Office for Nuclear Regulation

ONR GUIDE			
DESIGN BASIS ANALYSIS			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-006 Revision 5		
Date Issued:	October 2020	**Review Date:**	October 2025
Approved by:	A Hart	Technical Director	
Record Reference:	CM9 2020/37019		
Revision commentary:	Major update to title, scope and technical content		

TABLE OF CONTENTS

Published 10/20

1. INTRODUCTION

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

2. PURPOSE AND SCOPE

2.1 The primary aim of this document is to provide technology-neutral guidance to ONR inspectors in support of the SAPs, so that the adequacy of licensee safety cases can be assessed more effectively and efficiently, and to guide inspectors in the exercise of their regulatory judgement. It is not intended to provide prescriptive instructions to licensees on how to design their facilities, undertake their activities or write their safety cases.

2.2 'Design basis' is an engineering term which refers to the conditions that are taken into account in the design of a facility. The International Atomic Energy Agency (IAEA) provides a definition of the term as (Ref. 2):

> *The range of conditions and events taken explicitly into account in the design of structures, systems and components and equipment of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits.*

2.3 'Design basis analysis' (DBA) is deterministic analysis used to establish many of the conditions that are considered when designing or modifying a facility. Its aim is to provide a robust demonstration of the fault tolerance of the facility and the effectiveness of its safety measures. Any uncertainties in the fault severity, progression and consequence analyses are usually addressed by the use of appropriate conservatism. In this approach, risk is not quantified, but the adequacy of the design and the suitability and sufficiency of the safety measures are assessed against deterministic rules or design principles.

2.4 This TAG does not cover specific analysis types used to demonstrate that safety measures are effective (e.g. reactor transient analysis, mechanical analysis, etc.) but provides advice to inspectors on a framework that such analyses can be performed within, as part of the wider demonstration that the risks from faults are reduced to as low as reasonably practicable (ALARP). It is therefore written with the intent of providing guidance on DBA to most technical specialists within ONR.

2.5 It is important to note that DBA is only part of the overall body of analysis that should be considered in the design and reported within a safety case. International consensus is that the appropriate strategy for achieving safety objectives is through the application of defence in depth. The conservative, deterministic approach taken to DBA has a role to play in demonstrating the effectiveness of some levels of defence in depth, but to ensure that the constraints on construction and operation are not unduly onerous, its application should be limited to faults with significant unmitigated radiological consequences and initiating event / sequence frequencies within a defined frequency range.

2.6 A combination of deterministic and probabilistic methods should be followed by the licensee (and reported in the safety case) to demonstrate the extent and effectiveness of the defence in depth provision included within a nuclear facility to ensure fault tolerance. The expectations for these wider analyses (i.e. probabilistic safety analysis,

PSA, and severe accident analysis, SAA), which could also influence the design and operations of a facility, are different from those of DBA, and therefore are largely outside the scope of this TAG. However, some advice is provided on how aspects of the DBA SAPs could help to judge these interfacing aspects of a safety case.

Terminology

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

Structure, system and / or component (SSC): An item important to safety within the facility design which provides a safety function.

Fault (or event): Any unplanned departure from the specified mode of operation of a SSC due to a malfunction or defect within the SSC, or due to external influences or human error.

Safety system: A system that acts in response to a fault to protect against radiological consequences.[1]

Safety measure: A safety system or a combination of procedures, operator actions and safety systems that protect against a radiological consequence, or a specific feature of plant designed to prevent or mitigate a radiological consequence by passive means.

Safety-related system: A system in place to perform an operational function but which also provides a safety benefit. This is distinct from safety systems, which are systems which do not perform any operational functions and are included solely because of the safety functions they perform.

Fault sequence: A combination of an initiating fault and any additional failures, faults and internal or external hazards which have the potential to lead to an accident. Fault sequences can also include any safety measures or safety-related systems which are expected to respond to the initiating fault and the subsequent transient.

A *design basis fault sequence* is the sequence considered in the (conservative) DBA. It can bound several similar initiating faults with a range of severities and assumes the successful operation of the claimed safety measures whose effectiveness is being demonstrated by the DBA (albeit with a limiting single failure amongst the safety measures). The correct performance of any associated safety-related or non-safety equipment, where it would alleviate the consequences of the fault, is not assumed.

2.8 *Licensee* has been used throughout this TAG as a single term that includes other dutyholders, Requesting Parties participating in a Generic Design Assessment (GDA), and any other organisation or individual involved in the development or application of DBA. *Designer* has been used in some cases to give an indication of where in the life cycle of a facility safety case activity should be undertaken. The designer may or may not be the Licensee or Requesting Party.

2.9 *Hazard* is generally used with reference to internal and external hazards, where it applies to an initiating or consequential event that directly challenges the safety of a

[1] The IAEA definition (Ref. 2) states that safety systems consist of a protection system, the safety actuation system, and the safety system support features (the services such as cooling, lubrication and power that are required by the protection and actuation systems). Ref. 2 also acknowledges that components of safety systems may be provided solely to perform safety functions, or may perform safety functions in some operational states and non-safety functions in other operational states.

nuclear facility (such as a fire, flood or earthquake). However, it has also been used (usually preceded by *radiological)* to refer to the potential for harm arising from the intrinsic property or disposition of something to cause detriment. Some safety case methodologies mentioned in this TAG may include hazard in a different context (for example, HAZOP) but beyond using it to define an abbreviation, the term has not been used in that way.

3. RELATIONSHIP TO LICENCE CONDITIONS AND OTHER RELEVANT LEGISLATION

3.1 The Licence Conditions (LCs) place legal requirements on the licensee to make and implement arrangements to ensure that safety is being managed adequately. The licence conditions provide a legal framework which can be drawn on in assessment.

> *Licence Condition 23 - Operating Rules: "The licensee shall, in respect of any operation that may affect safety, produce an adequate safety case to demonstrate the safety of that operation and to identify the conditions and limits necessary in the interests of safety. Such conditions and limits shall hereinafter be referred to as operating rules"….. "The licensee shall ensure that operations are at all times controlled and carried out in compliance with such operating rules".*

3.2 DBA has a significant role to play in the safety case for demonstrating the safety of operations. Assumptions made in DBA demonstrations are only valid if they are reflected in the design and operation of a facility, and therefore it is an important source of conditions and limits, and relevant to a licensee's LC23 arrangements.

> *Licence Condition 24 - Operating Instructions: "The licensee shall ensure that all operations which may affect safety are carried out in accordance with written instructions hereinafter referred to as operating instructions"…. "The licensee shall ensure that such operating instructions include any instructions necessary in the interests of safety and any instructions necessary to ensure that any operating rules are implemented".*

3.3 DBA has a role to play in identifying human actions which are important for the delivery of safety functions. LC24 is important for ensuring human based safety claims made and set out in the safety case are achieved on the plant. The written instructions produced in accordance with this LC are derived from the safety case, and should detail how safety measures reliant on human actions are to be prompted and enacted. Therefore, there should be a clear and unambiguous link from the DBA to the relevant parts of these instructions to ensure operations are implemented in line with safety case expectations. This linkage should also extend to the derivation of the operating instructions which facilitate and ensure that the operators are able to comply with the operating rules, and hence keep the plant within its safe operating envelope.

> *Licence Condition 15 - Periodic Review: "The Licensee shall make and implement adequate arrangements for the periodic and systematic review and reassessment of safety cases".*

3.4 DBA is not just a 'one-shot' process, carried out only during the initial design phase of a facility. The legal requirement of LC15 is that the licensee must carry out periodic reviews of its safety cases. This is necessary, as facilities may degrade over time, or be progressively modified in some way, or be used in a way not conceived of in the original design. Legacy nuclear facilities may not have been originally designed with the same level of analytical and engineering rigour that would be used if those same facilities were to be designed today. Therefore it is expected that all nuclear facilities

review their DBA (alongside other portions of the safety case) when performing periodic reviews to ensure that it remains appropriate.

> *Licence Condition 27 - Safety Mechanisms, Devices and Circuits: "The licensee shall ensure that a plant is not operated, inspected, maintained or tested unless suitable and sufficient safety mechanisms, devices and circuits are properly connected and in good working order".*
>
> *Licence Condition 28 - Examination, Inspection, Maintenance and Testing (EIMT): "The licensee shall make and implement adequate arrangements for the regular and systematic examination, inspection, maintenance and testing of all plant which may affect safety".*

3.5 DBA should identify and quantify the safety functions required to be delivered to ensure the safety of the facility. This in turn leads to the requirement to have suitable and sufficient safety measures which can be demonstrably shown to reduce the consequences ALARP. Hence a rigorous DBA should also identify any safety measures required, the safety classification that is to be applied, and the associated design, reliability, availability, qualification and code / standards requirements that follow from the safety classification.

3.6 Given DBA's central role in safety function categorisation and SSC classification, it also has an important role in informing EIMT requirements. The licensee will need to demonstrate that any SSC considered in the DBA safety case can perform its safety function to a level commensurate with its classification. EIMT will be part of this ongoing demonstration throughout the lifetime of the facility.

3.7 Taking plant out of service in order to perform EIMT may compromise the provision of safety functions. DBA can be used to inform and define conditions governing permitted plant configurations and the availability of safety systems and safety-related equipment. The permissible plant configurations need to be carefully defined (generally through limits and conditions) in order that nuclear safety is not reduced by taking plant out of service.

4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS

SAPs and interfacing TAGs

4.1 The SAPs EKP.1 and EKP.2 (Ref.1) establish the general expectations that the aim for any nuclear facility should be an inherently safe design (consistent with the operational purpose of the facility) and that the sensitivity of the facility to potential faults should be minimised. However, even when these expectations are met so far as is reasonably practicable, there is still a need for potential faults to be identified and considered within the design.

4.2 SAP EKP.3, consistent with IAEA Safety Requirements (Refs 3 and 4), states that nuclear facilities should be designed and operated with defence in depth against potentially significant faults or failures through the provision of multiple independent barriers. Defence in depth should prevent faults, or if prevention fails should ensure detection, limit the potential consequences and stop escalation.

4.3 Defence in depth is generally applied in five levels, which should be, as far as practicable, independent from one another. The aim of each level, as set out in IAEA documentation, is summarised in Table 1 of the SAPs:

Level	Objective	Defence/Barrier
Level 1	Prevention of abnormal operation and failures by design	Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels
Level 2	Prevention and control of abnormal operation and detection of failures	Control, indication, alarm systems or other systems and operating procedures to prevent or minimise damage from failures
Level 3	Control of faults within the design basis to protect against escalation to an accident	Engineered safety features, multiple barriers and accident or fault control procedures
Level 4	Control of severe plant conditions in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents	Additional measures and procedures to protect against or mitigate fault progression and for accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Emergency control and on- and off-site emergency response

4.4 DBA is an essential component of the wider demonstration that is needed in a safety case to show that a facility is fault tolerant, and that it has adequate defence in depth. The long standing approach in GB safety cases is that DBA focuses on the effectiveness of Level 2 and 3 defence in depth measures, through the consideration of all faults with significant unmitigated radiological consequences and initiating event frequencies greater than 1×10^{-5} pa.

4.5 SAPs FA.1 to FA.3 on the general requirements of fault analysis are a pre-requisite for DBA, as they are for the other complementary probabilistic and deterministic analysis methods (PSA and SAA) that should be applied in a suitable and sufficient way in a safety case. SAPs FA.4 to FA.9 specifically relate to DBA. This TAG is therefore focused on providing advice on the interpretation and application of these SAPs.

4.6 SAPs ECS.1 and ECS.2 define some important principles for the effective implementation of the safety aspects sought by many subsequent engineering principles. ECS.1 states that safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regard to safety. ECS.2 states that SSCs that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety. The requirement to categorise safety functions and classify SSCs (and operator actions, where appropriate) applies across all levels of defence in depth within the control of a licensee (it may not be a practicable proposition for some aspects of Level 5 defence in depth) but it is a fundamental aspect of DBA. Safety functions identified as necessary through DBA are likely to be categorised highly, and SSCs claimed in the safety case as having the highest safety classifications will almost certainly need to be substantiated through the application of DBA. However, detailed guidance on the assessment of categorisation and classification schemes in safety cases, consistent with SAPs ECS.1 and ECS.2 is provided outside of this TAG in NS-TAST-GD-094 (Ref. 5).

4.7 There are many other engineering principles in the SAPs which are directly linked or associated (sometimes implicitly) with DBA. The extent to which they apply, can be relaxed, or should be subject to additional regulatory attention often depends upon the safety classification applied to a safety measure, and therefore the extent to which the

safety measure is claimed in the DBA. Notable for their close association with DBA are:

- EKP.4 and EKP.5 on safety function and safety measures
- EDR.1 to EDR.4 on design for reliability
- ERL.1 to ERL.4 on reliability claims
- EHA.1 to EHA.18 on external and internal hazards
- ESS.1 to ESS.27 on safety systems
- ERC.1 to ERC.4 on reactor core
- EHT.1 to EHT.5 on heat transport systems
- EHF.1 to EHF.12 on human factors
- ECR.1 and ECR.2 on criticality safety.

4.8 This TAG is focused on the high level principles and concepts of DBA and does not generally go into the detail associated with these engineering SAPs. However, most of these SAPs have their own TAGs:

- NS-TAST-GD-013: External Hazards (Ref. 6)
- NS-TAST-GD-014: Internal Hazards (Ref. 7)
- NS-TAST-GD-003: Safety Systems (Ref. 8)
- NS-TAST-GD-036: Redundancy, Diversity, Segregation and Layout of Mechanical Plant (Ref. 9)
- NS-TAST-GD-041: Criticality Safety (Ref. 10)
- NS-TAST-GD-060: Procedure Design and Administrative Controls (Ref. 36)
- NS-TAST-GD-075: Safety of Nuclear Fuel in Power Reactors (Ref. 11).

4.9 With regards to criticality safety, SAP ECR.2 states that criticality safety cases should employ the double contingency approach. Additional advice is provided in NS-TAST-GD-041 (Ref. 10) on how this approach can be used alongside and together with DBA techniques (such as fault identification and analysis of consequences) in a safety case, and therefore it is not repeated within this TAG.

4.10 The numerical targets in the SAPs are used by inspectors as an aid to judgement when considering whether radiological hazards are being adequately controlled and risks reduced to ALARP. Numerical Target 4 specifically applies for DBA. It provides suitably challenging objectives and graded limits (determined by initiating fault frequency) for the effective dose received by any person on or off site.

