedule 5, with sufficient detail and references to enable ONR to confirm the conclusions reached. The RoA is based on the duty holder's assessment of radiation accident hazards and risks (the Hazard Identification and Risk Evaluation (HIRE)). The ONR also undertakes a technical assessment of the HIRE and this assessment is used by ONR in the determination of the extent of the REPPIR off-site emergency planning area (required by Regulation 9(1)).

3.24 The HIRE report should characterise the likelihood, nature and magnitude of the radiation-related threats that may occur through consideration of the full spectrum of events. Specifically, the minimum area is usually informed by the area around the site in which a member of the public could receive an effective dose in excess of 5 mSv in the year following a reasonably foreseeable radiation accident. SAA in the safety case should be used to inform the HIRE report. Further information on ONR's guidance for assessing HIRE reports is provided in TAG T/AST/082 [10].

3.25 REPPIR also provides a framework for controlling the exposure of 'intervention personnel' during a radiation emergency. These are usually employees of the operator or emergency services, required to intervene in an emergency e.g. to bring help to the people at risk or to prevent a large number of people being exposed. These employees may, as a result, be exposed to ionising radiation that exceeds the dose limits in Schedule 3 of the Ionising Radiations Regulations 2017 (IRR17) [11]. REPPIR calls these 'emergency exposures', and they are only permitted for authorised employees who have received appropriate information, training and proper equipment. The Licensee's SAA should be used to inform the analysis of such exposures so that the emergency response can be suitably planned and hence suitable equipment provided in line with the guidelines and regulations such as; [24], [25] and [26].

[1] The ONR is the enforcing authority for the provisions of REPPIR in so far as they apply to GB nuclear sites, [Subsection 18(1A) of the Health and Safety at Work etc. Act 1974, added to by section 116 and Schedule 12 of the Energy Act 2013] and authorised defence sites, new nuclear build sites & nuclear warship sites [Regulation 4A of the Health and Safety (Enforcing Authority) Regulations 1998, added by article 6(2) and Schedule 3 of the Energy Act 2013 (Office for Nuclear Regulation) (Consequential Amendments, Transitional Provisions and Savings) Order 2014)].

3.4 HEALTH AND SAFETY AT WORK (ETC) ACT 1974

3.26 Amongst other things, this act places a duty on licensees to reduce their risks SFAIRP – commonly termed "As Low as Reasonably Practicable (ALARP)". Guidance on ONR expectations for ALARP is set out in TAG T/AST/005 [12]. The licensee's SAA should provide an input for consideration of how to meet its duty to reduce risks SFAIRP.

3.27 The ALARP TAG [12] focuses on achieving good designs, prevention of faults and protection against their consequences, i.e. in a nuclear context, Levels 1 to 3 of defence in depth. In these circumstances, cost benefit analyses can sometimes be helpful in determining whether it would be grossly disproportionate to make a particular safety improvement. For Levels 4 and 5 however, use of cost-benefit analysis will rarely suggest making safety improvements, as the licensee's provisions in Levels 1 to 3 will already have reduced the numerical risks to very low levels. This does not mean that there are no reasonably practicable provisions that can be adopted at the plant, for the reasons set out in the following paragraphs:

- Cost benefit analysis is not a particularly useful tool for the circumstances in which SAA is required. Section 5.2 below sets out the 3 classes of scenario that should typically be addressed within the scope of a licensee's SAA. Only the first two of these are amenable to a probabilistic approach and even then, the analysis will likely be subject to considerable uncertainties. In the second class, where a design basis provision has failed, something unforeseen in the original safety analysis must have occurred. Similarly, in the third class, a cost benefit analysis would struggle to apply meaningful values to the likelihood of malevolent acts. For these reasons, cost benefit analysis will usually become a blunt tool for assisting with ALARP decisions associated with severe accidents.
- As explained in the HSE publication "Reducing Risks, Protecting People" (R2P2) [13] and TAG 005 [12] the term "risk" when applied to ALARP also means "the possibility of danger", or "hazard" in technical parlance. The duty to reduce risks SFAIRP is therefore a wider matter than simply minimising the product of frequency and consequence. There does however, need to be a threshold at which the possibility of danger is sufficient to make it reasonable for duty holders to take steps. At nuclear facilities, posing a hazard of the magnitude described above, this "possibility of danger" needs to drive SAA to assist with the licensee's consideration of what is reasonably practicable.
- In addition, as explained in TAG T/AST/005 [12], the starting point for any ALARP analysis should be appropriate relevant good practice. In many cases, meeting the standard of relevant good practice will be synonymous with achieving ALARP and this should normally be the basis of the licensee's safety case rather than a cost benefit analysis. In the context of SAA there is a considerable quantity of relevant good practice that the licensee, and the inspector, may consult. Notable among these, in addition to the SAPs, are IAEA Safety Standards and WENRA Reference Levels. The relevance of these is outlined in the following section.

4. RELATIONSHIP TO WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS

4.1 WENRA SAFETY REFERENCE LEVELS

4.1 The objective of the Western European Nuclear Regulators Association (WENRA) harmonisation programme is to develop a common approach to nuclear safety in Europe by comparing national approaches to the application of IAEA safety standards. WENRA Safety Reference Levels (SRLs) [14], which are based on the IAEA safety standards, represent good practice in the WENRA member states and provide a

consensus regarding the main requirements for ensuring nuclear safety. The UK is committed to aligning its regulatory guidance with the WENRA safety reference levels while in keeping with ONR's guidance on the demonstration of ALARP [12]. Inspectors should consider the WENRA SRLs to be Relevant Good Practice for civil nuclear reactors. Though the SRLs strictly only apply to operating, commercial Nuclear Power Plants (NPPs), the underlying principles may be applicable to other nuclear facilities with similar levels of hazard (e.g. Nuclear Fuel Cycle Facilities), and so where possible should be applied accordingly.

4.2 The WENRA SRLs [14] directly relevant to this TAG are primarily included within Issue F (Design Extension of Existing Reactors) and are represented in **Appendix 1** although some of these are more relevant to DBA analysis when considered within the UK context. Section 5 of ND-TAST-GD-005 identifies the WENRA Reference levels as Relevant Good Practice for existing civil nuclear reactors, and the reader is strongly advised to also consult the relevant SRLs and TAG for additional advice and information relating to ALARP. This Section of Appendix 1 also offer a cross referencing with ONR SAPs to direct the reader to the relevant SAPs paragraphs.

4.3 The SRLs relating to Issue LM (Emergency Operating Procedures and Severe Accident Management Guidelines) and Issue R (On-site Emergency Preparedness) are set out in full in **Appendix 1**. It should be noted that some are focussed on Emergency Arrangements that are covered elsewhere by ONR guidance on DBA analysis and LC11 arrangements rather than SAA; these are listed individually and are provided for convenience to help the reader.

4.2 IAEA SAFETY STANDARDS

4.4 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. The main IAEA Safety Standard of relevance here is the Safety Requirements SSR-2/1 [5], in which chapter 5 sets requirements for plant design including a section on severe accidents (describing severe accidents within Level 4 of the defence in depth concept). A number of design considerations with severe accidents in mind are then detailed.

4.5 Other IAEA guidance of particular relevance to assessment of severe accidents include:

- IAEA NS-G-2.15: Severe accident management programmes for nuclear power plants [15] – this provides recommendations on meeting the requirements for accident management, including managing severe accidents as described in Section 5 of [1], Sections 3 and 5 of [16] and Section 4 of [17].
- IAEA SSG-4: Development and application of Level 2 probabilistic safety assessment for nuclear power plants [18] – this details design aspects important to severe accidents and acquisition of information is discussed. Guidance is also provided on how accident progression should be analysed from source term to release of radioactivity and on determining consequences following plant damage states.
- IAEA GSR Part 4 [17], NS-G-1.10 [19] and NS-G-2.2 [20] are also of relevance. In particular Chapter 4 of NS-G-1.10 - Safety assessment, includes BDB and severe accident considerations; covering selection, methods, assumptions, acceptance criteria, design considerations and emergency planning.
- IAEA NS-G-1.10 [19] Chapter 6, provides guidance on design considerations for severe accidents covering structural behaviours of the containment, energy management and management of radionuclides and combustible gases. Provision of instrumentation required for monitoring the conditions inside the

containment by operators to execute emergency procedures and assess the consequences is also discussed in detail.

- IAEA NS-G-2.2 [20] Section 8, provides guidance on development of Emergency Operating Procedures (EOP)[2], and how they relate to BDB accidents. It states that the EOPs, or accident management guidance, necessary to cope with BDB accidents should be identified by systematic analysis of those BDB accidents and the plant's vulnerabilities to such accidents. Furthermore, strategies should be developed to deal with these vulnerabilities. The report concludes that for BDB accidents, owing to the wide variety of conditions that may exist, symptom based EOPs[3] and accident management guidance are preferable to an events based approach; that is, they will use parameters indicating the plant state to identify optimum recovery routes for the operator, without the need for accident diagnosis.