Design basis fault sequences – any person	**Target 4**

The targets for the effective dose received by any person arising from a design basis fault sequence are:

On site:

BSL: 20 mSv for initiating fault frequencies exceeding 1×10^{-3} pa
200 mSv for initiating fault frequencies between 1×10^{-3} and 1×10^{-4} pa
500 mSv for initiating fault frequencies between 1×10^{-4} and 1×10^{-5} pa

BSO: 0.1 mSv

Off site:

BSL: 1 mSv for initiating fault frequencies exceeding 1×10^{-3} pa
10 mSv for initiating fault frequencies between 1×10^{-3} and 1×10^{-4} pa
100 mSv for initiating fault frequencies between 1×10^{-4} and 1×10^{-5} pa

BSO: 0.01 mSv

4.11 Its general application will be discussed in this TAG but there are other SAPs and TAGs that are relevant and potentially helpful to an ONR inspector to making judgements against Numerical Target 4 for DBA:

- SAPs FA.10 to FA.14 on probabilistic safety analysis, and the associated TAG NS-TAST-GD-030 (Ref. 12), could be relevant for coming to a view on initiating fault frequencies.
- In many cases, computer modelling is needed to predict the performance of the plant, radiological hazard, safety measures, status of barriers and to predict the source term etc in fault conditions. SAPs AV.1 to AV.8 set out expectations for the assurance requirements on data and models, and are supported by the associated TAG NS-TAST-GD-042 (Ref. 13).
- Should radionuclides bypass the physical barriers as a result of a fault condition, the dispersion and uptake of the derived source term need to be analysed. In addition to the general guidance provided by NS-TAST-GD-042, specific guidance on radiological analysis in fault conditions is provided by TAG NS-TAST-GD-045 (Ref. 15).

4.12 SAP ESS.11 and FA.8 set an expectation for a fault schedule to be included within safety cases to provide a clear link between fault, fault sequences and safety measures. In the vast majority of cases, fault schedules prioritise attention on initiating events and safety measures identified in the DBA. This TAG therefore provides additional guidance to what is stated in the two identified SAPs on ONR's expectations for fault schedules (see Section 5.9 and Appendix 2).

IAEA and WENRA Guidance

4.13 There is a significant amount of IAEA documentation relevant to the (regulatory) assessment of DBA safety cases. The General Safety Requirements publication "Safety Assessment for Facilities and Activities" Requirement 4 (Ref. 4) defines the purpose of safety assessment (undertaken by the licensee), and includes the statement:

> *The safety assessment shall address all radiation risks that arise from normal operation (that is, when the facility is operating normally or the activity is being carried out normally) and from anticipated operational occurrences and accident conditions (in which failures or internal or external events have occurred that challenge the safety of the facility or activity). The safety assessment for anticipated operational occurrences and accident conditions shall also address failures that might occur and the consequences of any failures.*

4.14 It goes on to provide further detailed guidance, including on the need to assess defence in depth (Requirement 13) and to follow deterministic approaches as part of the analysis (Requirement 15).

4.15 The Specific Safety Requirements publication "Safety of Nuclear Power Plants: Design" (Ref. 3) includes a detailed introduction of the concept of defence in depth and its application (Requirement 7). Through Requirements 13 to 28 inclusive, a series of expectations are set out for consideration in the design (i.e. the design basis for the facility). Requirement 42 defines the need for deterministic safety analysis (along with probabilistic analysis) to be undertaken to establish and confirm the design bases for all items important to safety, as part of providing assurance that defence in depth has been applied. The parallel Specific Safety Requirements publication "Safety of Nuclear Fuel Cycle Facilities" (Ref. 16) has a similar approach, with Requirement 5 stating that

the adequacy of the design needs to be verified by means of a comprehensive safety assessment that is documented and which defines the operational limits and conditions required for safety. Section 6 of this IAEA reference sets out, through Requirements 7 through 52, a set of design expectations to be demonstrated by (or be informed by) analysis. The majority of these requirements require demonstration through DBA.

4.16 The guidance provided by the relevant SAPs and this guide for what inspectors should expect to see demonstrated in safety cases is consistent with these IAEA requirements.

4.17 The IAEA has a safety guide that sets expectations for how to conduct deterministic safety analysis for nuclear power plants (Ref. 17) notably (but not exclusively) for design basis faults. Its specificity to (light water) nuclear power plants and the level of detail it provides mean that it is not a prime reference for this technology-neutral TAG but it is a useful source of relevant good practice for identifying initiating faults for inclusion within the DBA (FA.5) and how to analyse the consequences of design basis fault sequences (FA.7).

4.18 It should be noted that IAEA guidance uses the abbreviation DBA to refer to design basis accidents. Design basis accidents are typically the limiting or most onerous faults or fault sequences that set the design requirements of Level 3 defence in depth safety measures. ONR's SAPs use the abbreviation DBA for design basis analysis, and apply it to the deterministic techniques that are followed to identify and conservatively analyse faults and fault sequences which meet the criteria set out in SAPs FA.5, FA.6, FA.7 and Numerical Target 4. What the IAEA describe as design basis accidents can be considered analogous to 'infrequent design basis faults' as used in GB safety cases (initiating event frequency $< 1 \times 10^{-3}$ pa). The IAEA descriptor of 'anticipated operational occurrences' (AOO) is broadly equivalent to 'frequent design basis faults' as used in GB safety cases (initiating event frequency $> 1 \times 10^{-3}$ pa) for which it is expected that analysis is presented to show the effectiveness of independent Level 2 and Level 3 defence in depth safety measures.

4.19 Complementing the IAEA expectations, the Western European Nuclear Regulators Association (WENRA) also establishes expectations for the inclusion of defence in depth within the design of a nuclear facility, and the importance of analysis of faults within the design basis for demonstrating the effectiveness of the design. The WENRA Safety Reference Levels for Existing Reactors (Ref. 18) define a set of expected practices to be implemented in WENRA countries. Issue E on the design basis envelope establishes the need to consider defence in depth, identify safety functions to be delivered during AOOs and design basis accidents, establish a design basis, and to identify a set of internal events and external hazards to be taken into account in the design. It also requires analysis to be undertaken to show that technical acceptance criteria are met, with appropriate conservatism and safety margins included.

4.20 WENRA's report on the safety of new nuclear power plant designs (Ref. 19) also clearly establishes expectations on the application of defence in depth, with independence demonstrated between different levels. However, it also broadens the expectation that single initiators of AOOs and design basis accidents are covered to include multiple failure events as part of Level 3 defence in depth:

- AOOs and a postulated common cause failure (CCF) of redundant trains of a safety system;
- Single postulated initiating events and a postulated CCF of redundant trains of a safety system;

- Complex or specific scenarios including CCF of safety systems or safety related systems needed to fulfil the fundamental safety functions in normal operation

4.21 These WENRA expectations are consistent with the common GB practice of demonstrating diversity for frequent faults, and expectations in SAP FA.6 for fault sequences to be identified and analysed with DBA techniques down to a sequence frequency in the region of 1×10^{-7} pa.

4.22 Both IAEA and WENRA have expectations that events and sequences outside of the 'traditional' design basis should be analysed deterministically and probabilistically to show that they will not escalate into a severe accident. The IAEA publication "Safety of Nuclear Power Plants: Design" (Ref. 15) states that the purpose of this consideration of so called design extension conditions is for "further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures". This type of analysis is outside the scope of DBA and the principal intent of this TAG. However, it follows that the definition of what constitutes the limits for DBA will be highly relevant to what licensees should be analysing as beyond design basis events or design extension conditions. Some limited advice has therefore been included in Section 5 on wider deterministic analysis, by reference and exception to the guidance for DBA.

4.23 A tabular summary of how WENRA Safety Reference Levels and Objectives are covered in this TAG is supplied in Appendix 6.

5. ADVICE TO INSPECTORS

5.1 Introduction

5.1.1 LC14(1) requires the licensee to make and implement adequate arrangements for the production and assessment of safety cases consisting of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases. LC23(1) requires the licensee to produce an adequate safety case to demonstrate the safety of operations.

5.1.2 As it is a fundamental component of a safety case, a licensee should have its own robust and effective arrangements and guidance for undertaking DBA to be compliant with LC14 and LC23. It will be relatively rare for an ONR inspector to be involved in the establishment or fundamental review of a licensee's DBA arrangements. Instead, the majority of safety case submissions considered by ONR should demonstrate the application of the licensee's extant DBA methodology, which should have already been benchmarked against GB and international relevant good practice.

5.1.3 The stated primary purpose of the SAPs (Ref. 1) is to provide inspectors with a framework for making consistent regulatory judgements on safety. In the case of fault analysis, and specifically DBA, the FA series of SAPs (FA.1 to FA.9) gives guidance on what should be provided and considered, so far as is reasonably practicable, in a licensee's arrangements and the safety cases produced following those arrangements.

5.1.4 To provide structure to this TAG, each of these SAPs (FA.1-9) is considered in turn below. This guidance on each SAP can be used in isolation when assessing a specific aspect of a safety case submission, or taken together to consider whether the licensee's arrangements and safety case methodology is providing an adequate framework for DBA. However, this TAG and the associated SAPs do not stand alone. The majority of the other SAPs and TAGs are relevant to, and apply in the context of, DBA, as part of demonstrating safety.

5.1.5 Like all SAPs and associated guidance, the principles discussed in this section are used to help judge whether reducing risks to ALARP is achieved. For this reason, they are written using 'should' or similar language. Priority should be given to achieving an overall balance of safety, rather than satisfying each principle or making an ALARP judgement against each principle. It also should be noted that paragraph 626 of the SAPs states that "Other approaches may be considered if they clearly achieve the purpose of DBA".

5.2 Fault Analysis Techniques (FA.1)

5.2.1 SAP FA.1 states that analysis of the risks arising from fault and accident conditions should be carried out comprising suitable and sufficient DBA, PSA and SAA to demonstrate that risks are ALARP.

5.2.2 The supporting text to SAP FA.1 recognises that the nature and extent of fault analysis will depend on the circumstances. These circumstances could involve the stage in the development or operational life cycle of the facility, the radiological hazard associated with the facility or operation considered by the safety case, the risks from a fault associated with the facility, the age and condition of the facility, and the scope of the safety submission under consideration (for example, a complete safety case for all operations or a minor modification to an existing safety case).

5.2.3 Regardless of the circumstances, the SAPs state that it should be rare for safety submissions in support of permissioning decisions not to include DBA, even if this is just to demonstrate that there are no qualifying design basis faults. Judgements that faults and their associated radiological consequences do not meet the criteria for DBA (on either dose or frequency grounds) need to be informed by the other DBA SAPs, with potentially a similar or greater level of substantiation to that which is needed for DBA events.

5.2.4 There still might be a need for deterministic consideration of faults that do not meet DBA criteria. Although the robust, conservative approaches expected for DBA need not be applied, SAPs FA.8 and FA.9 may still provide useful guidance on how fault analysis outside of the DBA should be linked to safety functions, performance requirements of SSCs, considered through the licensee's categorisation and classification scheme, presented on a fault schedule, linked to operating rules and setpoints etc. This is discussed further in Section 5.11.

5.2.5 ONR has separate guidance for its inspectors on PSA (Ref. 12) and SAA (Ref. 20), and therefore they are not expanded upon in detail in this TAG. The three techniques for analysing fault conditions complement each other. They are not replacement or rival methods for assessing the risk, instead they offer different insights into the design of the facility and its fault tolerance. A systematic DBA does not negate the need for a probabilistic analysis, and equally meeting PSA targets does not mean DBA rules can be disregarded.

5.2.6 The three-pronged approach helps to ensure appropriate treatment of uncertainty in ONR regulatory decisions. ONR's decision making needs to take into account uncertainty by, where possible, understanding its origin, magnitude, what can be done to reduce it and how it may affect our decisions. Through a multi-faceted safety case, based on independent and diverse arguments, no undue reliance should be placed on any single facet of the argument in the safety case.

5.2.7 DBA with its use of conservative data and assumptions is important for providing confidence that both the licensee's analysis and any resulting ONR regulatory decision is demonstrably erring on the side of safety. Inspectors will need to apply professional judgement on whether assumptions or estimates are supported by appropriate

evidence as part of any assessment. In cases where there remains significant uncertainty in the frequency of the fault, an appropriate assessment conclusion may be reached by focusing on the consequences of the event. Where the size of the radiological hazard or the resulting radiological consequence of the fault is uncertain, appropriate conservative assumptions should be made.

5.2.8 However, licensees need to take care when using conservative analysis to identify potential safety improvements; there can be occasions where design or operational outcomes driven by conservative bias may be less appropriate than decisions informed by more realistic analysis. The robustness of the DBA is therefore only likely to be part of any judgement on whether the licensee has adequately demonstrated that the level of risk has been reduced ALARP. Further advice on this challenge is given in Section 5 of Ref. 29.

5.3 Identification of Initiating Faults (FA.2)

5.3.1 SAP FA.2 states that fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement.

5.3.2 In this context, significant is any fault with the potential to lead to (unmitigated) doses of 0.1 mSv to workers or 0.01 mSv to a hypothetical person outside the site. Doses lower than this are regarded as normal operation and can be excluded from the fault analysis.

5.3.3 Not all of these faults will necessarily go on to be considered through DBA, but systematically identifying all initiators is a necessary prerequisite. This is consistent with requirements set out in IAEA and WENRA guidance, for example Requirement 16 from Ref. 3, Requirement 19 from Ref. 16, and Issue E.4 from the WENRA Reference Levels for Existing Reactors (Ref. 18).

5.3.4 The process for identifying faults should be systematic, auditable and comprehensive, and include:

(a) significant inventories of radioactive material and also radioactive sources that may be lost or damaged;

(b) planned operating modes and configurations, including shutdown states, decommissioning operations, and any other activities which could present a radiological risk; and

(c) chemical and other internal hazards, man-made and natural external hazards, internal faults (i.e. within and associated with the facility in question) from plant failures and human error, and faults resulting from interactions with other activities on the site.

5.3.5 The inspector should confirm that appropriate fault identification techniques have been employed. There are multiple ways fault identification can be undertaken, depending on the technology concerned, the scope of the safety case and activities being considered, the point in the design or operational life cycle at which the fault identification is being undertaken, and the preferences of the licensee. In some cases, it may be appropriate for the licensee to apply more than one technique to demonstrate that the list of faults is comprehensive.

5.3.6 Common techniques that are often cited include:

- Hazard and Operability Study (HAZOP)

- Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA)
- Plant walk downs
- Safety function breakdown
- Review of Operational Experience (OPEX)
- Checklists.

Appendix 1 provides additional guidance on these techniques.

5.3.7 Fault identification should be a multi-disciplinary activity for the designer and licensee. Similarly, it is likely that ONR's assessment will need to be multi-disciplinary. In addition to this TAG, expectations for fault and hazard identification are set out in Refs. 6, 7 and 12. The TAG on Human Reliability Analysis (NS-TAST-GD-063, Ref. 22) provides advice for ONR inspectors on the identification and understanding of human activities that are important to safety, including through the use of task analysis or similar structured and systematic human error identification processes. The chemical engineering SAP EPE.2 (Ref. 1) also states the importance of systematic techniques such as HAZOPs for fault identification.

5.3.8 It is neither possible nor necessary for the ONR inspector to attempt to repeat the licensee's fault identification activities, especially for complex facilities and processes. Sampling is key to ONR's assessment: looking at the process followed, the appropriateness of the individuals involved, the documentation and the audit trail in addition to the final output (i.e. the list of faults identified).

5.3.9 The scope of the fault identification is an important aspect to consider. All areas of the plant or facility (such as on-site processing or storage facilities for radioactive waste) and planned operating modes and configurations (notably outages, routine maintenance and testing) should be analysed. On reactor sites, the totality of the fuel route (new fuel storage and used fuel in ponds or dry storage) has significant hazard potential should a fault sequence develop (e.g. criticality due to water ingress, fuel drop leading to compaction, or loss of cooling). During outages or maintenance, the configuration of the plant (including safety systems) is often changed from its 'normal' status, confinement barriers are deliberately and necessarily bypassed, new initiators and hazards can be introduced, and workers are often in different locations.

5.3.10 Fault identification should be cognisant that initiating faults may arise due to any interconnectivity or interdependency that may exist between the particular plant in question and other facilities on the site. This is particularly relevant to nuclear chemical process plant, where the output from one plant / process is piped to another plant / process that may require the input to be within certain limits.

5.3.11 The loss of support or essential services (such as control systems; electrical, water, gas or compressed air supplies; heating, ventilation and air conditioning (HVAC) etc.) should be considered as potential fault initiators. The loss of shared or support services may give rise to multiple common cause faults across a facility, indeed across more than one facility.

5.3.12 For nuclear power plants, the list of faults that are considered has often been developed during the evolution of the plant design and via the experience of the designers, other regulatory bodies and international experience over the course of many decades. Notable examples are Chapter 15 of the US NRC's Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition (Ref. 23) and the IAEA safety guide on deterministic safety analysis for nuclear power plants (Ref. 17). Such well-established and widely recognised sources of information can be used by the licensee and should provide a significant benchmark for the ONR inspector. However, the inspector should still seek justification as to why the list of

identified faults is appropriate for the design put forward. This should take into account any novel features, dependencies on essential services and support systems, site-specific considerations, new OPEX, and the potentially broader objective set out in SAP FA.2 (Ref. 1) for faults associated with any significant inventories of radioactive material. In addition, all permitted operating modes need to be considered (i.e. not just the reactor at power).

5.3.13 The list of faults should be kept under review by the licensee, notably during periodic safety reviews, but also in response to operational experience, change in operations and practice (for example a move from power generation to defuelling), and modifications. A significant proportion of ONR safety case assessments in support of permissioning decisions will be associated with modifications to existing plant and operations. These will not necessarily require the licensee to completely re-evaluate the list of faults for a facility however it is appropriate to consider if the modification will result in new failure modes. It is also appropriate to consider if physical intervention to make a change could result in a fault, or a failure to return the plant back to its designed state upon completion of the modification could result in a fault not identified in the original safety case.

5.4 Development of Fault Sequences (FA.3)

5.4.1 SAP FA.3 sets a general and high level expectation that fault sequences should be developed from the initiating fault and their potential (radiological) consequences analysed. The scope, content, level of detail and methods used should be proportionate to the complexity of the facility and the hazard potential.

5.4.2 A combination of deterministic and probabilistic analysis will be necessary in most circumstances. However, the extent and sophistication of the analysis will vary. For a facility with the hazard potential and complexity of a nuclear power plant, rigorous DBA, PSA and SAA should be used to identify and analyse fault sequences and their potential consequences. For less radiologically hazardous facilities and activities (for example, some decommissioning operations or the storage of immobilised low level waste), a graded approach to the safety case and associated fault analysis should be taken, including the extent to which the full rigour of DBA is applied.

5.4.3 There will be many occasions where the severity or frequency of an identified fault condition is such that DBA is an unambiguous expectation, and requirements for robust safety measures, the identification of DBA sequences, and the analysis of radiological consequences (following the successful operation of the provided safety measures) should be consistent with the expectations set out in SAPs FA.4 to FA.9. However, there will also be cases where it is not immediately clear if a fault should or should not be considered as part of the DBA.

5.4.4 There should be a justification provided by the licensee for any identified initiating event (and the resulting sequence) excluded from DBA. This justification will need to be substantiated as appropriate. In rare cases, a simple and conservative calculation of the unmitigated consequences will be sufficient. However, it will often be reasonable (indeed necessary) for more thorough analysis to be undertaken with consideration of, for example: release paths, retention / decontamination factors, occupancy times and the expected response of both SSCs and workers and the subsequent fault sequence progression.

5.4.5 The inspector should look in some detail at these assumptions. There should be a high degree of confidence that the calculated radiological consequences will not be exceeded, regardless of how the identified fault proceeds, the plant responds, or the actions any operators take. The location of workers and occupancy assumptions are often important factors to be considered. In general:

- The person under consideration remains at the point of greatest dose for the maximum duration, although for extended faults a more realistic occupancy may be assumed after a suitable interval.
- The conditions under which the fault is analysed have characteristics which produce the highest dose to that person.
- No emergency countermeasures are implemented, other than those whose implementation can be shown to be highly likely.

5.4.6 The ‘maximum’ duration used in occupancy assumptions should be taken to be an appropriately conservative upper bound but does not need to be the absolute worst case. For example, for faults that are clearly revealed to the operators but that do not injure or impede escape, it would be appropriate to select a reasonable time period for vacating the area, which should also be clearly demonstrated to be safe and possible. To ensure appropriate conservatism, some reasonable delays in evacuation (such as a blocked exit or a co-incident injury) should be considered. Other factors, such as any initial shock or confusion, the influence of co-workers, or attempts to investigate and fix a problem should also be considered. Review by specialist human factors inspectors may be required if the claims made are significant to either the design or the safety case.

5.4.7 For faults or sequences that are not clearly revealed, then appropriately conservative assumptions must be made for the period of time in which a person could be exposed to the hazard and accumulate a dose. This may be several hours, such as the duration of all or part of a shift for an operator or a day or more in the case of a member of the public off the site. All assumptions on unrevealed exposure times should be appropriately justified.

5.4.8 The definition of unmitigated consequences within the SAPs glossary allows licensees to take credit for the dose-reducing effect of passive safety features (for example, large concrete shield walls) as part of an evaluation, if these features are unaffected by the fault. In cases where this approach is presented, ONR inspectors should satisfy themselves that the claimed safety features are clearly identified, and appropriately recorded and substantiated within the safety case. Furthermore, whilst it is reasonable for the design and analysis requirements for active safety measures to take cognisance of the presence of passive safety features, such features should not be used as a reason to abandon the principle of defence in depth and the objectives of DBA (discussed in subsequent sections below).

5.4.9 It may also be possible to exclude some fault sequences from DBA on the basis of frequency. Claims that a frequent initiating event with significant unmitigated radiological consequences can be screened out on the basis of the facility having multiple low classification safety-related or unclassified SSCs / operator actions should be treated with caution. It is difficult to substantiate the necessary levels of reliability and resilience to CCF expected in a safety case for faults with significant consequences without DBA techniques and expectations.

5.4.10 There is still a requirement to consider and protect against any fault which has radiological consequences above those of normal operation, so far as is reasonably practicable. This will include the provision of preventative, protective and mitigation measures. Even if these are not engineered and substantiated to the level required for DBA, many of the expectations set out and discussed in this TAG and elsewhere could still apply in full or partially (notably SAPs ECS.1, ECS.2, ESS.11, FA.8 and FA.9) to ensure they are appropriately captured in the safety case and are available during operation. This is discussed further in Section 5.11.

5.5 Demonstration of Fault Tolerance (FA.4)

5.5.1 The requirements to demonstrate fault tolerance and to design and operate a nuclear facility with defence in depth against faults or failures are key engineering principles (EKP.2 and EKP.3) established early in the SAPs (Ref. 1). They can be linked all the way back to Principle 8 in the IAEA Safety Fundamentals (Ref. 24) for all practical efforts to be made to prevent and mitigate nuclear or radiation accidents.

5.5.2 SAP FA.4 highlights the importance of DBA in providing a robust demonstration of fault tolerance of the engineering design and effectiveness of the safety measures. It gives DBA a clear purpose within the safety case, that contrasts it with the similarly important considerations of safety in normal operation, and the complementary techniques of PSA (a powerful tool to consider the overall risk from a facility and complex interdependencies) and SAA (an aid to designing and planning for severe events should other measures and methods fail).

5.5.3 DBA should be carried out as part of the engineering design, in other words the identification of faults and the measures to protect against the consequences of those faults should be considered throughout the design process, and not be an after-thought. Where this is not possible, for example when updating the safety case following a periodic safety review of an existing facility, the DBA should be developed alongside engineering and human factors analysis of the plant, to demonstrate that safety functions are delivered with suitable levels of confidence. It may not be possible to achieve the same levels of confidence as can be substantiated on a new facility, but this does not diminish the need or expectations of DBA. Any gaps against a licensee's deterministic DBA rules or other forms of relevant good practice (such as ONR's FA SAPs) should be identified and justified in accordance with the ALARP principle.

5.5.4 On a new plant, it is important that the final commissioned design and operational practices are consistent with the DBA. On an existing facility, it is similarly important that the DBA reflects the actual engineering (including its condition, reliability and performance, which may not be the same as originally conceived) and associated management arrangements.

5.6 DBA Initiating Faults (FA.5)

5.6.1 SAP FA.5 states that the safety case should list all initiating faults that are included within the design basis of the facility. For some high hazard facilities such as a generating nuclear power plant, a significant majority of all the initiating faults identified are likely to be subject to DBA. For lower hazard facilities, for example those at an advanced stage of decommissioning or passive waste storage, there may be a limited number of faults which qualify.

5.6.2 The means by which the safety case presents the initiating faults can also be expected to vary, depending on the radiological hazards and the complexity of the facility. In all but the most straight-forward of cases, some kind of introductory section or head document for the DBA safety case should provide an overview of what faults have been included and on what basis. A fault schedule (see Section 5.9 and Appendix 2) is also a powerful means within a safety case for a licensee to demonstrate consistency with the expectations of SAP FA.5.

5.6.3 ONR's expectations of what faults should be considered for DBA are set out in the text which immediately follows SAP FA.5. However, the licensee will need to have its own rules and processes for determining which faults need to be included within its DBA. Before the ONR inspector embarks on a fault-by-fault assessment against the expectations of SAP FA.5, a view should be formed on how the licensee's generic rules compare against ONR expectations. For many established licensees, the rules

for what to include within the DBA will map across to expectations in the SAPs. However, some designs, notably reactors with overseas origins, may have identified faults for inclusion in the DBA by alternative means such as historic precedent, requirements of home country regulators (for example, Ref. 23) or IAEA expectations (Ref. 17). It is not necessary for a licensee to have an approach that is identical to that set out in the SAPs but it should expect to have the resulting safety case assessed by ONR against FA.5, and any safety significant implications of a differing approach challenged.

5.6.4 The approach set out in the SAPs is based on the unmitigated consequences and initiating frequency of a postulated fault. SAP FA.5 builds upon the expectations established by SAP FA.2, namely that faults associated with significant inventories of radioactive material in all planned operating modes should be considered, including internal hazards, man-made and natural external hazards, internal faults from plant / process failures, human error and interactions with other activities on the site. However, SAP FA.5 goes on to state ONR's expectations on what can be excluded from the DBA:

a) faults in the facility that have an initiating frequency lower than about 1×10^{-5} pa;

b) failures of SSCs for which appropriate specific arguments for preventing the initiating fault have been made

c) natural hazards that conservatively have a predicted frequency of being exceeded of less than 1 in 10 000 years; and

d) those faults leading to unmitigated consequences which do not exceed the BSL [basic safety level] for the respective initiating fault frequency in Numerical Target 4.

5.6.5 Exclusion point a) is a relatively straightforward criterion to set but it can be challenging to demonstrate. The initiating fault frequencies should be determined on a best estimate basis but they need to be appropriately substantiated. This may be by reference to probabilistic analysis of a failure mechanism (for example, fault tree analysis), operational experience, design code compliance or engineering judgement (for example, expert elicitation methods for pipe break frequencies). SAP ERL.1 states that the reliability claims for any SSC should take into account its novelty, experience relevant to its proposed environment, uncertainties in operating conditions, physical data and design methods. It is likely that any high reliability claim / low failure frequency in the region of 1×10^{-5} pa will have significant uncertainties associated with it and / or be supported by limited data. Therefore, the SAP FA.5 criterion is not an absolute limit (i.e. it says "about" 1×10^{-5} pa) and careful consideration to cliff-edge implications for the design or safety case should be explored.

5.6.6 Exclusion point b) is relevant to specific cases where special arguments are put forward that demonstrate failures of SSCs can be discounted from DBA. This is typically used where the consequences of a gross failure will be severe but there are no reasonably practicable measures that can be taken to effectively protect against those consequences (for example, the gross failure of a reactor pressure vessel). The engineering and safety case requirements for discounting a failure can be onerous, and therefore it is expected that the cases where such arguments are invoked will be limited in number. Further guidance is provided in SAPs EMC.1 to EMC.3, and the supporting TAG NS-TAST-016 (Ref 25).

5.6.7 Exclusion point c) sets a limit of the severity of natural hazards (e.g. seismic event, rainfall, extremes of temperature) to be considered by DBA. The design basis event should be derived conservatively for a 1 in 10,000 year event to take into account data and modelling uncertainties (the data are not available to support the derivation of less

frequent events). Man-made external hazards and internal hazards should be limited to conservative challenges or loads to the plant with a return frequency of 1 in 100,000 years. Further details are provided in TAG NS-TAST-GD-013 – External Hazards (Ref. 6)

5.6.8 Points a) to c) are focused on initiating event frequency. However, exclusion point d) recognises the significance of the predicted radiological consequences in the treatment of faults. The Basic Safety Levels (BSLs) set out in Numerical Target 4 provide a graded screening tool for ONR inspectors to use to judge whether an individual fault has unmitigated radiological consequences (to either on-site workers or the members of the public) that are not severe enough to merit DBA. The dose that is acceptable (for DBA not to be necessary) increases the lower the initiating event frequency.

5.6.9 The result of SAP FA.5 and Numerical Target 4 is a concept sometimes referred to as the 'design basis region'. This is a region (defined in terms of initiating event frequency and unmitigated radiological consequences) within which it is expected that initiating faults will be subject to DBA. It is illustrated graphically below in Figure 1.