4.6 Although the emphasis of these documents is on nuclear power plants, the principles discussed are often more widely applicable. Inspectors are thus encouraged to use these documents as sources of relevant 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 NPP approach may not necessarily translate directly.

5. ADVICE TO INSPECTORS

5.1 BASIS AND CHARACTERISTICS OF SEVERE ACCIDENT ANALYSIS

5.1 The general principles of SAA described in this Section have been written to apply to the full spectrum of UK nuclear facilities. Technical aspects addressing SAA with specific relevance to Pressurised Water Reactors (PWR) are set out in the advisory note [27]. In addition, a recently commissioned work "Requirements[4] on Severe Accident Analyses for ABWR Plant Design" [28] covers the SAA aspects relevant to the Advanced Boiling Water Reactors (ABWR). Both these notes are relatively detailed, reflecting the significant extent of the effort that has gone into analysing and researching this topic worldwide, particularly for Light Water Reactors (LWR). Inspectors may adapt the general principles and philosophy set out in these complimentary notes for non reactor systems as appropriate, noting that there is much variability in the types of severe accident that could occur in nuclear chemical plants (compared with reactors) since the process and technologies are varied. Inspectors are also advised to review the WENRA SRL, some of which are represented in **Appendix 1**, for additional guidance and information.

5.2 As already noted, SAA should be included in safety cases for facilities where the potential exists for the following fault sequences:

a) Unmitigated consequences exceeding 100 mSv off-site (conservative assessment), or

---

[2] **Event-based EOPs:** enable the operator to identify the specific event and encompass information for determining the status of the plant, and

- Mandatory operating instructions that need to be taken as a result of the event,
- Subsequent operator actions directed to returning the reactor to a normal condition or to provide for safe, extended and stable shutdown conditions.

[3] **Symptom based procedures**: A procedure or guidance for actions to be taken depending on the value of directly measurable plant parameters.

[4] Note: this report uses the word "requirement" in its title to highlight the future contract requirements for the review of ABWR design and it is not intended to place any requirements on duty/Licence holders.

b) A substantial[5] unintended relocation of radioactive material within the facility to place a demand on the integrity of the remaining physical barriers.

5.3 Case a) is derived from SAPs Numerical Target 4 and so should be considered on a conservative basis. The degree of conservatism applied by the licensee will be dependent on the type of analysis it has performed. There is typically some conservatism in safety case analysis for off-site doses (e.g. up to a factor of 10 for weather assumptions alone).

5.4 Experience suggests that it is often disproportionate to seek SAA in situations where the only limit of concern from a postulated unmitigated fault is 500 mSv on-site. Target 9 includes on-site and off-site fatalities. In cases where the doses in para 5.2 (a) and/or (b) are exceeded, SAA should be applied, but in a proportionate manner.

5.5 For consistency with WENRA SRLs, scenarios with an imminent or an actual core melt (or equivalent significant damage to fuel in storage facilities) should be treated as being beyond 100 mSv and then subjected to SAA, irrespective of the results of detailed consequence calculations.

5.6 As with all the Numerical Targets defined in SAPs, the numbers quoted above should be used approximately rather than as exact cut-offs. So for example, a fault sequence which conservatively could give off-site consequences of nearly 100 mSv should be taken to be a candidate for further SAA. Para 704 of the SAPs provide additional caution against potential simplifications or manipulations of the targets.

5.2 CLASSES OF SEVERE ACCIDENT ANALYSIS

5.7 It is desirable that a complementary approach to conventional fault analysis is applied for cases where there is a very large hazard to ensure the analysed risks are acceptably low. SAA provides such an approach and is based primarily on consideration of the size of the hazard rather than the risk, focussing on the states and situations that might theoretically arise, rather than fault sequences leading to a particular state. The duty holder is required to consider, in advance, the necessary actions in the event of a major accident occurring, and to make adequate provisions which may include engineering measures, where reasonably practicable, emergency plans and procedures.

5.8 The actual circumstances of any given severe accident will differ significantly from the scenarios considered in the SAA. However, the thinking required for the SAA, and the provisions so derived, will likely encompass the actual circumstances and prove invaluable following an accident. Time spent by the Licensee analysing severe accidents and its consequences in advance should reduce the risk in a severe accident.

5.9 There are two classes of scenario that should typically be addressed within the scope of a licensee's SAA:

i. High consequence events of low frequency beyond the design basis; and

ii. Design basis events where the safety provisions are assumed to fail.

5.10 In addition, the licensee may choose to address within the scope of its SAA:

iii. Scenarios traditionally not covered by the safety case such as malevolent acts,

5.11 Fault sequences for analysis should be selected to provide a comprehensive and representative sample of types of events beyond the design basis that could make a significant contribution to the risk posed by the facility. In cases where the plant risk

[5] In this context, "substantial" means an amount akin to the consequences specified in the SAPs' societal risk target.

target for major off-site release is 10^{-6} per year sequences with an assessed frequency of around 10^{-7} per year would normally be included. This expectation is highlighted in para 631 of the SAPs "whatever frequency is adopted it should be justified and should ensure that accidents with such frequencies are covered in the DBA or the SAA". However, the sequence frequency should not be the exclusive determining factor. It is equally important that analysis includes adequate coverage of accident phenomena, plant performance and engineering considerations (e.g. see SAP EKP.3).

5.12 Special attention should be paid within the first class to events initiated by gross failures of plant and equipment that rely on claims of high structural integrity in the safety case, particularly those relating to maintaining pressure / containment boundaries (e.g. where the licensee has made such a claim or where the fault has been "practically eliminated"[6]). Here the analysis will need to go beyond 10^{-7} per year so that cliff edge effects from these failures can be suitably addressed.

5.13 The second and third classes (ii. and iii. above) are less amenable to probabilistic treatment. Instead, the licensee's approach should be to analyse "what could be done if …?" scenarios. For events in the second class, the approach should be to ensure as much independence as is reasonably practicable between the levels of defence in depth (SAPs Para 768 and EKP.3). This is on the basis that if some aspects of the design basis protection have failed, a common cause may well have rendered other provisions at this level also unavailable. The SAA should thus assume that the plant and equipment claimed for the Design Basis is no longer available, and then determine what extra plant and equipment is needed to recover the situation whilst minimising the accident consequences.

5.14 Irrespective of class, the approach taken for the SAA should be broadly the same, aiming to determine what plant, equipment, supplies / consumables, strategies, procedures, staffing levels, activities etc. are needed to provide Level 4 mitigation in scenarios where Levels 1-3 have failed to prevent / protect against a developing accident scenario. The outputs from the SAA may also inform the Level 5 off-site response. *The levels of protection are defined in paragraph 152, Table 1 of the SAPs.*

5.15 The SAA should be carried out in a systematic manner looking in turn at how each fundamental safety function will be delivered during the accident. For reactors, SAPs Para 540 defines the fundamental safety functions to be control of reactivity, removal of heat from the core and confinement or containment of radioactive substances. For other facilities, this list should be adapted as appropriate e.g. to include control of criticality for nuclear chemical plants and spent fuel stores, or to include maintenance of cooling systems removing heat from the heat-generating waste stores and fuel ponds etc.

5.16 The SAA should utilise deterministic, best-estimate analyses to predict options for how the accident might progress. These predictions should be used to determine priorities and timeframes for action and any cliff edge deteriorations that could occur. The analyses should be presented in such a way to usefully inform the licensee's proposed accident response strategies and guidance, and to enable the licensee to brief other stakeholders on aspects relevant to the off-site emergency response.

5.3 BEST-ESTIMATE BASIS

5.17 In line with SAPs Para 669 and WENRA SRL F3.1, SAA should be performed on a best-estimate basis. This applies to calculated conditions and radiological consequences. Providing realistic calculations is crucial, so that those managing the emergency response can make appropriately informed decisions regarding immediate

[6] In this context, the possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise (from IAEA NS-G-1.10), [20].

priorities for action. It also allows realistic appraisal of the actual conditions within the facility based on measured conditions. Applying the conservatism normally associated with DBA can easily bias the response inappropriately, so it is unlikely that deterministic analysis used for the DBA can be recycled for direct use in the SAA.

5.18 A further reason for being wary of conservatism is that severe accident phenomena are often diverse, complex and counter-intuitive. This leads to situations in which a 'conservative' assumption in one area produces a non-conservative outcome in another. Indeed, what is 'conservative' in DBA may become 'non-conservative' in accident conditions. As a result, each set of analysis should be approached with the intention of evaluating the progression of events in as realistic a manner as possible, since a key objective should be to inform accident management strategies and emergency planning. Level 2 PSA is recognised as providing a structured framework to trying to ensure this.