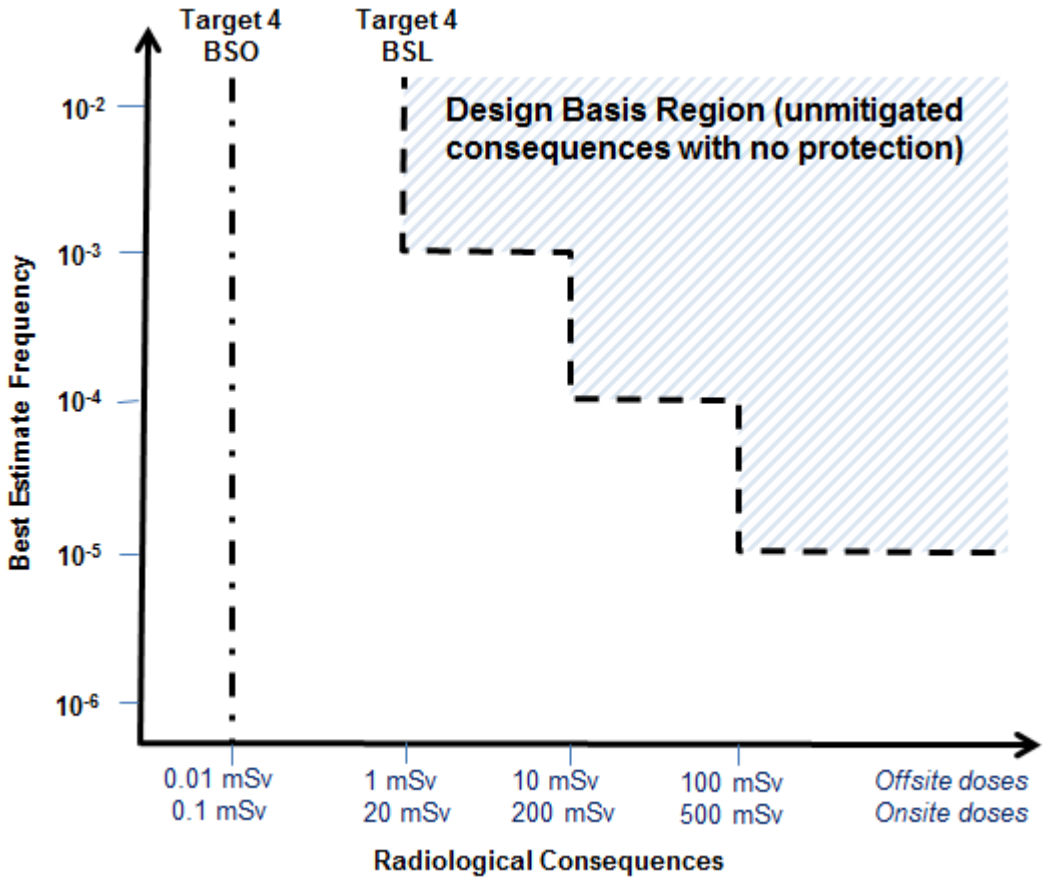

FIGURE 1 – 2014 SAPS TARGET 4 DOSE / FREQUENCY BANDS

5.6.10 As with all guidance in the SAPs, Numerical Target 4 is just a broad and initial expectation for the ONR inspector, in this case, to consider when judging whether DBA has been applied to appropriate faults. It is not a rigid rule; licensees are expected to have their own methods for determining what falls within the DBA region tailored to their specific circumstances. Consideration should also be given to uncertainties in the derived initiating event frequencies and any cliff-edge safety case implications for faults on the edges of the design basis region.

5.6.11 This definition of where DBA should be applied is not intended to imply that safety measures are not needed elsewhere. Initiating faults with unmitigated consequences below the BSLs still require consideration in the safety case and the application of relevant good practice to ensure risks are reduced ALARP. Similarly, faults with high consequences but very low frequencies (and extreme hazards) should also be considered through proportionate deterministic and probabilistic analyses to inform the judgements on the adequacy of the design provision and accident management guidance.

Further guidance on assessment of initiating event frequencies is provided in Appendix 3.

5.7 Identification of Design Basis Fault Sequences (FA.6)

Safety Measures credited in DBA

5.7.1 SAP FA.6 states that for each fault within the DBA, the relevant fault sequences should be identified. To do this, it is necessary to identify a set of safety measures to be credited in DBA which can be shown to be effective in managing the fault in question.

5.7.2 To effectively manage a fault condition, in many cases more than one safety function will need to be delivered (for example, reactivity control, cooling and confinement). Depending on the complexity of the facility and fault condition, establishing what safety functions are required could be straight forward or could require a detailed consideration within the safety case documentation. Guidance on the identification of safety functions and their categorisation is given by SAP ECS.1 (Ref. 1) and the supporting TAG NS-TAST-GD-094 (Ref. 5). Crucially, a safety function should usually be specified or described with minimal reference to the physical means of achieving it.

5.7.3 Safety measures should be identified for each safety function that needs to be delivered for the identified fault. Assuming the defence in depth principle is being followed, it is possible that there will be more than one engineered means or operator action to deliver each safety function. The SSCs providing these different means should be classified; further guidance is given in SAP ECS.2 (Ref. 1) and TAG NS-TAST-GD-094 (Ref. 5).

5.7.4 The design basis fault sequence is the principal series of assumed actions and operations, which if successfully delivered, will ensure that each safety function is provided to effectively control the consequences of the initiating event, independent of whether other defence in depth systems work as designed. The safety functions required and safety measures delivering them will usually have the highest designations in the licensee's categorisation and classification scheme.

5.7.5 Correct performance of safety-related equipment and safety measures with a low classification should not be assumed within the design basis fault sequence, unless their operation results in a greater challenge for the claimed DBA safety measures. Typically, safety-related or non-safety equipment that is not associated with or impacted by the initiating event should be assumed to have frozen in their pre-fault state (and not able to respond to the fault), or assumed to operate correctly as per their design specification, depending on which results in the most challenging scenario. The safety case should clearly explain what has been assumed, potentially substantiated with sensitivity analyses.

Design Expectations for DBA Safety Measures

5.7.6 To meet the objective for DBA to provide a robust demonstration of fault tolerance, there needs to be a high level of confidence that identified safety measures will be

available to deliver their respective safety functions. This requires the following to be taken into account:

- Safety measures need to be designed with sufficient integrity and reliability.
- No single random failure anywhere within the safety measures provided to secure a safety function should prevent the performance of that safety function.[2]
- Failures consequential upon the initiating fault (for example, SSCs lost to flood water released by a pipe break or operator access to equipment is prevented by a building collapse), and failures expected to occur in combination with the initiating fault arising from a common cause (for example, a loss of power) need to be considered.
- The qualification of the claimed SSCs (and / or human actions) to operate in the conditions they will experience, including any adverse conditions that could arise as a consequence of the fault sequence.
- The worst permitted configuration of equipment outages for maintenance, test or repair.[3]
- The most onerous initial operating states of a facility that are permitted by the operating rules.
- The time, information, procedures and training required to diagnose a fault and take appropriate action if a manual action by an operator is required.

5.7.7 Gaining confidence in the adequacy of the claimed safety measures, and therefore how the points above have been considered by the licensee in the design and safety case are likely to be a prime objective of any ONR assessment.

5.7.8 Ideally, the licensee will have a clear set of design and engineering rules for DBA safety measures, which is driven by the SSC safety classification. Design requirements for redundancy, diversity, segregation, separation, automation, independence, single failure tolerance, equipment qualification, code compliance, reliability expectations, availability constraints etc should all follow from the designated classification.

5.7.9 The ONR inspector should have an appreciation of these rules in a generic sense and sample their application in specific fault sequences. Further guidance on reliability expectations and system design is available in the EKP, EDR and ERL series of SAPs (Ref. 1), TAG NS-TAST-GD-094 on safety categorisation and classification (Ref. 5), and various engineering TAGs, including:

- NS-TAST-GD-014 Internal Hazards (Ref. 7)
- NS-TAST-GD-003 Safety Systems (Ref. 8)
- NS-TAST-GD-036 Redundancy, Diversity, Segregation, and Layout of Mechanical Plant (Ref. 9)
- NS-TAST-GD-064 Allocation of Function Between Human and Engineered Systems (Ref. 14).

5.7.10 It will usually be necessary for the licensee to further demonstrate the adequacy of safety measure design through a complementary probabilistic analysis of reliability. Similarly, ONR assessments of the adequacy of DBA safety measures are likely to require considerations of probabilistic arguments. In a narrow interpretation of the concept, DBA is a deterministic methodology that assumes claimed safety measures will work with a high degree of confidence, therefore a quantification of the likelihood of a safety measure failing and a comparison of the resulting sequence against probabilistic criteria is out of scope. However, the appropriate application of

[2] See Appendix 4
[3] See Appendix 5

deterministic rules should result in design outcomes that are consistent with numerical reliability requirements or expectations stemming from probabilistic analysis.

5.7.11 TAG NS-TAST-GD-094 (Ref. 5) sets some broad expectations for ONR inspectors on safety measure reliability based on safety classification:

SSC Class	Failure frequency per year (ff)	Probability of failure on demand (pfd)
Class 1	$10^{-3} \geq ff \geq 10^{-5}$	$10^{-3} \geq pfd \geq 10^{-5}$
Class 2	$10^{-2} \geq ff > 10^{-3}$	$10^{-2} \geq pfd > 10^{-3}$
Class 3	$10^{-1} \geq ff > 10^{-2}$	$10^{-1} \geq pfd > 10^{-2}$

5.7.12 What is actually claimed by a licensee in a safety case and is achieved by the design of the facility will vary depending on the nuclear and radiological operations of the site, and the safety classification scheme applied (the three tier approach set out in the SAPs and Ref. 5 is only one example of the type of schemes used by GB licensees). Irrespective of the exact approach taken, the safety measures and requirements associated with them should be identified and substantiated (through both deterministic and probabilistic methods) in the safety case documentation.

Diversity Expectations for DBA Safety Measures

5.7.13 Whilst a key requirement for DBA safety measures is that they are very reliable (for high consequences faults, ONR's reliability expectations will typically be consistent with those set out for Class 1 SSCs), vulnerability to CCF is difficult to eliminate, even if redundancy and single failure tolerance is a feature of the design. SAP EDR.3 (Ref. 1) states that claims for CCF should not be better than 1×10^{-5} pfd. This represents a judgement by ONR for conservative DBA considerations of what can be reasonably supported for a simple system. Complex or novel systems (for example, a SSC actuated by a software control system) should be associated with more modest reliability claims.

5.7.14 These identified bands and limits on SSC reliability and CCF provide a numerical context for a deterministic rule widely applied in licensees' safety cases, namely that diverse means of delivering safety functions should be provided for 'frequent' design basis faults. In the same way that unlikely initiating faults can be excluded, fault sequences with very low expected frequencies can be screened out of DBA. SAP FA.6 states that judgement should be exercised but for high hazard facilities, a fault sequence frequency of 1×10^{-7} pa is a typical cut-off for DBA techniques. For a low frequency initiating event considered at the edge of the design basis region (for example $<1 \times 10^{-4}$ pa) with suitable safety measure provision for each safety function (i.e. they have the design characteristics of Class 1 SSCs such as single failure tolerance and multiple redundancy), a postulated fault sequence where one or more SSCs delivering safety functions fail would be beyond ONR's expectations for DBA. In contrast, for a more frequent fault (for example $>1 \times 10^{-2}$ pa), even the best safety measure will be limited by CCF to a reliability no better than 1×10^{-5} pfd (1×10^{-4} pfd would be still be a challenging claim to substantiate), meaning that the tolerance of the facility to a fault sequence made up of the identified initiating event and the failure of a safety measure should be demonstrated through DBA.

5.7.15 In practice, this logic should manifest itself in the licensee's safety case as a general, deterministic rule for diversity to be considered and demonstrated for frequent faults through DBA, rather than as a probabilistic fault-by-fault approach to setting design expectations. However, there may be cases where a licensee puts forward

probabilistic arguments to justify the adequacy of the design basis provision on an operating facility in response to an emerging issue or challenge. A probabilistic approach can also be a useful tool for the ONR inspector to probe a licensee's deterministic DBA rules and their application to gain confidence that appropriate engineered outcomes are being provided.

5.7.16 It is therefore typical to see a single fault sequence identified for an infrequent initiating event (10^{-3} > initiating event frequency > 10^{-5} pa), which identifies Class 1 SSCs as the means to deliver the necessary safety functions. Frequent initiating events (initiating event frequency > 10^{-3} pa) will similarly be protected Class 1 SSCs but a second fault sequence should also be identified with diverse and independent safety measures for delivering the necessary safety functions. These secondary means still need to be reliable and robust to meet the expectations of DBA, but they do not necessarily need to be designed with the same levels of redundancy and single failure tolerance as the principal means identified for delivering the required safety functions. As a result, the second means could be Class 2 SSCs, from which appropriately graded design and reliability requirements follow. So far as is reasonably practicable, they should be independent, and conceptually diverse in their manner of operation, from the principal means, not share the same power supplies, control systems, HVAC, heat sinks, human resources etc and not be vulnerable to the same hazards.

5.7.17 Care should be taken not to confuse the expectation for two diverse or independent safety measures to protect against frequent faults (with significant unmitigated consequences) with the expectation set out in SAP ESS.7 for Class 1 protection systems to employ diversity in their detection of and response to fault conditions, preferably by the use of different variables. The provision of diversity within a safety measure can be a design attribute of a Class 1 SSC but it is rarely necessary to demonstrate the effectiveness of each diverse detection means through conservative DBA, unless the failure of one of those means is judged to be a limiting single failure (see Appendix 4).

Grouping of Fault Sequences for Analysis

5.7.18 Similar events leading to fault sequences protected by the same safety measures may be grouped, and their initiating event frequencies summed for the purposes of the DBA. To demonstrate the effectiveness of the safety measures, the most challenging of those similar initiating events should be considered in the analysis. For analytical simplicity and safety case clarity, it can sometimes be appropriate to combine starting conditions and consequential effects from different (but similar) initiating events to show the robustness of the common safety measures (even if these combinations are physically impossible). 'Trivial' analyses of fault sequences that are unambiguously bounded by others are not needed but it should be made clear in the safety case (potentially through the fault schedule) which initiating faults and fault sequences are covered by analyses that have been presented (see Section 5.9 on SAP FA.8).

5.7.19 The converse of this grouping approach is that initiating events leading to similar fault sequences (i.e. requiring the same safety functions to be delivered) should not be subdivided to evade requirements for DBA safety measures, notably those by the expectations that follow from a fault being designated as 'frequent', 'infrequent' or outside of the design basis region.

5.7.20 There are times when sub-dividing an initiating event is appropriate, if the variations of the same broad event can result in demands on different safety measures (as opposed to less challenging demands on the same safety measures) and therefore a different fault sequence. One example is a break in the pipework of a pressurised water reactor (PWR). A large break can be sufficient to consequentially depressurise the primary circuit, resulting in accumulator water injection and the conditions for low pressure

safety injection without any operator action. In contrast, a small break in the pipework could see the primary circuit remaining at high pressure until a deliberate action is taken to depressurise via a SSC not required in the large break fault sequence. Another example would be an initiating event occurring during 'normal' operations and the same fault occurring during a maintenance operation or outage. The prompts for SSC activation, the time taken to reach SSC setpoints, the availability of safety measures, the configuration of the plant, and the location of workers could all be significantly different during an outage, and therefore the design basis fault sequence for 'normal' operations might not be appropriate for demonstrating the effectiveness of the safety measures claimed for the shutdown version of the event.

5.7.21 Grouping can also depend on (or influence) design and safety case approaches. If the fault in question is the drop from height of a container during handling, and the safety case 'choice' is to provide a robust demonstration of the integrity of the container following the drop, it may be appropriate to group all the different ways and heights the container can be dropped by a single bounding fault sequence (the initiating event frequency will be the summation of the frequencies for all the different causes of a drop). However, if the safety case approach is to avoid (with a high degree of confidence) dropping the container, different safety measures may be required to prevent operator errors, control system faults and mechanical failures etc.

5.7.22 Fault sequences to demonstrate the effectiveness of diverse safety measures for frequent faults do not necessarily need to have different SSCs for every safety function to those assumed in the 'main' fault sequences considering the principal DBA safety measures. If the principal safety measures are well designed and maintained consistent with the expectations for Class 1 SSCs, a fault sequence that assumes the complete failure of the SSCs delivering, for example, the reactivity control, cooling and confinement functions, could be below the 1×10^{-7} pa sequence frequency cut-off established by SAP FA.6. Therefore, it may be appropriate for a design basis fault sequence intended to demonstrate the effectiveness of the diverse means of providing reactivity control to assume the successful operation of the principal safety measures for cooling and confinement. However, separate fault sequences will need to be identified to demonstrate the effectiveness of the diverse safety measures providing the other safety functions (in this example, cooling and confinement). Conservatively assuming the failure of all the principal safety measures may be an extreme scenario that is outside of the design basis region but it could reduce the analytical burden. It could also be appropriate to assume a failure of multiple principal safety measures if they share power supplies, control systems, heat sinks, human resources etc.

5.8 Analysis of Design Basis Fault Sequences (FA.7)

Acceptance Criteria

5.8.1 Paragraph 635 that accompanies SAP FA.7 states that fault sequence analysis should demonstrate, so far as is reasonably practicable, that the correct performance of the claimed passive and active safety systems should ensure that:

(a) none of the physical barriers to prevent the escape or relocation of a significant quantity of radioactive material is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity;

(b) there is no release of radioactivity; and

(c) no person receives a significant dose of radiation.

5.8.2 This should be the primary goal when demonstrating the fault tolerance of a nuclear facility through DBA. Situations such as a failure of a vessel within a large containment

structure / vault, a criticality event within a large volume of water, or a release of radioactive gases through a large bank of filters could all result in no or very limited harm to a person. However they also represent a loss of control, a degradation of at least one level of defence in depth, and could result in demands being placed on other safety measures and actions for ongoing management of safety despite the successful actuation of DBA safety measures. ONR inspectors should therefore not just consider whether the design and safety case meet the licensee's declared radiological and risk acceptance criteria, but also if they have met the expectations of SAP FA.7, especially if different options were available to manage a fault.

5.8.3 The inclusion of additional levels of defence in depth (including SSCs for severe accidents) within the design should not weaken these objectives for DBA and therefore the functional requirements of the claimed DBA safety measures. For example, the presence of a leak tight containment building and a core catcher on a new PWR design should not alter the objectives of DBA for most fault sequences, which is to show that the fuel cladding and the primary circuit remains intact through the successful operation of claimed safety measures.

5.8.4 Where these criteria cannot be fully met within the design, SAP FA.7 seeks minimal (radiological) consequences for design basis fault sequences. Some initiating events, for example those associated with a break of a pipe or the spurious opening of a relief valve on a primary circuit, are inherently associated with a loss of a physical barrier and the release of a finite amount of radioactivity. The challenge for the safety systems is often to detect that something abnormal has happened, respond quickly to terminate additional releases and take the plant to a safe, stable state before radiological limits are reached.

5.8.5 The means by which the licensee should demonstrate compliance with these expectations is through the identification of clear acceptance or success criteria in their safety cases that should be met through the correct operation of the identified DBA safety measures. The safety case should also state the origins or objectives of the applied criteria. Typically, there are two types of acceptance criteria in DBA:

- Radiological targets which ensure regulatory expectations and legal requirements are met.
- Technical criteria (sometimes referred to as derived or decoupled criteria) which relate directly to the integrity of barriers to the release of radioactive material (e.g. the fuel matrix, fuel cladding, the reactor pressure boundary, and the containment building). These will usually be specific to the type of facility and the fault sequence being considered. If these are met, the extent to which radiological targets need to be demonstrated can often be significantly reduced.

5.8.6 Where there are unique or novel features with a design or activity, the licensee will need to derive and justify the relevant technical criteria. In some 'standard' cases, for example PWRs, there may be internationally recognised criteria set by overseas regulators or industry, whether that be very specific (for example Ref. 23) or just high level (Ref. 17). These widely recognised criteria could represent relevant good practice for GB licensees and it may be appropriate for them to be used in the safety case, subject to an adequate justification of their relevance to the safety case claims being made and consistency with ONR regulatory expectations.

5.8.7 It can be appropriate for the different technical criteria to be identified based on the frequency of the initiating event. For frequent faults, there should be a strong starting expectation that no physical barriers are breached and no radioactivity is released, with a high degree of confidence. Given the relatively high likelihood that these faults occur at least once within the lifetime of the facility, it is reasonable to expect that the

successful operation of safety measures will allow an eventual resumption of operations to be justified without a substantial increase risk to workers and the public.

5.8.8 For less frequent initiating events (or design basis fault sequences where a safety measure has assumed to have failed) it may be acceptable to relax some of the criteria or have less confidence in the integrity of one physical barrier (with other barriers to release remaining intact). For example, a licensee could set a criterion for frequent reactor faults of no fuel pin failures, but claim that a small number of fuel pin failures are permissible for infrequent faults whilst still demonstrating clad melt does not occur and showing that the remaining barriers will be effective in ensuring no person receives a significant dose of radiation.

5.8.9 The SAPs are technology neutral and unlike other nuclear safety regulators, ONR does not set any specific technical criteria beyond SAP FA.7. However, the appropriateness, completeness, applicability and traceability of the licensee's declared technical criteria should be an area for consideration in an ONR assessment. Established relevant good practice also needs to come into consideration.

5.8.10 Through Numerical Target 4, ONR does have radiological targets for DBA. These are primarily provided to aid ONR's judgements on whether claimed safety measures are effective. Licensees need to establish their own radiological targets and limits. These do not necessarily need to be identical to ONR's targets in the SAPs (Ref. 1) but there are obvious advantages in ONR's and the licensee's radiological targets being consistent and comparable.

5.8.11 Radiological targets need to be consistent with the methodologies followed to predict doses for comparison. If the licensee's methodology includes best estimate assumptions or has probabilistic components, the radiological targets need to be set accordingly. ONR does not prescribe a detailed calculation route or set of assumptions to be used in DBA radiological consequences but the Numerical Target 4 values are set on the basis that the radiological consequences analysis will be conservative (but not overly pessimistic[4]). It is possible for the ONR inspector to reach regulatory judgements using a single dose value to compare against Numerical Target 4 and one of the risk targets which assume best estimate calculations (for example Numerical Target 8) but it should be done carefully and cognisant of the levels of conservatism appropriate for the different numerical targets. Further guidance on ONR's expectations for the different numerical targets, including Numerical Target 4, is given in Ref. 15.

5.8.12 Numerical Target 4 includes Basic Safety Objectives (BSOs) in addition to the BSLs. There is a separate BSO for on site and off site doses. They provide a benchmark that reflects modern safety standards and expectations, and are set at a level comparable with the BSOs for operational dose targets. They effectively quantify the deterministic expectations set out in FA.7 that DBA sequences should not result in loss of barriers and releases of radioactivity, so far as is reasonably practicable, regardless of the initiating event frequency. In situations where all technical criteria are met by the successful operation of DBA safety measures, it is often reasonable to assume the Numerical Target 4 BSOs will be met without a dose calculation.

5.8.13 If a licensee's DBA has demonstrated that the Numerical Target 4 BSOs have been met, inspectors need not seek further improvements from the licensee (to meet DBA

[4] If a fault sequence already includes conservative assumptions for pre-fault operation, performance and response time for safety measures, limiting single failures etc, it may be unnecessary or inappropriate for the licensee to layer further extreme conservatisms into the radiological consequences analysis.

objectives) and the regulatory focus should be on assessing the validity of the arguments presented and other areas with higher risks.

5.8.14 In cases where the licensee can provide evidence that it is not reasonably practicable to meet the BSOs, the claimed safety measures should still be able to reduce the potential dose consequences to below the initiating frequency-banded Numerical Target 4 BSLs. ONR's policy is that a new facility or activity should at least meet the BSLs. There may be occasions on existing facilities where the BSLs are exceeded. This may be ultimately acceptable but the ONR inspector should press the licensee for a robust ALARP demonstration to show that there are no reasonably practicable measures to be taken to reduce risks further in both the short and long term.

5.8.15 The requirement for the licensee to reduce risks to ALARP applies regardless of whether the BSO or BSL have been met. At the design stage, this could involve optioneering different, additional, or alternatively-sized DBA safety measures (to the benefit of Numerical Target 4 comparisons). It could also include strengthening other levels of defence in depth that have no influence on the DBA but are to the benefit of safety.

Fault sequence analysis

5.8.16 The principle set out by SAP FA.7 is that analysis of design basis fault sequences should use appropriate tools and techniques, and be performed on a conservative basis to demonstrate that consequences are ALARP.

5.8.17 There will be occasions where meeting this expectation is a relatively trivial task, providing there is confidence in the safety measures to effectively and reliably deliver a simple safety function, for example situations where the closing of a valve or the actuation of an emergency brake will terminate a fault sequence with no consequences.

5.8.18 However, for complex facilities and activities, notably nuclear reactors, analysis of fault sequences with appropriate tools and techniques can be the most important and sizeable part of the licensee's DBA safety case, and correspondingly the main focus of ONR's regulatory attention. For reactor faults, extensive use of sophisticated reactor kinetics and thermal-hydraulic system codes is necessary to demonstrate that the correct performance of safety measures will result in the identified technical criteria being met. Where appropriate, radiological consequences analysis is required, using the results of the system codes as inputs to the radiological calculation (for example, the extent of any fuel damage, mass of steam / gas released, and the timing of releases).

5.8.19 For other facilities and activities, different analysis techniques may be necessary but the expectations and objectives as set out in SAP FA.7 remain the same. For example, some safety case claims may require finite element analysis to show that civil engineering or structural integrity technical criteria are met, or criticality analysis to show that configurations of fissile material remain sub-critical.

5.8.20 Appropriate conservatism for any analysis starts with the assumptions made in design basis fault sequences themselves. For example, in accordance with SAP FA.6, no claims on the correct performance of safety-related equipment should be made (unless this makes the transient more onerous), the limiting single failure should be assumed to have occurred, and the most onerous permitted maintenance states and starting conditions should be assumed. Other parameters that could be conservatively set within the analysis include, but are not limited to: times for equipment to respond or open, decay heat levels, and the location of operators when a fault occurs.

5.8.21 Operator actions to diagnose a fault and initiate any necessary actions should not be credited until a conservatively specified time has passed. 30 minutes for control room actions and 60 minutes for field actions are commonly assumed in DBA but these times should be adequately justified and validated in the safety case through proportionate task analysis. Shorter times for operator actions may be justifiable or longer timescales may be necessary.

5.8.22 The conservatism can also extend to the analytical tools and methods themselves. Historically, it was common to use simplified but conservative tools, especially when computing power was limited. Many of these 'legacy' methods will provide adequate substantiation for extant safety cases and provide the bases for design features and setpoints (subject to review in periodic safety reviews). However, it is increasingly relevant good practice to use computer codes which model the physical behaviour of facilities, activities and transients as realistically as possible, but with conservative initial and boundary conditions. Uncertainties in key parameters and correlations still need to be allowed for (individually or combined statistically), and appropriately substantiated in the safety case.

5.8.23 In a further development, some licensees and designers are exploring the use of 'best estimate plus uncertainty' approaches, where the uncertainties are quantified and sampled in multiple runs of best estimate / realistic computer codes, with the results expressed as percentiles or probability distributions of the calculated parameters. ONR inspectors should be open minded about these state-of-the-art methods which can offer operational benefits to the licensee whilst at the same time providing greater insights into the size of safety margins. However, the analytical, documentation, and resource requirements for these approaches are currently very high. This needs to be anticipated and planned for by both the licensee and ONR in regulatory engagements.

5.8.24 Specific guidance on what to expect from the different types of analyses that could be submitted to ONR and assessed against the expectations of SAP FA.7 is beyond the scope of this TAG. Further guidance for the assessment of some the methods and approaches can be found in:

- NS-TAST-GD-016: Integrity of Metal Components and Structures: (Ref. 25)
- NS-TAST-GD-020: Civil Engineering Containments for Reactor Plant (Ref. 26)
- NS-TAST-GD-021: Containment – Chemical Plants (Ref. 27)
- NS-TAST-GD-041: Criticality Safety (Ref. 10)
- NS-TAST-GD-045: Radiological Analysis for Fault Conditions (Ref. 15)
- NS-TAST-GD-075: Safety of Nuclear Fuel in Power Reactors (Ref. 11)
- ONR-CEEH-LTT-016: Modelling methods for the seismic analysis and design of safety-related nuclear structures (Ref. 30)
- IAEA Deterministic Safety Analysis for Nuclear Power Plants: SSG-2 (Rev 1) (Ref. 17).