5.19 However, Inspectors should note that severe accident phenomena presents a number of challenges such as fuel degradation and melt relocation, steam explosions, hydrogen explosions, hydrogen distributions in containment, and potential leakage through containment penetrations that are difficult to model. Furthermore, the interplay of the phenomena in severe accidents is more complex than in design basis scenarios. As such, the challenge of severe accident codes to correctly and accurately predict the severe accident progression and dispersion phenomena is considerable and limited experimental evidence is available to validate the codes.

5.20 A further consideration is the competency of the code user. While user effects in DBA modelling are known to be a source of uncertainty, the greater complexity of SAA modelling is likely to mean that user effects are correspondingly of greater significance. While initiatives such as International Standard Problems (ISP) provide additional insight into the impact of the user effects in DBA analyses, the scarcity of experimental data noted above means that insights to support the safety case and potential judgements by Inspectors could be less in SAA than DBA.

5.21 Given the above issues and the need for best-estimate analysis implies that additional care and attention needs to be given to the treatment of uncertainties as discussed in the next Section.

5.4 UNCERTAINTIES

5.22 The general intention of SAA is to determine the *likely outcome* of fault sequences not included within the design basis. As noted above the use of best-estimate analysis is appropriate for such sequences. However, in principle, a truly best estimate analysis only confirms a successful outcome at a 50% probability level. This is not likely to be sufficient for most applications and so where there is major uncertainty in the physical phenomena, consideration of what is the level of this uncertainty is appropriate.

5.23 This is particularly true when the uncertainty has a large effect with regard to determining the sizing of equipment, or the relevant environmental conditions in which the equipment will need to operate. In such situations it is expected that sensitivity studies will be performed to quantify and understand such affects. The scope of such studies is expected to be informed by the results of the L2 PSA to ensure that a balanced and proportionate consideration is made of the possible uncertainties. This should provide confidence that the associated equipment is likely to perform its function appropriately and demonstrate that safe, and stable conditions can be achieved post-accident conditions.

5.24 The impacts of major uncertainties in accident phenomena and in plant / equipment performance should be examined systematically. Likewise, the effects of alternate credible assumptions and process models on calculated results should be assessed.

Sensitivity analyses may also be employed to check that there are no sudden escalations in consequences just beyond the analysed conditions ("cliff edge effects").

5.25 A key uncertainty in the SAA will often be the manner in which the accident progresses. There will often be several accident paths (e.g. at Fukushima, different scenarios developed on the different units), which can be strongly affected by the type and timing of operator interventions. The uncertainty analysis should attempt to explore the main varieties of scenario that could develop as the accident progresses and the factors that determine which accident path will be followed.

Use of Research and Uncertainties

5.26 In view of the variety of potential applications of SAA, no general rules for the analysis of uncertainties have been included in this TAG. Instead, the general message is to seek an approach where duty holders are clear about any uncertainties and any conservatism applied in their SAA and are in a position to quantify their effects.

5.27 Where this is not possible, or where the uncertainties are large, in line with SAPs Para 671, the licensee should be encouraged to carry out research aimed at reducing the prevailing uncertainties and unknowns in order to refine its analysis. Examples of severe accident test facilities include those at the CEA's Cadarache site which have been used to provide the validation evidence on the behaviour of reactor activity releases and deposition in the primary circuit of PWRs in relation to how this contributes to lowering off-site releases. Other tests are on steam explosions and hydrogen distribution in containment. The PHEBUS FP (Fission Products) international research programme was conducted to improve understanding of the phenomena occurring during a core meltdown accident in a light water reactor and to validate the computational model used to represent these phenomena in reactor safety evaluations.

5.28 The need for further research will be a common outcome from SAA, given that the situations being analysed are often at, or beyond current limits of scientific knowledge. Here, 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, are being proactive in learning from major accidents and are commissioning work in areas of key uncertainty in their SAA.

5.5 RELATIONSHIP TO OTHER FAULT / ACCIDENT ANALYSES

5.29 As highlighted in SAP FA.25, SAA should be used to complement the DBA and PSA in situations where there is a large hazard, even if the calculated risks are low and/or the DBA provides a robust demonstration of fault tolerance. The SAA should not be a standalone piece of analysis deriving scenarios from first principles, but instead should build upon other types of analysis to create an overall safety case that is adequate in its coverage. The following paragraphs outline the relationship between SAA and other methods of fault / accident analysis.

Relationship to DBA

5.30 In classes i) and ii) above (paragraph 5.9), DBA should provide a guide for what needs to be included within the SAA. The DBA should indicate the bounding magnitude of the potential consequences and so determine what scenarios need consideration. Moreover, it should provide a systematic means of identifying:

- Scenarios excluded from the DBA by virtue of their low initiating event frequencies;

- DBA assumptions, which if incorrect could lead to a severe accident (e.g. where by 'claims of extremely high structural integrity; and
- The measures identified within the DBA that would need to fail for there to be a severe accident.

5.31 In class iii), the DBA can be used to identify what large hazards are present at the facility, and so provide the starting point for this aspect of SAA.

5.32 As SAA is focused on Levels 4 and 5 of the Defence in Depth hierarchy (EKP.3), the approach should normally assume that the safety measures identified for Level 3 protection are unavailable. The SAA should then determine the additional safety measures required to regain control of the accident. There will however be exceptions to this rule; for example, in cases where so many safety measures are claimed in the DBA that an argument could be made that adequate Level 4 protection / mitigation is provided by Level 3 plant and equipment. Arguments of this type need to be considered on their individual merits, taking account of aspects such as the degree of redundancy / diversity and the extent of vulnerabilities to common cause failures.

5.33 A key difference between DBA and SAA is that DBA should take a conservative approach, whereas SAA should be best-estimate. Inspectors should therefore be wary of cases where the licensee's SAA relies heavily on its DBA, checking the level of understanding of the conservatisms used regarding data, underlying assumptions and the simplifications in their analysis.

5.34 The SAA can also potentially feed into the DBA. For example, the analysis might identify previously unknown cliff edges lying just beyond the design basis. SAPs Para 628 a) suggests DBA should be applied to internal events that have an initiating event frequency exceeding *about* 10^{-5} per year, noting that in general the SAPs Numerical Targets should not be applied rigidly (e.g. as fixed thresholds). As such, consideration should be given by the licensee in such cases to modifying the design where it is reasonably practicable so to do; either to remove the cliff edge, or to extend the provisions of the design basis protection.

Relationship to PSA

5.35 There are strong links between PSA and SAA. SAA can inform PSA and vice versa, but the results of PSA should not be used as the sole reason not to perform SAA on a particular sequence.

5.36 The PSA should identify those areas or aspects of the design and operation that merit further attention and potential initiating events that could lead to a severe accident. For example, it should identify where the failure of a design basis measure could lead to a consequence that meets severe accident criteria. Additionally it ought to show readily which unprotected initiating events (non-design basis events) could lead to consequences that meet the severe accident definition. Overall, PSA will usually be a better tool for identifying scenarios for SAA than DBA, as it aims to group classes of events on a more best-estimate basis consistent with the approach expected for SAA and it is not subject to sequence frequency cut-offs.

5.37 As per SAPs Para 672, the results of SAA should be used as an input to the PSA. This should enable inspectors to determine the extent to which the SAPs Numerical Targets are met (in particular, the low frequency contributions / dose bands of Targets 5 to 8 and the societal risk Target 9) and whether additional protection or mitigation may be merited. For reactors, WENRA SRLs governing the aims and use of PSA in a severe accident context are relevant and applicable to all types of nuclear facilities.

5.38 It should be noted that, not all the scenarios that should be addressed in the SAA are particularly amenable to a numerical treatment. In particular, inspectors should be wary of safety case arguments that dismiss accident scenarios from the SAA solely on predicted sequence or event frequency grounds. Indeed, this was one of the

conclusions from the ENSREG Power Reactors Stress Tests Peer Review following the Fukushima accident.

5.39 SAA is a key input to the Level 2 PSA, which in turn provides a list of release categories / source terms and associated frequencies for input into a Level 3 PSA. The Level 3 PSA can be used to estimate the societal risk of 100 or more fatalities (late or early) for comparison with SAPs target 9. In some instances, it will be acceptable to show that the necessary precursors to releases capable of producing 100 or more fatalities are already below the target 9 BSO frequency.

Design Threat Analysis

5.40 Design Threat Analysis (DTA) is a best-estimate methodology concerned with security-based threats. Duty holders may choose to integrate any such analyses with their SAA so that each is appropriately informed by the other.

5.41 Because of the nature of scenarios forming security design basis threats the documentation associated with such analysis may need to carry a high-level protective marking.

5.42 In view of their close overlap, licensees may choose to document their DTA and SAA in combined documents. Safety-related aspects of such documents should be considered part of the facility's safety case, even though they, in part, address non-safety legislation and, in view of their likely security classification, will often need to be kept separate from the rest of the safety case. In performing their assessment of DTA scenarios safety inspectors will need to liaise with specialist security colleagues to understand the nature of the threats.

5.6 ACCIDENT MANAGEMENT STRATEGIES AND IMPLEMENTATION

5.43 This section covers how SAA should be used to inform accident management strategies including identification of measures and equipment; guidance and instructions; human and organisational factors. Further guidance can be found under SAP AM.1.

5.44 SAA should be a fundamental input to the facility's severe accident management strategies. It should also inform the off-site emergency plan (SAPs Para 672). The approach should be to use the analysis to gain confidence that accident management strategies and plans will work. Information on the potential accident progression possibilities and the resulting plant states should be used to identify the operator actions and the plant / equipment that would be required in these scenarios, and to verify that it is reasonable to expect these will be effective in the predicted environment(s).

Plant

5.45 There are two broad approaches to the provision of equipment for severe accident management. In the first approach, equipment is stored in robust locations (e.g. in offsite bunkers, or is seismically qualified and located where it will be needed) so that the SAA shows it will survive envisaged initiating events that could lead to a severe accident, and will then function for an appropriate duration in the prevailing environmental conditions. Examples of this include seismically-qualified containment filtered venting systems and Passive Autocatalytic Recombiners (PARs) used in LWRs, and diesel generators or gas turbines in heavily protected bunkers, capable of surviving severe flooding, seismic events, aircraft impacts etc.

5.46 The second approach is to use flexible equipment that can be brought to the facility and connected within reasonable timescales. These might be stored on (or near to) the site, or in central national / regional stores. Examples include mobile pumps and electrical generators, gas bottles for emergency instrument air systems, cooling

connections for fire tenders etc. Usually the equipment is over-supplied and stored in diverse locations so that even if some is damaged or made unavailable, there will still be enough to deliver the required safety functions. The provision of additional mobile equipment aligns with WENRA SRL F 4.3 and 4.4.

5.47 In the first approach, the equipment is on hand immediately to address the accident and so can be implemented quickly, without incurring excessive doses to the operators. Its location however means that it will be prone to the same initiating event that has led to the severe accident. It will also likely be inaccessible and so will need good excess capability margins. For this approach to be effective, therefore, entails robust and extensive engineering. Back fitting of such measures can be difficult and is likely to be expensive. Therefore following such an approach may not be justifiable as a reasonably practicable option.

5.48 The main advantage of the second approach is that it tends to be more flexible, which could be an essential attribute given the uncertainties of precisely what severe accident needs to be addressed. It will likely be a more cost effective option than providing robustly engineered equipment. Its main disadvantage is that these solutions will not work if connection points are damaged, or if appropriate access cannot be gained to the facility, doses to operators may be higher and the timescales for bringing the plant / equipment into service may be too long for this approach to be effective.

5.49 The approach adopted, which could be a combination of these two, thus needs to be appropriate to the individual circumstances of the facility; its adequacy should be justified within the SAA.

5.50 The plant and equipment required to address a potential severe accident, need not necessarily be designed to conservative engineering standards (SAPs Para 673). However, the use of such standards may prove necessary if the first approach is followed (e.g. in view of the potential for interfaces with other safety classified equipment (SAPs Para 167), or given the need for robust engineering).

5.51 In all cases, the SAA should justify the following for plant / equipment claimed in the analysis:

i. It can survive the initiating event, either by virtue of its inherent strength or its storage location, or through high levels of redundancy / capability to re-supply etc;

ii. It can be brought into service early enough in the accident scenario to deliver its required safety functions;

iii. Is qualified / substantiated to function in the predicted environment (pressure, temperature, humidity, radiation, chemical) till safe and stable condition is restored or further means can be introduced;

iv. Is adequately sized to deliver the required flow rate, power supply, etc to address all relevant scenarios;

v. Is suitably robust / flexible so that there is a high likelihood that the required safety functions can be delivered despite uncertainties in the nature of the actual accident that might need to be addressed;

vi. There should be adequate supplies (e.g. of fuel, lubricants, water, CO_2, air, chemicals, batteries etc), stored in suitably secure / safe conditions, to service the demands of the plant / equipment until re-stocking can be guaranteed. Experience from the Fukushima accident suggests facility autonomy-times should normally be measured in days rather than hours.

5.52 In addition, the plant / equipment identified for severe accident management is adequately controlled, maintained, inspected, tested etc, and so it needs to be provided with an appropriate classification within the licensee's scheme and then

managed accordingly. The classification applied should be informed by the licensee's SAA methodology.

5.53 Several WENRA SRLs (Appendix 1) apply to the plant / equipment provided for severe accident management at power reactors. In particular, F3.1 seeks SAA that is focussed on identifying reasonably practicable preventative or mitigating safety measures; F4.15 and 4.16 seek adequate instrumentation consistent with the facility's accident management procedures and control room requirements. SRLs F4.8 to 4.14 also provide guidance with regard to managing the condition within containment and LM3.4 relates to maintaining instruments, tools and equipment needed for accident management in good working order. As already noted, while the SRLs have been written for power reactors, the underlying principles will also apply for the SAA of other facilities.

People and Facilities

5.54 Managing and controlling a severe accident will place considerable stress upon the operators, who will likely need to undertake very demanding tasks in difficult and unfamiliar circumstances. Analysis of these tasks will therefore form a key component of the SAA, since it is hard to envisage realistic severe accident management strategies that do not require considerable human input. This will certainly apply where the strategy employed is the flexible option described in the previous section, but will also be applicable to a lesser extent where robustly engineered and installed means are adopted, as these will usually require manual initiation and ongoing operational support. In general, plant and equipment needed for severe accident management will usually be relatively low in the SAPs EKP.5 equipment hierarchy (i.e. at levels c to e) and so could necessitate significant human input.

5.55 The SAA therefore needs to provide appropriate justification that tasks identified as necessary to manage the accident will be completed successfully in sufficient time, while minimising radiological doses, giving consideration to the following;

i. the likely severe degraded conditions on the plant (e.g. the operators at Fukushima spent many hours trying to locate containment pressure relief valve controls, working in the dark, wearing Personal Protection Equipment (PPE), with normal access routes obstructed and key plant buried under debris washed-in or created by the floodwaters);

ii. emotionally stressful circumstances (e.g. family and colleagues may have been injured or killed by the initiating event, or their condition may be uncertain);

iii. lack of wider support – national infrastructure could be severely degraded and the facility(s) may need to cope on their own during the early stages of the accident.

5.56 To achieve these; the SAA will need to include appropriately detailed task analysis that looks at what needs to be done, taking due account of plausible working environments and circumstances. The details of what is expected from such task analysis are beyond the scope of this TAG. For example regarding training and emergency exercise aspects, staffing levels (including providing reinforcements in long duration accidents), maintaining communications and control structures etc; inspectors are instead referred to the human factors TAG [21] for further guidance.

5.57 The SAA should also include analysis of doses to operators during the accident. The relevant TAG on the radiological analysis of fault conditions provides guidance. This should be used to help determine aspects such as:

- Optimal ways of performing the necessary tasks;
- The need for pre-installed shielding, PPE etc;
- The staffing levels that will be required to accomplish the activities and the specifications for facilities on the site (e.g. shielding, filtration, bottled air supplies)

from where the plant will be controlled / monitored and emergency workers will be based during the accident.

5.58 Several of the above aspects are covered in WENRA SRLs. For example, LM6.3 asks for emergency interventions for severe accident management to be planned for; LM6.1 to 6.3 and R5.1 to 5.5 set standards for training for emergencies; and the R-series SRLs deal with emergency preparedness. R3.2 addresses the need for sufficient numbers of qualified staff and R4.1 to 4.3 deal with emergency facilities and the need for these to provide suitable protection for the staff working within them. Though written for power reactors, none of these SRLs is technology-specific and so all are considered to be applicable to other types of facilities capable of suffering a severe accident. Human aspects of managing severe accidents and emergencies are addressed in greater depth in the TAGs covering Human Machine Interface [22], Human Factors Integration [21] and Human Reliability Analysis [23].

Procedures and Guidance

5.59 Procedures and guidance for addressing severe accidents typically fall into two classes: Emergency Operating Procedures (EOP) and Symptoms Based Emergency Response Guidelines (SBERG); or Severe Accident Guidelines (SAG) which are also known as S.A Management Guidelines (SAMG). EOPs are symptom or event based, stepwise procedures typically developed alongside the DBA to deal with faults in Level 3 of the defence in depth hierarchy, but which can extend partly into Level 4. On power reactors, EOPs are used to prescribe fault / accident management activities up to core damage / melt and are focussed on prevention and protection. SAMGs are provided for situations that have escalated into Level 4 and are beyond the situations catered for by the EOPs. On power reactors, they apply where core damage either has occurred or is judged imminent. As suggested in their title, SAMGs are guidance intended to prompt and inform the operators of the options open to them in the circumstances; this is because of the significant range and extent of potential circumstances. SAMGs are focussed on mitigation, rather than prevention or protection; they are intended to be flexible, reflecting the range of scenarios where they might be applied, giving the plant operators freedom to use their judgement based on the prevailing circumstances, possibly without off-site support (in view of the potential for a degraded national infrastructure).