5.8.25 Regardless of the technical discipline and type of analysis employed, any models and methods used to demonstrate that consequences of design basis fault sequences are ALARP need to be appropriately verified and validated. SAPs AV.1 to AV.8 set out ONR's expectations for demonstrating the validity of data and models, with further guidance provided in TAG NS-TAST-GD-042 (Ref. 13). The expectations set out in this guidance are likely to apply to the fullest extent to achieve the levels of confidence required for DBA. However, the extent to which the ONR inspector chooses to sample the licensee's documentation will depend on the circumstances. In cases where the safety case is dependent on a new methodology or the application of an existing computer code to a previously unconsidered situation, a detailed examination of the available verification and validation information may be necessary. However, there will be occasions where the licensee uses well-established methods previously considered by ONR (and maybe overseas regulators and international bodies). In these cases, it

may be proportionate to limit the assessment to gaining confidence that the code's use is within limits of applicability, the practitioners using the code are appropriately experienced, and the analysis is adequately documented.

5.8.26 In areas of high safety significance, novelty, uncertainty or lack of safety margin, it may be necessary for ONR to request the licensee to undertake additional confirmatory analysis with independent tools, methods, and engineering teams, even if the expectations of SAPs AV.1 to AV.8 have been followed for its 'frontline' tools. Alternatively, it may be appropriate for ONR to commission its own independent confirmatory analysis to reach a regulatory judgement on the adequacy of a licensee's DBA. In either case, it will rarely be necessary to repeat the totality of the DBA with independent methods; a targeted selection of initiating events, fault sequences and system responses is likely to be sufficient to reach a judgement on the safety case claims put forward.

5.8.27 In addition to conservative assumptions in both the fault sequences and the system response, DBA of fault sequences should demonstrate that a small change in a DBA parameter will not lead to a disproportionate increase in radiological consequences. Such a disproportionate impact is commonly referred to as a cliff-edge effect. There are several aspects to this regulatory expectation that can be pursued by the ONR inspector, depending on the circumstances.

5.8.28 The importance of the initiating event frequency and the severity of the initiating event (which has implications for the unmitigated consequences) for determining which deterministic rules apply (including whether or not the event qualifies for DBA in accordance with SAP FA. 5) has already been mentioned (see Section 5.6 and Appendix 3). A small change in a single assumption associated with these two factors should not result in either different safety case or different design outcomes. It is most likely that this will be an area for ONR attention for initiating events on the edges of the design basis region established by the Numerical Target 4 BSLs. However, if a relatively high initiating event frequency has been assumed ($> 1 \times 10^{-3}$ pa), and the initiating event has been made pessimistic (for example, a failed valve fully opens instantaneously or all SSCs in a compartment are lost to floodwater), it can be straight forward to conclude the assumptions associated with the initiating event are not a potential cliff edge requiring extensive regulatory attention.

5.8.29 The capability of safety measures is a candidate area for ONR to consider in an assessment. Whilst the analysis might have demonstrated acceptable results with a set of performance assumptions, if the plant or operator responded slightly slower, or if a pump delivered slightly less flow than specified, would the acceptance criteria (technical or radiological) still be met?

5.8.30 In those cases where sophisticated tools are used to analyse design basis fault sequences, modelling assumptions could be a source of cliff edges. Parameters such as time steps or spatial nodalisation could have a significant impact on the predicted results.

5.8.31 Good safety case submissions should explain and demonstrate that the DBA (and therefore the fault tolerance and safety of the facility) is not sensitive to cliff edge effects. Appropriate discussion on the conservatism in the analysis, the treatment of uncertainties, and additional sensitivity studies to supplement the main analysis should be expected. However, the ONR inspector is required to exercise judgement in considering the adequacy of a submission in this respect. It may be necessary to request further information and analysis to have confidence in the claims made but demands for excessive pessimism should be avoided as this is unlikely to provide additional insights into the safety performance of a facility. In other cases, it may be

disproportionate to require additional sensitivity calculations if they will not alter the regulatory decision for the design or activity in question.

5.9 Linking of Initiating Faults, Fault Sequences and Safety Measures (FA.8)

5.9.1 SAP FA.8 states that DBA should provide clear and auditable linking of faults, fault sequences and safety measures; this is sometimes referred to as a 'golden thread'. This is important for transforming a series of analytical tasks into a coherent safety case that supports the purpose for DBA set out in SAP FA.4, i.e. a robust demonstration of the fault tolerance of the engineering design and the effectiveness of safety measures.

5.9.2 Fault schedules are a powerful way to demonstrate the completeness of the list of design basis faults, what safety functions need to be delivered and what safety measures have been identified to deliver those safety functions. They can concisely provide a link or reference to any analysis that demonstrates the performance requirements and effectiveness of the SSCs and operator actions claimed, including for initiating events and fault sequences where analyses of more onerous or challenging sequences provides adequate confidence that they are within the capability of the design. They can also efficiently show that other DBA rules and safety case expectations have been met, for example, all operating modes have been considered, safety functions are appropriately categorised and safety measures appropriately classified, adequate defence in depth is provided for each safety function, what operator actions are required, and the minimum availability requirements for systems with inbuilt redundancy.

5.9.3 Some licensees may complement the 'fault-based view' provided by a fault schedule with a 'system-based' view through an engineering schedule. This can be used to summarise the design and functional requirements for SSCs and link them back to the source of those requirements, including, where appropriate, DBA. The overlap and balance between the two schedules is usually a matter of choice and convention for an individual licensee. The ONR inspector should look across both schedules, and the substantive safety case and analysis that the schedules are summarising, to form a view on the adequacy with which SAP FA.8 has been met.

5.9.4 Further guidance on ONR's expectations for a fault schedule is provided in Appendix 2.

5.9.5 Paragraph 641 which accompanies SAP FA.8 states that safety measures should be shown to be capable of bringing the facility to a stable, safe state following any design basis fault. This is rarely about running transient analysis modelling of fault sequences out for extended periods of time, long beyond the point at which margins to technical acceptance criteria are smallest. Instead it is usually about considering the mission times required of SSCs when defining their performance requirements. Factors that should be considered include:

- The need for ongoing electrical power supplies, restoration of grid connections, recharging of batteries, or requirements to shed electrical loads to extend availability.
- Capacity of diesel fuel tanks, and the requirement / ability to replenish fuel supplies from both on-site and off-site stocks etc.
- Ongoing requirements for cooling water and availability of suitable supplies / reservoirs.
- HVAC requirements to ensure the local environmental conditions support the extended operation of an SSC.
- Any operator actions to monitor and maintain the delivery of safety functions, the human resources required, and their ability to undertake any actions.

- Parallel demands from other facilities on the site for the same equipment, inventories or personnel to deliver their required safety functions following a common cause initiator (e.g. a seismic event) or failures consequential to the initiating event (e.g. a loss of grid connection following a reactor trip).

5.9.6 Recovery actions from accidents are usually beyond the scope of DBA. The stable, safe state achieved by DBA measures should be maintainable for long enough for alternative equipment or processes to be introduced to take over the provision of safety functions, and allow time for appropriate planning and approval for any necessary recovery actions.

5.10 Further use of DBA (FA.9)

5.10.1 Whilst DBA should have an important role to play in influencing and substantiating the design of a facility, it should also have a significant ongoing impact on the procurement, construction, commissioning, operation and maintenance of an operational facility, and how decommissioning activities are planned and safely undertaken.

5.10.2 SAP FA.9 states that DBA should provide an input to the safety classification and the engineering requirements for SSCs performing a safety function. Although DBA will not necessarily provide the basis for every engineering requirement for every SSC delivering a safety function, it will be a major consideration for the most significant safety measures claimed in the safety case. The corollary of this is that a lack of a claim on a SSC in a DBA safety case can also have a significant impact on the safety classification applied, and therefore its design, operational and EIMT requirements. Similarly, DBA should provide an input to the requirements for human actions claimed as administrative safety measures or those which support the delivery of safety functions via a human-machine interface with SSCs.

5.10.3 When assessing a safety case, the ONR inspector should consider whether the implications of a DBA claim in the safety case on the design or operation of a facility are clear, and be confident there is a mechanism for ensuring this clarity is retained throughout the design and operational life of the facility and individual SSCs. If the safety case submission under consideration is a modification to an existing facility, the impact on extant DBA claims should be addressed and it might be appropriate for the ONR inspector to review (through a targeted sample) the on-going validity of claims established many years before.

5.10.4 FA.9 also states that DBA should provide an input to the limits and conditions for safe operation applied to a facility or activity. These conditions and limits may be parametric (e.g. limits on pressure, temperature, level, chemical composition etc.) or conditional (e.g. prohibiting certain operational states, requiring specified equipment to be in service, setting minimum staffing levels etc.). They should provide the main basis for performance requirements and settings for safety systems (and some safety-related equipment), controls on permitted plant conditions and the availability of safety systems, and the safe operating envelope for the facility in normal operation. The environmental parameters which safety measures (whether that be SSCs or operator actions) will experience and be required to operate effectively within following a design basis fault should also be identified to inform procurement, manufacturing and procedural documentation.

5.10.5 The actual limits and conditions employed on a facility may differ from those assumed in the analysis. For operational reasons, setpoints and tolerances may be set tighter in practice than those conservatively modelled in the DBA. It is also important that limits and conditions are defined in terms that are meaningful to the operator, and permit straightforward compliance and, where necessary, facilitate an appropriate response.

This may require them to be expressed in terms different to those input directly into the analysis, but 'line-of-sight' between how the plant is operated and what has been assumed in the DBA needs to be maintained.

5.10.6 Further guidance on the assessment of limits and conditions, including the link to DBA is provided in TAG NS-TAST-GD-035 (Ref. 31). The requirement to produce an adequate safety case to identify conditions and limits necessary in the interest of safety is established by LC23. The supporting technical inspection guide NS-INSP-GD-023 (Ref. 32) provides additional advice to ONR inspectors for when assessing a licensee's arrangements to complement NS-TAST-GD-035.

5.10.7 DBA is often iterative. Assumptions made in DBA undertaken during the design phase of nuclear facility should be reflected in the functional requirements for safety measures and demonstrated during commissioning. However, there could be cases where the equipment eventually procured and installed does not match every early design assumption. In these circumstances, it will be necessary for the licensee to revisit its DBA to demonstrate that its original safety case claims, arguments and evidence remain valid with the delivered functional performance, or to modify its safety case and design accordingly. Similarly, it is not unusual for SSC performance to drift or degrade over its operational life, or for the ability of operators to fulfil a claimed human action to change with time. An appropriate EIMT regime is vital for ensuring performance, reliability and availability claims made in the DBA are being reflected in practice (see TIG NS-INSP-GD-028, Ref. 33).

5.10.8 In modern designs, claims on inherent safety, passive systems or automation can significantly reduce the number of claims on operator actions in DBA. This does not necessarily mean the requirement for operators has been eliminated. Consistent with the principle of defence in depth, there may be multiple means for an operator to intervene to minimise demands on automatic safety systems or as a backup to the automatic initiation of safety systems. Design work, drills, training and analyses need to be undertaken to ensure that any such actions are reliable and effective so far as is reasonably practicable. However, the extent to which ONR examines the licensee's substantiation, and potentially seeks improvements, should be determined cognisant of the safety case importance placed on individual actions.

5.10.9 The continuing validity of the safety case (of which the DBA is a major component) for the actual state of the facility is a fundamental part of a periodic safety review. ONR inspectors should look for evidence that a review of the DBA has been undertaken as part of this process. Any gaps revealed by the periodic safety review may result in a modification to plant to bring it back into line with the safety case, a revision to the DBA to reflect the state of the plant, or a combination of the two. Further guidance is provided in TAG NS-TAS-GD-050 (Ref. 34)

5.11 Deterministic Analysis outside of the Numerical Target 4 Design Basis Region

5.11.1 Paragraph 628 of the SAPs states that when initiating faults are excluded from the DBA, the safety case should still demonstrate that the resultant risks are as low as is reasonably practicable by applying other approaches such as relevant engineering good practice, PSA or other forms of deterministic analysis. IAEA GSR Part 4 (paragraphs 4.46 and 4.48 of Ref. 4) states that necessary layers of protection for achieving defence in depth have to be identified and adequate safety margin to be shown through safety assessment / analysis. These expectations for analysis to demonstrate fault tolerance are not limited to DBA and apply to faults and fault sequences excluded from DBA due to either limited radiological consequences or low frequencies.

5.11.2 By definition, the DBA SAPs FA.4 to FA.9 apply to faults that are within the design basis region (as established by SAP FA.5). However, if applied proportionally and in a graded manner, they can provide a framework for both the licensee to present its wider deterministic safety case (beyond the DBA), and for ONR to consider its adequacy. For example:

- Deterministic analysis can demonstrate the fault tolerance of a facility (by demonstrating additional defence in depth) and show the effectiveness of safety measures not claimed within the DBA, broadly consistent with FA.4.
- SAP FA.5 not only provides a clear definition of what is within the DBA, but equally defines which faults should be considered outside of it.
- Relevant fault sequences crediting SSCs not claimed within the DBA but which can be effective in alleviating the consequences of faults, should be identified as per FA.3 and in a similar way to FA.6. However, it is reasonable to expect the licensee to apply some clearly identified relaxations from the conservative assumptions set out in FA.6.
- Appropriate analysis of fault sequences outside of the design basis region should be undertaken to support claims of defence in depth and to show that the consequences are ALARP, similar to the expectation of FA.7. However, the level of conservatism can be relaxed relative to the expectations for DBA. It still should be an objective to demonstrate, so far as is reasonably practicable, that the correct operation of a defence in depth safety measure results in no breach of physical barriers, or that at least one barrier remains intact; that there is no release in radioactivity and no person receives a significant dose of radiation. If this cannot be achieved, it is important to note that it is likely to be inappropriate to compare the radiological consequences directly with Numerical Target 4 as this is specifically for DBA. Dutyholders may choose to set its own dose or risk targets for such sequences. ONR inspectors can use Numerical Targets 6 and 8 to compare such sequences against the BSLs / BSOs.
- Including faults / fault sequences outside of the design basis region, along with the safety measures which will be effective in alleviating their consequences, on a fault schedule in accordance with FA.8 is a powerful way for the licensee to demonstrate the completeness of its safety case and existence of defence in depth within the facility.
- It is important that all SSCs making a contribution to safety are appropriately classified, that the safety functions they are required to deliver are identified, and that the engineering requirements and setpoints for effective action are established through analysis, consistent with the expectations of FA.9. If the licensee has adopted a graded approach to categorisation and classification (consistent with Ref. 5) and limits and conditions (consistent with Ref. 31), this should not result in onerous design or operational constraints.

5.11.3 These principles can be applied in a graded manner to both faults with unmitigated consequences less onerous than the threshold for DBA (Numerical Target 4 BSL) and faults / fault sequences with large unmitigated consequence but are predicted to occur less frequently than the criteria set out in FA.5 and FA.6.