5.60 The SAA, in providing a systematic analysis of all potential severe accidents that could occur at the facility, should be a key contributor to the development of a comprehensive suite of EOPs and SAMGs. The suite of EOPs and SAMGs should address all identified potential severe accidents and cover all permitted operating modes of the facility (e.g. strategies on an LWR for a severe accident during refuelling will need to be different to those that could be used for accidents during power operation as the vessel head will have been removed).

5.61 Key aspects where the SAA can provide input to the EOPs and SAMGs include:

i. Identifying the symptoms that will allow the operators to identify the true state of the plant and / or imminent escalations in severity;

ii. The timescales and priorities for action;

iii. Appropriate points for enacting the transition from EOPs to SAMGs;

iv. Identifying alternative scenarios for how the accident might escalate and an analysis of the likely effectiveness of different strategies, including the pros and cons of each;

v. Analysis of the expected radiation dose levels and means of minimising exposures;

vi. Through task analysis, whether the procedures and SAMGs could reasonably be expected to be followed in the likely severely degraded plant condition following a severe accident;

vii. Helping to quantify the numbers of operators needed to address steps in the procedures / stages in the SAMGs;

viii. Other human factors aspects of the EOPs and SAMGs as discussed in the previous section, e.g. the availability and use of communications systems and control structures.

5.7 MULTI-FACILITY SITES

5.62 At multi-facility sites, an accident at one plant can have significant repercussions on surrounding facilities. The primary event may not be a severe accident but could lead to events with potential for consequences, which in sum exceed severe accident thresholds. Particular consideration should therefore be given to the identification of such scenarios to ensure these events can be dealt with in a coordinated manner. Consideration should be given to establishing a central site-wide control centre to coordinate response to emergencies and severe accidents. The SAA should include assessment of the likely interactions between facilities, including the repercussions of a severe accident at one facility on operations at others on the site.

5.63 A key aspect of such domino effects is the potential for an accident at one facility to limit or prevent access to other facilities, possibly for an extended period. Equally, the accident could lead to facilities on the site being starved of resources (e.g. human, equipment, supplies) as these would be needed elsewhere on the site to address the ongoing accident. The SAA should consider such possibilities for escalation of the event in order to assist with the site's overall planning.

5.64 A severe external event (such as an earthquake or a site flood) could cause the loss of site services (e.g. loss of off-site power) affecting multiple facilities. At multi-facility sites, resilience to loss of services on site should be considered within the SAA on a site-wide basis as well as for individual plants. Consideration should also be given to combinations of events e.g. loss of services coincident with other faults such as fire or explosions and the effects of such events. Analysis of these scenarios, regarding timescales and demand levels, should be used to assist with the site's prioritisation for deploying supplies and equipment to individual plants on the site.

6. REFERENCES

1 ONR *Safety Assessment Principles for Nuclear Facilities*, 2014 Edition, Revision 0. *http://www.onr.org.uk/saps/saps2014.pdf*

2 ONR Technical Assessment Guide, *Deterministic Safety Analysis and the Use of Engineering Principles in Safety Assessment*, NS-TAST-GD-006, Rev. 04, April 2015.

3 ONR Technical Assessment Guide, *Transient Analysis for DBAs in Nuclear Reactors*, NS-TAST-GD-034, Rev. 03, July 2016.

4 ONR Technical Assessment Guide, *Probabilistic Safety Analysis*, NS-TAST-GD-030, Rev. 05, June 2016.

5 INTERNATIONAL ATOMIC ENERGY AGENCY Safety Standard Series SSR-2/1 (Rev 1)*, Safety of Nuclear Power Plants: Design Specific Safety Requirements*, IAEA, Vienna, 2016.

6 Office for Nuclear Regulation *Licence condition handbook.* February 2017*.* *http://www.onr.org.uk/silicon.pdf*

7 ONR Technical Assessment Guide*, Limits and Conditions for Nuclear Safety (Operating Rules),* NS-TAST-GD-035, Rev.05, Oct 2017.

8 *The Radiation Emergency Preparedness and Public Information Regulations (REPPIR) 2001*
http://www.legislation.gov.uk/uksi/2001/2975/contents/made

9 Council Directive 96/29/Euratom (BSS96 Directive)
http://ec.europa.eu/energy/nuclear/radioprotection/doc/legislation/9629_en.pdf

10 ONR Technical Assessment Guide*, The Technical Assessment of REPPIR Submissions and the Determination of Detailed Emergency Planning Zones,* NS-TAST-GD-082, Rev. 03, Dec 2016.

11 The Ionising Radiations Regulations 2017 (IRR17)
https://www.legislation.gov.uk/uksi/2017/1075/contents/made

12 ONR Technical Assessment Guide*, Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable),* NS-TAST-GD-005, Rev. 08, July 2017.

13 *Reducing Risks, Protecting People – R2P2,* HSE Publication, 2001.

14 Western European Nuclear Regulators' Association. Reactor Harmonization Group. www.wenra.org. *WENRA Safety Reference Levels for Existing Reactors Update in Relation to Lessons Learned from TEPCO Fukushima DAI-ICHI Accident*; September 2014
http://www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for existing_reactors,

15 INTERNATIONAL ATOMIC ENERGY AGENCY, *Severe Accident Management Programmes for Nuclear Power Plants,* IAEA Safety Standards Series No. NS-G-2.15, IAEA Vienna (2009).

16 INTERNATIONAL ATOMIC ENERGY AGENCY, *Safety of Nuclear Power Plants: Commissioning and Operation,* IAEA Safety Standards Series No. SSR-2/2, IAEA, Vienna (2016).

17 INTERNATIONAL ATOMIC ENERGY AGENCY*, Safety Assessment for Facilities and Activities,* IAEA Safety Standards Series No. GSR Part 4, General safety requirements, IAEA, Vienna (2016).

18 INTERNATIONAL ATOMIC ENERGY AGENCY, *Development and Application of Level 2 Probabilistic Safety ASSESSMENT FOR Nuclear Power Plants*, Safety Specific Guide, No. SSG-4, 2010.

19 INTERNATIONAL ATOMIC ENERGY AGENCY*, Design of Reactor Containment Systems for Nuclear Power Plants,* IAEA Safety Standards Series No. NS-G-1.10, IAEA Vienna (2004).

20 INTERNATIONAL ATOMIC ENERGY AGENCY*, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants,* IAEA Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000).

21 ONR Technical Assessment Guide, *Human Factors Integration*, NS-TAST-GD-058, Rev. 03, March 2017.

22 ONR Technical Assessment Guide*, Human Machine Interface,* NS-TAST-GD-059, Rev. 3, November 2016.

23 ONR Technical Assessment Guide, *Human Reliability Analysis,* NS-TAST-GD-063, Rev. 3, April 2015.

24 Provisional HSE Internal Guidance on Dose Levels for Emergencies; *http://www.hse.gov.uk/radiation/ionising/doses/dose-pr.htm*

25 Work with Ionising Radiation - Ionising Radiations Regulations 1999 - Approved Code of Practice and guidance (HSE, 2000)

26 Documents of the NRPB Volume 1 No 4 1990 - pp 1 - 4 *Principles for the Protection of the Public and Workers in the Event of Accidental Releases of Radioactive Materials into the Environment and Other Radiological Emergencies*

27 Advisory Note, *Severe Accident Analysis for Nuclear Reactors*, TRIM Ref. 2016/61794.

28 GRS Report *Requirements on Severe Accident Analyses for ABWR Plant Design,* GRS – V – ONR195 – WSP8*,* Revision 1, 10 June 2014, TRIM Ref. 2014/276321.

Note: ONR staff should access the above internal ONR references via the How2 Business Management System.

7. GLOSSARY AND ABBREVIATIONS

ABWR	Advanced Boiling Water Reactor
ALARP	As low as reasonably practicable
BDB	Beyond Design Basis
BSL	Basic Safety Level
BSL(LL)	Basic Safety Level (legal limit)
BSO	Basic Safety Objective
CCF	Common Cause Failure
CNS	Civil Nuclear Security (Office for Nuclear Regulation)
DBA	Design Basis Analysis
DTA	Design Threat Analysis
ENSREG	European Nuclear Safety Regulators Group
EOI	Emergency Operating Instructions
EOP	Emergency Operating Procedures
HF	Human Factors
HIRE	Hazard Identification and Risk Evaluation
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
LA	Local Authority
LC	Licence Condition
LWR	Light Water Reactor
NEPLG	Nuclear Emergency Planning Liaison Group
NPP	Nuclear Power plant
ONR	Office for Nuclear Regulation
OR	Operating Rules
PAR	Passive Autocatalytic Recombiners
PPE	Personal Protection Equipment
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
REPPIR	Radiation (Emergency Preparedness and Public Information) Regulations; 2001
RoA	Report of Assessment
SAA	Severe Accident Analysis
SAG	Severe Accident Guidelines
SAMG	Severe Accident Management Guidelines
SAP	Safety Assessment Principle(s)
SBERG	Symptoms Based Emergency Response Guidelines
SF	Safety Function
SFAIRP	So far as is Reasonably Practicable
SM	Safety Measures
SRL	Safety Reference Level

SSC	Structures, Systems and Components
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association

APPENDICES

APPENDIX 1: WENRA Reactor Safety Reference Levels

Issue F - Design Extension of Existing Reactors

SRL No	Safety Reference Level	
1.	**Objective**	**Comparison SAPs [1]**
1.1	As part of defence in depth, analysis of Design Extension Conditions (DEC) shall be undertaken with the objective of improvement of the safety of the nuclear power plant by identifying ways of enhancing the plant's capability to withstand more challenging events or conditions than those considered in the design basis, minimising radioactive releases harmful to the public and the environment as far as reasonably practicable, and ensuring sufficient margins to "cliff-edge effects"[7].	Para 663 of SAPs deals with SAA to identify reasonable practicable improvements and the need to deal with more challenging events. Margins etc are covered in Para 667 and Para 669.
1.2	There are two categories of DEC: i. **DEC A:** for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved; ii. **DEC B:** with postulated severe fuel damage. The analysis shall identify reasonably practicable provisions that can be implemented for the prevention of severe accidents. Additional efforts to this end shall be implemented for spent fuel storage with the goal that a severe accident in such storage becomes extremely unlikely to occur with a high degree of confidence. Despite these provisions, severe accidents shall be postulated for fuel in the core and, if not extremely unlikely to occur with a high degree of confidence, for spent fuel in storage, and the analysis shall identify reasonably practicable provisions to mitigate their consequences.	SAPs highlight the role of PSA and DBA. It should be noted that: L1 PSA and the UK approach to DBA in effect systematically cover DEC A, and L2 PSA systematically covers DEC B. SAPs emphasise the links and relationship between SAA, PSA and DBA. Para 663 identifies more severe initiators (DEC A). All sources of radioactivity are covered by the SAPs. SAPs FA.15 requires severe accidents to be analysed. Para 611 defines the scope of SAA in line with practical elimination.
2.	**Selection of Design Extension Conditions**	
2.1	A set of DECs shall be derived and justified as representative, based on a combination of deterministic and probabilistic assessments as well as engineering judgement.	Covered in SAPs Para 666.
2.2	The selection process for DEC A shall consider all events and combinations of events, which cannot be considered with a high degree of confidence to be extremely unlikely to	DEC A terminology is not explicitly used in the SAPs. In general the DEC A type

[7] A cliff edge effect occurs when a small parameter change leads to a disproportionate and severe increase in consequences.

	occur and which may lead to accident conditions more challenging than those included in the design basis accidents. It shall cover: – Events occurring during any possible operational states of the plant; – Events resulting from internal or external hazards; – Common cause failures (CCFs); – All reactors and spent fuel storages on the site; – Events potentially affecting all units on the site, potential interactions between units as well as interactions with other sites in the vicinity.	analysis is actually the success criteria for the L1 PSA – see Para 651. TAG 30 [4] covers all plant states, CCF, hazards, all sources of radioactivity etc. The need to deal with multiple units is noted in SAP ST.6.
2.3	The set of category DEC B events shall be postulated and justified to cover situations, where the design capability of the plant is exceeded or where the equipment provided is assumed not to function as intended, leading to severe core damage.	Covered in SAPs Para 665 and FA.15; Note: the SAPs are intended to cover all types of nuclear installation, so the terminology is not always reactor centric.
3.	**Safety analysis of design extension conditions**	
3.1	The DEC analysis shall: (a) Rely on methods, assumptions or arguments which are justified[8], and should not be unduly conservative[9]; preferably, this safety function shall be fulfilled at all times; if it is lost, it shall be re-established after a transient period. (b) Be auditable, paying particular attention where expert opinion is utilized, and take into account uncertainties and their impact; (c) Identify means or possibilities to prevent fuel damage (DEC A) and mitigate severe accidents (DEC B) by enhancing the plant's capability to withstand more challenging conditions than those considered in the design basis; (d) Evaluate potential on-site and off-site radiological consequences resulting from the DEC (given successful accident management measures); (e) Consider plant layout and location, equipment capabilities, conditions associated with the selected scenarios and feasibility of foreseen accident management actions; (f) Demonstrate sufficient margins to "cliff-edge effects"; (g) Reflect insights from PSA level 1 and 2; (h) Take into account severe accident phenomena, where relevant; (i) Define an end state, which should where possible be a safe state, and associated mission times for SSCs.	a) SAPs Para 669 advocate best-estimate assumptions in the analysis. b) Point covered in SAPs and Para 671. Uncertainties and sensitivities are covered in SAP AV.6 and within the L1 and L2 PSA, TAG 30, [4]. c) The RL is a restatement of the "identify reasonably practicable measures" so is covered – see also Para 672.

[8] These methods can be more realistic than for DBA, including best-estimate. Modified acceptance criteria may be used in the analysis

[9] For the fulfilment (or re-establishment) of the fundamental safety functions in DEC A and DEC B, the use of mobile equipment on-site can be taken into account, as well as support from off-site, with due consideration for the time required for it to be available

4.	Ensuring safety functions and accident management in design extension conditions	
	General	
4.1	In DEC A, it is the objective that the plant shall be able to fulfil, the fundamental safety functions: – control of reactivity[10], – removal of heat from the reactor core and from the spent fuel, and – confinement of radioactive material. In DEC B, it is the objective that the plant shall be able to fulfil confinement of radioactive material. To this end removal of heat from the damaged core shall be established[11].	The DEC A sequences that don't get to core damage are covered within the DBA and PSA SAPs. In essence DEC B represent BDB sequences and are covered within SAA by the SAPs.
4.2	It shall be demonstrated that SSCs[42] (including mobile equipment and their connecting points, if applicable) for the prevention of fuel damage or mitigation of consequences in DEC have the capacity and capability and are adequately qualified to perform their relevant functions for the appropriate period of time.	SAPs don't distinguish between mobile and fixed equipment, but the same principles apply. Covered in SAPs EQU.1 and Paras 174-177. See Para 178 to 180 and Para 673. Also SAPs ESS.1 relevant to alternative sources
4.3	If accident management relies on the use of mobile equipment, permanent connecting points, accessible (from a physical and radiological point of view) under DEC, shall be installed to enable the use of this equipment. The mobile equipment, and the connecting points and lines shall be maintained, inspected and tested.	SAPs don't distinguish between mobile and fixed equipment, the principles apply to all equipment that may be used. ONR's LCs require adequate arrangements for examination, inspection, maintenance and testing; e.g, LC27, 28, etc.
4.4	A systematic process shall be used to review all units relying on common services and supplies (if any), for ensuring that common resources of personnel, equipment and materials expected to be used in accident conditions are still effective and sufficient for each unit at all times. In particular, if support between units at one site is considered in DEC, it shall be demonstrated that it is not detrimental to the safety of any unit.	No obvious coverage of this in Severe Accident Section of SAPs. This has been explained in this TAG. See Section 5.
4.5	The NPP site shall be autonomous regarding supplies supporting safety functions for a period of time until it can be demonstrated with confidence that adequate supplies can be established from off site.	This is covered in the LC arrangements. Section 5 also discusses the need to consider grace period to have adequate supplies from established off site locations.

10 SSCs including their support functions and related instrumentation.

11 For the fulfilment (or re-establishment) of the fundamental safety functions in DEC A and DEC B, the use of mobile equipment on-site can be taken into account, as well as support from off-site, with due consideration for the time required for it to be available.

	Long-term sub-criticality	
4.6	In design extension conditions, sub-criticality of the reactor core shall be ensured in the long term[12] and in the fuel storage[13] at any time.	Need for ensuring sub-criticality is ensured post accident conditions is discussed in the tech. note [27].
	Heat removal functions	
4.7	There shall be sufficient independent and diverse means including necessary power supplies available to remove the residual heat from the core and the spent fuel. At least one of these means shall be effective after events involving natural hazards within the DEC.	The intent is covered in SAPs EDR.2, EHT.3 and subsequent Paras supporting these expectations. The expectation here is the provision for heat removal to an adequate heat sink both in normal operations and during faults and accidents. The safety case should consider the potential non-availability of external resources and also site-related environmental parameters such as variations in air and water temperatures. The contributions of such events are also expected to be covered by the supporting PSA.
	Confinement functions	
4.8	Isolation of the containment shall be possible in DEC. For those shutdown states where this cannot be achieved in due time, core damage shall be prevented with a high degree of confidence. If an event leads to bypass of the containment, core damage shall be prevented with a high degree of confidence.	This will need to be covered by L2 PSA.
4.9	Pressure and temperature in the containment shall be managed.	The expectation for management of pressure and temperature within the containment is covered in the SAPs and this TAG.
4.10	The threats due to combustible gases shall be managed.	Section 4 refers to the IAEA Guidelines, which highlights the need for managing the combustible gases post SA conditions, and are covered in the related Tech. Note [27].