5.11.4 Both IAEA and WENRA have adopted the term ‘Design Extension Conditions’ (DEC) for onerous plant states outside the (traditional) design basis region which should be analysed (both probabilistically and deterministically). The IAEA Specific Safety Standard SSR-2/1 (Ref. 3) states:

> *A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant’s capabilities to withstand, without unacceptable radiological*

consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.[5]

5.11.5 WENRA's interpretation of this for new nuclear power plants is that this sets a clear expectation for the original design to address extreme events, multiple failures and the consequences of severe accidents (Position 1 in Ref. 19). For existing facilities, WENRA interprets the objectives of DECs to be to identify reasonably practicable provisions that can be implemented for the prevention of severe accidents [in addition to what was included in the original design] (Issue F of Ref.18).

5.11.6 Both international organisations make a distinction for nuclear power plants between DECs which occur without significant fuel degradation (DEC-A) and DECs progressing to core melt (DEC-B). The expectations for the analysis and assessment of design extension conditions with core melt are effectively the same as those well established in the SAPs (FA.15, 16 and 25) and the TAG, NS-TAST-GD-007 on SAA (Ref. 20), and are therefore not discussed further in this TAG.[6]

5.11.7 The IAEA Specific Safety Standard SSG-2 (Ref. 17) provides further guidance and examples to Ref. 3 on what plant states to consider as nuclear power plant DEC-As:

- Initiating events that could lead to situations beyond the capability of safety systems that are designed for design basis accidents.
- Frequent design basis accidents combined with multiple failures (e.g. CCFs in redundant trains) that prevent the safety systems from performing their intended function to control the postulated initiating event.
- Credible postulated initiating events involving multiple failures causing the loss of a safety system while this system is used to fulfil its function as part of normal operation.

5.11.8 Some licensees have been meeting many of the international expectations through long-established practices, such as:

- Applying a graded categorisation and classification scheme that is not restricted to DBA.
- Identifying diverse and independent means of delivering safety functions for frequent design basis faults.
- Regardless of the levels of redundancy and high levels of safety classification, considering CCFs within the DBA, consistent with SAP EDR.3.
- Capturing the claims above in fault schedules and demonstrating through analysis the effectiveness of diverse means of delivering safety functions.
- Performing additional sensitivities to demonstrate no cliff-edge effects in the DBA.
- Modelling fault sequences and the operation of SSCs not claimed in the DBA (and documenting the results) to support the facility's PSA.

---

[5] IAEA SSR4 on the Safety of Nuclear Fuel Cycle Facilities (Ref. 16) has a similar definition, with "nuclear power plant" changed to "nuclear fuel cycle facility".

[6] IAEA SSR4 on the Safety of Nuclear Fuel Cycle Facilities (Ref. 16) does not make a distinction between different types of DECs. It states that the main technical objective of DEC analysis for a facility with the potential for a large release or an early release of radioactive material shall be to provide assurance that the design of the facility is such as to prevent accident conditions not considered design basis accidents, or to mitigate their consequences, as far as is reasonably achievable.

- Undertaking suitable and sufficient severe accident analysis consistent with SAPs FA.1, 15, 16 and 25.
- Considering whether it is ALARP to provide additional measures even when deterministic and probabilistic rules and targets have been met.

5.11.9 Therefore, when assessing safety cases or periodic safety review submissions for existing facilities, the ONR inspector should be cognisant of the international expectation of DECs to be analysed to determine whether extant design features and arrangements are adequate, or whether additional improvements in both analysis and engineered provision are reasonably practicable. However, it may be possible to judge this from existing safety case approaches without a change in methodology or terminology.

5.11.10 The expectations for new designs with the potential for large or early releases are different, especially for new nuclear power plant designs. Plant states outside of the design basis region should be explicitly considered in the design and safety case in a structured and deliberate manner. Safety measures should be identified, appropriately classified, designed and qualified to specified standards, shown to be effective through analysis against appropriate technical and radiological acceptance criteria, and demonstrated to be independent from safety measures provided for other levels of defence in depth so far as is reasonably practicable. It is reasonable to expect deterministic claims and arguments to be clearly made for DECs (supported by appropriate analysis) that complement probabilistic evaluations of overall facility risk.

5.11.11 There are long-established expectations that transient analysis to support PSA and severe accident analysis / DEC-B should be best estimate (SAPs FA.13 and 15). International guidance for analysing DEC-A plant states is less definitive. SSR-2/1 (Ref. 3) states that it could be performed by means of a best estimate approach but more stringent approaches may be used according to States' requirements. SSG-2 (Ref. 17) states that the requirements on the selection, validation and use of computer codes specified for design basis accidents should apply in principle for analysis of DEC-A events. It also states that a best estimate code combined with conservative boundary conditions and assumptions (or best estimate plus uncertainty approaches) consistent with those used for DBA can be used. It concedes that best estimate analysis without quantification of uncertainties may also be used, if adequate margins to avoid cliff edge effects are demonstrated.

5.11.12 The licensee's methodology should set out its assumptions for starting conditions and system availability. It is reasonable to expect these to be relaxed relative to the DBA, notably the assumptions made about single failure tolerance. If a demand would only be placed on a DEC-A SSC after a CCF of single failure tolerant Class 1 SSC, it may be unreasonable to further penalise any assessed fault sequence by assuming an additional single failure (not associated with the initiating event, any consequential damage, or the reason for the Class 1 SSC failure). SSG-2 (Ref. 17) states that it may not be necessary for the unavailability of safety features due to maintenance to be considered. However, inspectors should look for a coherent strategy for the maintenance of SSCs, including those claimed for DEC-A, that takes into account deterministic and probabilistic considerations, design rules that follow from SSC classification, relevant good practice and the ALARP principle. If there are no availability controls on DEC-A systems (for example, setting limits on the time they are unavailable, or restricting maintenance in certain operating modes or when other levels of defence have reduced availability), claims of diversity and defence in depth could be undermined. It should be noted that the common GB practices of providing diversity for frequent faults and considering loss of essential services as part of the DBA sets precedents that maintenance unavailability should be considered for some DEC-A plant states.

5.11.13 A special type of beyond DBA is that of external hazards more severe but less frequent than the definition set out in SAPs EHA.4 and FA.5. The expectation to analyse such scenarios is set out in SAP EHA.18, with extensive further guidance provided in TAG NS-TAST-GD-013 (Ref. 6).

6. REFERENCES

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

2 IAEA 2018 Glossary: 2018 Edition
https://www.iaea.org/publications/11098/iaea-safety-glossary-2018-edition

3 IAEA Safety Standards – Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1, Revision 1
https://www-pub.iaea.org/MTCD/publications/PDF/Pub1715web-46541668.pdf

4 IAEA General Safety Requirements (GSR) Part 4 – Safety assessment for facilities and activities, Revision 1
https://www-pub.iaea.org/MTCD/publications/PDF/Pub1714web-7976998.pdf

5 NS-TAST-GD-094, Categorisation of Safety Functions and Classification of Structures, Systems and Components, Revision 1 July 2019
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-094.pdf

6 NS-TAST-GD-013, External Hazards, Revision 7 October 2018
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-013.pdf

7 NS-TAST-GD-014, Internal Hazards, Revision 3 April 2013
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-014.pdf

8 NS-TAST-GD-003, Safety Systems, Revision 8 March 2019
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-031.pdf

9 NS-TAST-GD-036, Redundancy, Diversity, Segregation and Layout of Mechanical Plant, Revision 4
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-036.pdf

10 NS-TAST-GD-041, Criticality Safety, Revision 6 June 2019
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-041.pdf

11 *NS-TAST-GD-075, Safety of Nuclear Fuel in Power Reactors, Revision 3 October 2020*
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-075.pdf

12 NS-TAST-GD-030, Probabilistic Safety Analysis, Revision 6, June 2019
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-030.pdf

13 TAG NS-TAST-GD-042, Validation of Computer Codes and Calculation Methods, Revision 4, March 2019
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-042.pdf

14 NS-TAST-GD-064, Allocation of Function Between Human and Engineered Systems, Revision 3, December 2017
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-064.pdf

15 NS-TAST-GD-045, Radiological Analysis for Fault Conditions, Revision 5, July 2019
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-045.pdf

16 IAEA Safety Standards – Safety of Nuclear Fuel Cycle Facilities, Specific Safety Requirements No. SSR-4
https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1791_web.pdf

17 IAEA Safety Standards – Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide SSG-2 Revision 1
https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1851_web.pdf

18 WENRA Safety Reference Levels for Existing Reactors (Update in relation to Lessons Learned from Fukushima Dai-Ichi Accident, September 2014)

http://www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf

19 *WENRA Safety of new NPP designs (Study by Reactor Harmonization Working Group RHWG March 2013)*
http://www.wenra.org/media/filer_public/2013/08/23/rhwg_safety_of_new_npp_designs.pdf

20 NS-TAST-GD-007, Severe Accident Analysis, Revision 4 September 2017
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-007.pdf

21 Review of Hazard Identification Techniques, HSL/2005/58, M. Glossop, A. Ioannides, J. Gould, [CM9 2008/97912]

22 NS-TAST-GD-063, Human Reliability Analysis, Revision 4 October 2018
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-063.pdf

23 US NRC: Chapter 15, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, NUREG 800
https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/

24 IAEA Safety Fundamentals – Fundamental Safety Principles, SF-1
https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1273_web.pdf

25 NS-TAST-GD-016, Integrity of Metal Structures, Systems and Components, Revision 5 March 2017
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-016.pdf

26 NS-TAST-GD-020: Civil Engineering Containments for Reactor Plant, Revision 4 December 2017
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-020.pdf

27 NS-TAST-GD-021: Containment – Chemical Plants, Revision 5 July 2019
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-021.pdf

28 NS-TAST-GD-005: Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), Revision 10, December 2019
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-005.pdf

29 Risk informed regulatory decision, June 2017
http://www.onr.org.uk/documents/2017/risk-informed-regulatory-decision-making.pdf

30 Modelling methods for the seismic analysis and design of safety-related nuclear structures, ONR-CEEH-LTT-016 Revision 1, CM9 2017/196808

31 NS-TAST-GD-035: Limits and Conditions for Nuclear Safety (Operating Rules), Revision 5 March 2018
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-035.pdf

32 NS-INSP-GD-023: LC23 Operating Rules, Revision 5 March 2019
http://www.onr.org.uk/operational/tech_insp_guides/ns-insp-gd-023.pdf

33 NS-INSP-GD-028: LC28 Examination, Inspection, Maintenance and Testing, Revision 6 September 2019
http://www.onr.org.uk/operational/tech_insp_guides/ns-insp-gd-028.pdf

34 NS-TAST-GD-050: Periodic Safety Reviews, Revision 7 July 2017
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-050.pdf

35 NS-TAST-GD-046: Computer Based Safety Systems, Revision 5 April 2019
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-046.pdf

36 NS-TAST-GD-060: Procedure Design and Administrative Controls, Revision 3 November 2017
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-060.pdf

37 WENRA Waste and Spent Fuel Storage Safety Reference Levels, Report of Working Group on Waste and Decommissioning (WGWD) Version 2.2, April 2014 http://www.wenra.org/media/filer_public/2014/05/08/wgwd_storage_report_final.pdf

38 WENRA Decommissioning Safety Reference Levels, Version 2.2, April 2015 http://www.wenra.org/media/filer_public/2015/10/14/wgwd_report_decommissioning_srls_v2_2.pdf

7. ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
AOO	Anticipated Operational Occurrences
BSL	Basic Safety Level
BSO	Basic Safety Objective
CCF	Common Cause Failure
C&I	Control and Instrumentation
DBA	Design Basis Analysis
DEC	Design Extension Condition
EIMT	Examination, Inspection, Maintenance and Testing
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
GDA	Generic Design Assessment
HAZOP	Hazard and Operability Study
HDL	Hardware Design Language
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
LC	Licence Condition
LWR	Light Water Reactor
OPEX	Operational Experience
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
SAA	Severe Accident Analysis
SAP(s)	Safety Assessment Principle(s)
SSC	Structure, System and Component
TAG(s)	Technical Assessment Guide(s)
US NRC	United States Nuclear Regulatory Commission
WENRA	Western European Nuclear Regulators' Association

8. APPENDICES

8.1 APPENDIX 1: FAULT IDENTIFICATION TECHNIQUES

8.1.1 Licensees can utilise a range of fault identification techniques in their safety cases, depending on the type of facility, its novelty, and where in the design or operational life cycle the analysis is being undertaken. Common techniques that are often cited include:

- **Hazard and Operability Study (HAZOP) –** This is a systematic approach used to evaluate processes or operations for hazards by application of guide words to identify deviations and subsequently evaluate problems that may represent risks to personnel or equipment. This approach employs a number of select individuals in a meeting type format. When inspectors are considering HAZOP type studies, they should ensure that the appropriate specialists were involved in the process with an adequate understanding of the plant. It is important that individuals familiar with the operation of the facility (or operation of similar facilities) are present at the meeting. It is also important to ensure that the appropriate breakdown of the facility was considered and the appropriate application of guide words was used. As HAZOP studies are undertaken by groups in a meeting type format they have limitations, such as it is difficult to demonstrate the comprehensiveness for highly complex systems or situations that involve complex mechanisms, in these cases a bottom-up technique might be more appropriate. However, with appropriate key words and the right people in attendance, they can be an effective way to identify failures arising from operational processes and maintenance operations.

- **Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA) –** This is a systematic ‘bottom-up’ approach that evaluates the impact of failures of all individual components and assesses the relative impact of different failures to build up a picture for sub-systems and whole systems. It is based on understanding, component-by-component the ways (failure modes) in which an item can fail and the effects (on the wider system) of this failure. It may also consider the potential causes of the failure (including human error), the nature of how fast failures may progress and whether or not the failure is revealed or unrevealed. This technique is used to understand the behaviour of complex systems where the failure modes of each component are well understood. Note, it may not be suitable to analyse components whose internal failures are complex, such as software-based systems or Hardware Design Language (HDL) configured systems. Additional advice on the assessment of software-based systems or HDL configured systems is described in NS-TAST-GD-046 (Ref. 35)

- **Plant Walk downs -** This is a technique whereby experienced plant operators and engineers will visually inspect the plant with an eye to identifying the possibility of hazards and the subsequent possibility of any faults that may arise from these hazards. Plant walk downs are often used to identify hazards on existing plants or to consider the effect or extent of a degraded plant condition.

- **Safety Function Breakdown (or Safety Function Decomposition) –** This is a ‘top down’ fault identification process based on consideration of the safety functions and the systems that deliver them. The technique first identifies the top level safety functions that need to be delivered by the design, these typically are: reactivity control, removal of heat; confinement of radioactive material and radiation shielding. These top level safety functions are then broken down, where the second level considers how the top level functions

could be challenged. These would be subdivided again to consider what could challenge each sub safety function. At each stage, the failure to maintain control of a safety function serves to identify potential fault sequences and the faults that can initiate them. In this regard, it is similar to the fault tree based master logic diagram. Analysing a design using this high-level, 'top-down' viewpoint is a powerful method of identifying initiating faults and any fundamental flaws in the basic design, as it should be apparent where the design is lacking in adequate measures to provide these safety functions.