12 It is acknowledged that in case of DEC B, sub-criticality might not be guaranteed during core degradation and later on during some time in a fraction of the corium.

13 This refers to decisions concerning measures on-site as well as, in case of DEC B Off-site.

4.11	The containment shall be protected from overpressure. If venting is to be used for managing the containment pressure, adequate filtration shall be provided.	Section 5.5 highlights the need for managing and preventing over pressurisation of the containment post-accident conditions and the need for consideration for overpressure protection system and provision of filtration if discharged to environment. The LWR specific issues are covered in the relevant Tech. Note [27].
4.12	High pressure core melt scenarios shall be prevented.	This is covered in the LWR Tech. Note [27].
4.13	Containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable.	This is covered in the LWR Tech. Note [27].
4.14	In DEC A, radioactive releases shall be minimised as far as reasonably practicable. In DEC B, any radioactive release into the environment shall be limited in time and magnitude as far as reasonably practicable to: (a) allow sufficient time for protective actions (if any) in the vicinity of the plant; and (b) avoid contamination of large areas in the long term.	This is a restatement of ALARP principles which underpins ONR SAPs.
	Instrumentation and control for management of DEC	
4.15	Adequately qualified instrumentation shall be available for DEC for determining the status of plant (including spent fuel storage) and safety functions as far as required for making decisions[14].	SAPs require that qualification procedures should be applied to confirm that structures, systems and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives.
4.16	There shall be an operational and habitable control room (or another suitably equipped location) available during DEC in order to manage such situations.	SAPs Para 673 and 674 cover this, but in high level to some extent. covered in Para 771 to 773 which discusses the need for developing Accident Management Strategies to manage the escalation of accidents and to restore control of the situation.

[14] This refers to decisions concerning measures on-site as well as, in case of DEC B, off-site.

	Emergency power	
4.17	Adequate power supplies during DEC shall be ensured considering the necessary actions and the timeframes defined in the DEC analysis, taking into account natural hazards.	covered in SAPs Para 771 to 773 which discusses the need for developing Accident Management Strategies to manage the escalation of accidents and to restore control of the situation.
4.18	Batteries shall have adequate capacity to provide the necessary DC power until recharging can be established or other means are in place.	covered in SAPs Para 771 to 773 which discusses the need for developing Accident Management Strategies to manage the escalation of accidents and to restore control of the situation.
5.	**Review of the design extension conditions**	
5.1	The principle of continuous improvement shall be applied to design extension conditions. In addition to regular review of design extension conditions, specific reviews shall be undertaken in response to significant operating experience and significant new information relevant to safety. All reviews of design extension conditions shall use both deterministic and probabilistic approaches to identify needs and opportunities for improvement.	ONR SAPS cover the generality of this for all elements of the safety case and as such there is no direct reference to this expectation.

APPENDIX 1 Contd.: WENRA Reactor Safety Reference Levels

Issue LM – Emergency Operating Procedures and Severe Accident Guidelines

SRL No	Safety Reference Level
1.	**Objective**
1.1	A comprehensive set of Emergency Operating Procedures (EOPs), as well as guidelines for Severe Accident Management (SAMG) shall be provided, covering accidents initiated during all operational states.
2.	**Scope**
2.1	EOPs shall be provided to cover Design Basis Accidents. These EOPs shall provide instructions for recovering the plant state to a safe condition.
2.2	EOPs shall be provided to cover DEC A. The aim shall be to re-establish or compensate for lost safety functions and to set out actions to prevent core and spent fuel damage.
2.3	SAMGs shall be provided to mitigate the consequences of severe accidents for the cases where the response to events including the measures provided by EOPs have not been successful in the prevention of core damage.
2.4	EOPs for Design Basis Accidents shall be symptom based or a combination of symptom based and event based[15] procedures. EOPs for DEC shall be symptom based unless an event based approach can be justified.
2.5	EOPs and SAMGs shall be suitable to manage accidents that simultaneously affect the reactor and spent fuel storages, and shall take potential interactions between reactor and spent fuel storages into account.
2.6	Possibilities for one unit, without compromising its safety, supporting another unit on the site shall be covered by EOPs and SAMGs.
2.7	EOPs and SAMGs shall be such that they are able to be implemented even if all nuclear installations on a site are under accident conditions, taking into account the dependencies between the systems and common resources.
3.	**Format and Content of Procedures and Guidelines**
3.1	EOPs shall be developed in a systematic way and shall be supported by realistic and plant specific analysis performed for this purpose. EOPs shall be consistent with other operational procedures, such as alarm response procedures and severe accident management guidelines.
3.2	EOPs shall enable the operator to recognise quickly the accident condition to which it applies. Entry and exit conditions shall be defined in the EOPs to enable operators to select the appropriate EOP, to navigate among EOPs and to proceed from EOPs to SAMGs.
3.3	SAMGs shall be developed in a systematic way using a plant specific approach. SAMGs shall address strategies to cope with scenarios identified by the severe accident analyses[16].

[15] Event-based EOPs enable the operator to identify the specific event, and
Symptom-based EOPs enable the operator to respond to situations for which there are no procedures to identify accurately the event that has occurred.

3.4	EOPs for design basis accidents shall rely on adequately qualified equipment and instrumentation. For DEC, EOPs and SAMGs shall primarily rely on adequately qualified equipment.
3.5	EOPs and SAMGs shall consider the anticipated on-site conditions, including radiological conditions, associated with the accidents they are addressing and the initiating event or hazard that might have caused it.
4.	**Verification and Validation**
4.1	EOPs and SAMGs shall be verified and validated in the form in which they will be used in the field, as far as practicable, to ensure that they are administratively and technically correct for the plant, are compatible with the environment in which they will be used[17] and with the human resources available.
4.2	The approach used for plant-specific validation and verification shall be documented. The effectiveness of incorporating human factors engineering principles in procedures and guidelines shall be judged when validating them. The validation of EOPs shall be based on representative simulations, using a simulator, where appropriate.
5.	**Review and Updating of EOPs and SAMGs**
5.1	EOPs and SAMGs shall be kept updated to ensure that they remain fit for their purpose.
6.	**Training and exercises**
6.1	Control room staff shall be regularly trained and exercised, using full-scope simulators for the EOPs and simulators, where practicable, for the SAMGs.
6.2	Licensee emergency response staff shall be regularly trained and exercised, commensurate with their expected role in managing an emergency, for situations and conditions covered by EOPs and SAMGs.
6.3	The transition from EOPs to SAMGs for management of severe accidents shall be regularly exercised.
6.4	Interventions called for in EOPs and SAMGs and needed to restore necessary safety functions, including those which may rely on mobile or off-site equipment, shall be planned for and regularly exercised. The potential unavailability of instruments, lighting and power and the use of protective equipment shall be considered.

[16] Analysis aimed at identifying the plant vulnerabilities to severe accident phenomena, assessment of plant capabilities and development of accident management measures, including for containment protection as defined in Issue F (Design Extension of Existing Reactors) in RLs 4.8 to 4.14. It is understood that for these accident conditions also SAMGs shall be developed.

[17] In particular, expected manual operation of equipment shall be possible.

APPENDIX 1 Contd.: WENRA Reactor Safety Reference Levels

Issue R – On-site Emergency Preparedness

SRL No	Safety Reference Level
1.	**Objective**
1.1	The licensee shall provide arrangements for responding effectively to events requiring protective measures at the scene for: (a) Controlling an emergency situation arising at their site, following any reasonably foreseeable event, including events related to combinations of hazards as well as events involving all nuclear installations and facilities on the site; (b) Preventing or mitigating the consequences at the scene of any such emergency: and (c) Co-operating with external emergency response organizations in preventing adverse health effects in workers and the public.
2.	**Emergency Preparedness and Response Plan**
2.1	The licensee shall prepare an on-site emergency plan and establish the necessary organizational structure for clear allocation of responsibilities, authorities, and arrangements for co-ordinating plant activities and co-operating with external response agencies in a timely manner and throughout all phases of an emergency.
2.2	The licensee shall provide for: (a) Prompt recognition and classification of emergencies, consistent with the criteria set for alerting the appropriate authorities; (b) Timely notification and alerting of response personnel; (c) Ensuring the safety of all persons present on the site, including the protection of the emergency workers; (d) Informing the authorities and the public, including timely notification and subsequent provision of information as required; (e) Performing assessments of the current and foreseeable situation on the technical and radiological points of view (on and off site); (f) Monitoring radioactive releases; (g) Treatment and first aid of a limited number of contaminated and/or overexposed workers/persons on site; and (h) Plant management and damage control.
2.3	The site emergency plan shall be based upon an assessment of reasonably foreseeable events and situations that may require protective measures on- or off-site. The plan shall: - address long-lasting situations; - clarify how site (and if applicable corporate) resources (human and material) common to several installations are used; - be co-ordinated with all other involved bodies; The plan shall be capable of extension, should more severe events occur.

3.	**Organisation**
3.1	The licensee shall have people on-site at all times with the authority and responsibilities to classify and declare an emergency and, upon classification, to initiate promptly the appropriate on-site response[18].
3.2	Sufficient number of qualified personnel shall be available at all times for staffing appropriate positions promptly following the declaration and notification of an emergency. Arrangements shall be established to ensure that sufficiently qualified personnel can staff appropriate emergency positions in long-lasting situations.
3.3	Arrangements shall be made to provide technical assistance to operational staff. Teams for mitigating the consequences of an emergency (e.g. radiation protection, damage control, fire fighting, etc) shall be available.
3.4	Arrangements shall be made to alert off-site responsible authorities promptly.
3.5	The licensee shall identify those who are authorized to carry out the response functions assigned in the emergency plan.
3.6	The licensee emergency response shall be functional in cases where infrastructures at the site and around the site are severely disrupted.
3.7	Arrangements to support on-site actions shall be in place with considerations for large-scale destruction of infrastructure in the vicinity of the site due to external hazards.
4.	**Facility and Equipment**
4.1	Appropriate emergency facilities shall be designated for responding to events on site and that will provide co-ordination of off-site monitoring and assessment throughout different phases of an emergency response.
4.2	An “On-site Emergency Control Centre”, which is separated from the main control room, shall be provided for on-site emergency management staff. Important information shall be available in the control centre about the plant and radiological conditions on and around the site. The centre shall have means of communicating with the control room, any supplementary control room, other important points on site, and with the on-site and off-site emergency response organizations[19].
4.3	Emergency facilities shall be suitably located, designed and protected to: - remain operational for accident conditions to be managed (including design extension conditions) from these facilities; - allow the protection from radiation as well as control of radiation exposure of emergency workers. Appropriate measures shall be taken to protect those occupying emergency facilities for a protracted time from hazards resulting from accidents.
4.4	Instruments, tools, equipment, documentation, and communication systems for use in emergencies (including necessary mobile equipment), whether located on-site or off-site, shall be stored, maintained, tested and inspected sufficiently frequently so that they will be available and operational during DBA and DEC. Access to these storage locations shall be possible even in case of extensive infrastructure damage.

[18] The on duty shift supervisor could be among those authorised to declare an emergency and to initiate the appropriate on-site response.

[19] The On-site Emergency Control Centre is the office accommodation and associated office services set aside on or near to the site for staff who are brought together to provide technical support the operations staff during an emergency or where the licensee emergency response is directed. It may have plant information systems available, but is not expected to have any plant controls.

5.	Training, Drills and Exercises
5.1	Arrangements shall be made to identify the knowledge, skills, and abilities needed for personnel (operating organization staff and, if necessary, contractors) to perform their assigned response functions.
5.2	Arrangements shall be made to inform all employees and all other persons present on the site of the actions to be taken in the event of an emergency.
5.3	Training arrangements shall include basic emergency training and ongoing refresher training on an appropriate schedule and shall ensure that emergency response personnel (operating organization staff and, if necessary, contractors) meet the training obligations.
5.4	The site emergency plan shall be regularly exercised at least annually. Some exercises shall be integrated to include as many as possible of the off-site organizations concerned. For sites with multiple nuclear installations, some exercises shall address situations affecting multiple facilities on the site. Exercises shall also include the use and connection of mobile equipment, if any.
5.5	Emergency exercises shall be evaluated systematically, and the emergency preparedness arrangements and the plan shall be subject to review and updating in the light of experience gained.

APPENDIX 2:

Severe Accident Analysis Adequacy Checklist

The checklist below is not an exhaustive list of questions to consider, but is intended as a quick guide that can be used as a starting point when assessing the adequacy of a licensee's safety case.

Severe Accident Analysis Criteria

Severe Accidents are defined in the SAPs to be

> *"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.*"

Standards Addressed

1. Does the submission and supporting analysis use and make reference to accepted standards and relevant good practice such as IAEA guidelines, WENRA Reference Levels and any relevant operational experience?
2. If not, what justifications are given for not using such references?
3. Has severe accident analysis been used in the consideration of further risk-reducing measures?

Engineering Key Principles

1. Does the design include measures to prevent the development of a transient or fault into a severe accident?
2. Does the design of the facility achieve defence in depth against potentially significant faults or failures by the addition of measures to mitigate the consequences of severe accidents?
3. Are the mitigation measures sensitive to any perturbations to accident conditions resulting from an operational state?
4. Are there any positive feedback mechanisms or cliff-edge effects inherent in the design or the provision of the mitigation measures?
5. Is the SAA comprehensive, does it cover the period and required to bring the facility to safe and stable conditions and does it consider findings from other analyses (DBA and PSA)?
6. Is there sufficient provision of monitoring equipment to provide the operators with information regarding the plant state and accident progression?
7. Has the proposed equipment been qualified for the operating environment that may exist during post-accident conditions and the duration claimed to bring the plant to a safe and stable condition?
8. Does the design incorporate features to provide adequate heat removal capability, prevent re-criticality and maintain containment, in the event of a severe accident?
9. Is the fixed and mobile recovery equipment accessible in conditions that may exist following severe accident conditions?

Initiating Faults

Does the submission consider the scenario that should typically be addressed within the scope of a licensee's SAA?

a. High consequence events of low frequency beyond the design basis; and

b. Design basis events where the safety provisions are assumed to fail;

Fault Sequences

1. Has a comprehensive list of initiating events been developed including those beyond design basis events originally screened out of the DBA on the grounds of low frequency?
2. Have the initiating faults been fully developed into any corresponding fault sequences, and have subsequent failures caused by the initiating fault also been considered?
3. Has the licensee elected to include accidents initiated by a security incident within the SAA?
4. Are all plant states considered, including shutdown and maintenance states?
5. Do the fault sequences consider the possible combinations of plant for equipment outages, maintenance or repair?

Defence-in-Depth

1. Are there adequate layers of protection or barriers between the radioactive materials and the outside world?
2. Do these barriers derive from a conservative engineered design with appropriate safety margins, or are the barriers administrative and managerial.
3. What is the evidential basis provided in the analysis for having confidence in any claimed administrative or managerial safety measures?

Fault Consequences and Analysis

1. Are the fault analysis tools used appropriate and the analytical models sufficiently detailed to capture all of the relevant features of the fault transient sequences and supported by appropriate validation?
2. Has the SAA been carried out in a systematic manner looking in turn at how each fundamental safety function will be delivered during the accident?
3. Does the SAA utilise deterministic, best-estimate analyses to predict options for how the accident might progress? Has consideration been given to the level of uncertainty associated with the analysis?
4. Does the SAA cover the behaviour of the plant until safe and stable conditions are achieved?
5. Have arrangements been made for emergency preparedness and response in case of an accident?

Control and Instrumentation of Safety Related Systems

1. Is suitable and sufficient safety-related system control and instrumentation available to the facility operator in a control room, and as necessary at appropriate secondary control or monitoring locations remote from the plant?

SSCs, SF and SM

1. Are Safety Functions (SF) defined as a natural consequence of the analysis, and does the analysis also identify corresponding Safety Systems and Components (SSCs) which will provide the required SF?
2. Are suitable and sufficient Safety Measures (SM) defined to provide dose mitigation?
3. Have the effects of adverse environmental conditions (such as high temperatures, pressures, radiation, adverse weather) on any claimed SM or SSCs been considered in the analysis?
4. Do the SM claimed as protection act in a passively safe manner such that they rely on natural physical mechanisms such as natural convection, gravity driven feeds and radiative processes to provide their defined safety function?
5. Are any claims of high structural integrity made for key SSCs?

EOP and SAMGs

1. Are there appropriate Emergency Operating Procedures (EOPs) which provide clear, concise and unambiguous guidance to the operators?
2. Are there appropriate Severe Accident Management Guidelines (SAMGs) which provide clear, concise and unambiguous guidance to the operators?

Additional Considerations

1. Has an accepted, recognised systematic and auditable process been used to identify all of the potential initiating events/scenarios?
2. Have Human Factors (HF) been considered as fault initiators and subsequent influence on the severe accident?
3. Have the initiating event frequencies been calculated on a best-estimate basis, with the dose consequences being calculated conservatively? Noting that the dose calculations referred to here are to identify the unmitigated consequences to see whether SAA is required.
4. The dose calculations when considering the mitigated consequences for supporting the L3 PSA and for off-site planning should be best-estimate like the rest of the analysis for SAA.
5. Does the analysis also consider any interdependencies or interconnectivity between the plant of interest and any surrounding plant in terms of initiating faults?
6. Finally, have adequate considerations been given to the application of ALARP and relevant good practice in the submissions supporting the sever accident analysis.