- **Operational Experience (OPEX) -** The use of operational experience is an important means of fault identification. This may be OPEX from the plant itself, from the wider organisation, or OPEX from national and international bodies and facilities. Potential faults may also be identified by comparison with similar safety cases for other facilities with a similar function, or using similar plant items. Inspectors should ensure that licensees have taken due account of OPEX in their fault identification and they should ensure that OPEX has been sought from an appropriate range of sources.

- **Checklists –** Checklists are often employed in combination with HAZOP type studies to ensure that a comprehensive approach has been employed relating to a well understood group of hazards. Checklists are available which identify the key conventional, internal / external hazards and human failure modes. The checklist should be used to ensure that all generic hazards that apply to a given facility have been considered.

8.1.2 A more detailed introduction to some of the methods used to identify hazards is given in 'Review of Hazard Identification Techniques' (Ref. 21).

8.2 APPENDIX 2: FAULT SCHEDULE

8.2.1 It is long-established GB relevant good practice to capture the initiating design basis faults and the main safety case claims for those faults in a tabular summary commonly called a 'fault schedule'.

8.2.2 SAP ESS.11 (paragraph 407) sets out some high level expectations for what a fault schedule should contain:

> *"A fault schedule (sometimes known as a safety schedule or a fault and protection schedule) should be provided to link faults, fault sequences and safety measures (see Principle FA.8). For each initiating fault or event, the schedule should identify the relevant initiating fault frequencies, the potential fault consequences, the safety systems and administrative safety measures that provide protection, any beneficial safety-related systems, the mitigated fault sequence frequency and the overall protection claim. The fault schedule should also identify any passive safety measures claimed to prevent faults or mitigate their consequences."*

8.2.3 SAP FA.8 (paragraph 640) also states

> *"The analysis should demonstrate that:*
> *a) all design basis initiating faults are addressed;*
> *b) appropriate safety functions have been identified for the design;*
> *c) the performance requirements for the safety measures have been identified; and*
> *d) suitable and sufficient safety measures are provided.*
> *This demonstration should be summarised on a Fault Schedule."*

8.2.4 Beyond the wording of the specific SAPs, ONR does not prescribe the format or scope of the fault schedule. ONR inspectors should expect and / or encourage each licensee to adopt a format that works for its technology, safety case and its users. As a summary vehicle, the fault schedule cannot capture the totality of the DBA safety case but there are no constraints on what information can be included beyond what can be fitted into a landscape table whilst remaining legible and helpful. Through the use of bold / italicised / coloured fonts, or alpha-numeric coding, significant added value can be provided if the licensee so chooses.

8.2.5 By way of examples, the following lists some safety case information which could be included in addition to the basic requirements:

- Links to Failure Modes and Effect Analysis (FMEA), Hazard and Operability Study (HAZOP) or human error analysis detailing the identification of faults.
- Beyond design basis / DEC-A initiating events.
- Clarity of all faults bounded by the limiting event entries included on the fault schedule.
- The operating mode, plant configuration or plant state assumed for the initiating event.
- Links to references for initiating event frequency information.
- Safety functions and associated safety measures broken down to sub-function level (e.g. short term and long term cooling, systems to get to a controlled state and then to a safe shutdown state).
- The category of the safety function to be delivered, and the classification of the SSCs delivering the safety function.
- Minimum number of trains or divisions required to deliver the safety function.
- Number of trains or divisions available in a specific operating mode / plant state to deliver the safety function.

- Whether a safety measure is passive, automatic or manually initiated.
- The key parameters and control and instrumentation (C&I) platform, including systems and / or equipment, that initiates operation of a safety measure.
- The provision of defence in depth measures in addition to ‘front-line’ design basis measures.
- Essential support systems (e.g. containment functions, power, cooling water requirements, human resource etc.) required by the front-line safety measures.
- Links or references to where supporting narrative and transient analysis can be found in the main safety case submission.
- Links or references to where to find additional engineering details and substantiation in the safety case submission.

8.2.6 It is reasonable, indeed often desirable for there to be more than one fault schedule for a plant in recognition that some facilities or activities will require different safety functions to be delivered. For example, the fuel route faults or radioactive waste store faults will require different safety functions to be delivered to a reactor, and reactor operating modes may not be relevant.

8.2.7 Fault schedules can be complemented with engineering schedules (a system by system view of requirements including design codes, maintenance and inspection regime etc) and hazard schedules (a compartment by compartment view of the threats and provided protection for hazards). The ONR inspector should be flexible and look across all the schedules and underpinning safety case to form a view on the adequacy with which they together demonstrate the adequacy of the system design (ESS.11) and the linking between faults, fault sequences and safety measures (FA.8).

8.2.8 The fault schedule should be produced early on in the design and safety case development process, and continue to develop and be refined throughout the life of the facility. It needs to be kept up to date with the underpinning safety case and any modifications to the plant. Its ownership, status and validity are areas ONR inspectors could consider sampling during LC 14 and 23 inspections and LC 15 and 20 and 22 assessments.

8.3 APPENDIX 3: GUIDANCE ON INITIATING EVENT FREQUENCIES

8.3.1 DBA is predominately a deterministic approach concerned with demonstrating the effectiveness of safety measures to reduce the consequences of fault sequences to ALARP (consistent with SAP FA.7). Judgements against risk targets are largely matters for PSA. Despite this, frequencies, in particular, initiating event frequencies have an important role to play in DBA. This Appendix is intended to provide some additional guidance on what is included in the DBA SAPs (FA.4 to FA.9) and the main text of this TAG.

8.3.2 It should be noted that some licensees have 'DBA' schemes which are a hybrid of deterministic and probabilistic techniques, whilst others may provide submissions to ONR that combine probabilistic and deterministic arguments without clear demarcation between the different techniques followed to produce the holistic safety case. Neither of these situations is automatically unacceptable; the ONR inspector will need to use judgement on a case-by-case basis and may need look for guidance beyond this TAG.

8.3.3 It is also recognised that to demonstrate compliance with deterministic acceptance criteria with a high degree of confidence, some licensees and designers have developed sophisticated 'Monte Carlo' and 'response surface' statistical methodologies which apply probability / frequency distributions to operational parameters and potential plant responses (for example best estimate plus uncertainty models for PWR loss of coolant faults, or fission gas pressure limit compliance modelling on AGRs). Whilst these approaches are usually applied within the context of DBA, they are beyond the scope of this Appendix. Further guidance on the acceptability of these approaches is provided in Refs 13 and 17.

Role of Initiating Event Frequency in DBA

8.3.4 In the GB goal-setting regulatory approach, ONR does not prescribe which faults need to be analysed in DBA, what safety measures need to be provided and demonstrated to be effective, or what acceptance criteria need to be considered. However, the ONR inspector can use the initiating event frequency attributed to a fault for:

- Judging whether a licensee has appropriately identified that a fault should be assessed with conservative DBA techniques, by reference to SAP FA.5 and Numerical Target 4.
- Judging whether a licensee has appropriately designated a fault as 'frequent' or 'infrequent', resulting in different expectations for the number of independent and diverse safety measures to consider as relevant good practice.
- Determining whether appropriate technical and radiological acceptance criteria have been considered by the licensee to demonstrate that the safety measures effectively reduce consequences to ALARP; in a graded approach, the lower the initiating event frequency, the more relaxation that can be considered in the criteria relative to higher frequency events.

Conservatism in Initiating Event Frequency

8.3.5 Initiating event frequencies should be calculated on a best estimate basis. However, the ONR inspector should be able to determine from the licensee's safety case submission what faults, and variations of faults, are included within the best estimate frequency. The initiating event frequency should not just be an estimate of the likelihood of the limiting conditions assumed in the conservative modelling of the fault. In many cases it will need to include a frequency contribution for all the less severe manifestations of the fault (or similar faults) that the identified safety measures are claimed to be effective for. In other words, it should be the sum of all the frequencies

attributed to the different initiators of a particular fault, and not just the frequency of the most challenging version of the fault.

Taking credit for Safety Measures in Initiating Event Frequencies

8.3.6 The best estimate initiating event frequency attributed to a fault can take credit for features included in the design (for example redundancy, preventative safety measures, administrative controls or surveillance measures). Whilst paragraph 630 of the SAPs states that the correct performance of safety-related and non-safety equipment should not be assumed in the DBA demonstrating the effectiveness of identified safety measures (to reduce the consequences of a fault), that does not mean they cannot be assumed to work in the estimation of the initiating event frequency of the fault (assuming they are independent from the initiating event and protected against the consequential hazards resulting from the fault).

8.3.7 It is reasonable for a licensee to assert that a particular fault will be less likely to occur, and therefore less likely to place a demand on a DBA safety measure, if the plant has some additional preventative safety measures (compared to a similar, perhaps older plant without those features).

8.3.8 There will be limits on what can be claimed for the reliability of safety-related or non-safety equipment (and some operator responses), linked to the safety classification applied. Only modest reliability claims for SSCs with lower safety classifications should be made (see Section 5.7), and the presence of multiple low classification SSCs are unlikely to be an acceptable reason to avoid the requirements of DBA.

Assumptions associated with Pre-fault Operation

8.3.9 Operations on many plants will be within a defined safe operating envelope. Although in normal operation the plant may spend most of its time in a particular part of that envelope (and not at the extremes), part of the conservative approach of DBA is to assume that pre-fault operations are in the most limiting part of the envelope (to maximise the challenge on the safety measures), with no account taken for the frequency of operations in that part of the envelope. It is not unknown for DBA consequence analysis to assume the plant to be in physically impossible parts of the envelope to demonstrate the effectiveness of safety measures (e.g. limiting pressures and temperatures are assumed to occur together in a single transient, both of which are within the envelope but the plant could never have the two assumed parameters at the same time). This is acceptable but care needs to be taken not to confuse initiating event frequency with the likelihood of conservative assumptions (made to simplify the analysis) occurring in reality.

8.3.10 In cases where it is theoretically possible to drive the plant outside the safe operating envelope, but this is prevented by safety-related equipment or administrative controls (e.g. operating rules, technical specifications, surveillance requirements etc), it can be reasonable to assume the initiating event frequency for such a variation of the fault will be different from the same fault occurring from within the safe operating envelope. The reduction in initiating event frequency (and whether the resulting fault requires consideration in the DBA) will depend on the integrity / classification / reliability of the preventative measures.

8.3.11 Some licensees make an allowance for ‘conditioning factors’, claiming that an initiator will only have consequences if it occurs together with some other prevailing circumstances that have to be present. These could apply to the plant, external conditions, or location of workers etc. Making some probabilistic allowance for such factors can be acceptable but they are candidate areas for closer ONR scrutiny. If the lack of a claimed condition simply results in a less severe version of the fault in

question but with the same demands on safety measures, the approach adopted may not be consistent with ONR's expectations for DBA. However, if the absence of the condition results in no demand on candidate safety measures, there could be credible reasons for the licensee to exclude the scenario from the DBA. A reliance on luck or good fortune that certain conditions are not present at the time of fault, without any means for the licensee to check or control those conditions, is not a strong basis for reducing DBA expectations and should be challenged by the ONR inspector with reference to:

- SAP FA.6 paragraph 631 "Each design basis fault sequence should include as appropriate……..the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules"
- SAP NT.2 "There should be sufficient control of radiological hazards at all times".

Calculation, substantiation and traceability of Initiating Event Frequencies

8.3.12 Initiating event frequencies are a form of safety claim which need to be clearly identified in the safety case and appropriately substantiated.

8.3.13 The approach and techniques a licensee uses to calculate initiating event frequencies can be expected to vary, based on the design, complexity / novelty of the facility, and the stage of design or operation. Amongst the methods that could be cited are:

- Direct application of component failure and human reliability data (whether that be from the specific plant under consideration, data from similar applications, generic reliability data or engineering judgement),
- Fault tree analysis combining multiple sources of failure data together,
- OPEX,
- Design code expectations / limitations (for example ASME III for pipework or IEC 61508 for programmable electronic devices),
- Safety classification expectations / limitations,
- Precedent or relevant good practice as set out in earlier designs, IAEA guidance or overseas regulatory expectations,
- Expert elicitation,
- Engineering judgement.

8.3.14 The level of substantiation expected from the licensee and the extent to which the ONR inspector should sample the available evidence will also depend on the circumstances. For frequent faults ($<1 \times 10^{-3}$ pa) where a modest frequency claim has been made (for example 0.1 pa), it may be disproportionate for the ONR inspector to look for additional evidence beyond what is in the main submission as it will not alter the judgements of adequacy against deterministic criteria. Where the initiating frequency has significant implications for the design and safety case, greater regulatory attention will be merited, with a focus on cliff-edge sensitivities.

8.3.15 In all cases, the basis of an initiating event frequency should be traceable through the safety case from the top-level presentation (for example, in the fault schedule) through to its source.

8.3.16 The number of significant figures an initiating event frequency is reported to will rarely be directly significant to DBA, however an appropriate level of precision can be helpful for tracing the origins of a figure.

8.3.17 Where assumptions have been made in the calculation of initiating event frequencies, for example the number of times an operation is performed a year, these should be

clearly identified in the safety case so that they can be monitored and perhaps constrained during operation.

Interface with PSA

8.3.18 Where a detailed PSA exists, it is sensible for a licensee to utilise a common source of initiating event frequency data between it and the DBA. Exploring consistency between the PSA and DBA initiating events and associated frequencies can be an effective means for the ONR inspector to gain confidence in the substantiation and traceability of initiating event frequencies.

8.3.19 There are occasions when differences between the PSA and DBA are appropriate because of their different purposes:

- PSA models sometimes group faults differently, or break down initiators into more detail than DBA.
- Limits on reliability may be placed on SSCs in DBA because the design code states that better claims cannot be substantiated to a high degree of confidence. These constraints inform the deterministic rules that are applied such as whether DBA is required or the number of safety measures required. However, the PSA may use different methods to calculate a best estimate initiating event frequency. The resulting figure cannot be substantiated with DBA levels of confidence but it does ensure the insights the PSA gives on the overall balance of plant risk are informed by the actual design in question, as opposed to being biased by inherent conservatism in generic design codes.
- PSA models estimating the risk to the public from a facility need to consider the 'actual' frequency with which rare (but essential and planned) operating modes and activities take place (for example, refuelling operations or certain infrequent maintenance activities). The DBA for the same activity, which is focusing on showing that there is sufficient control of these rare activities, may assume an initiating event frequency that is an 'annualised' manifestation of the event frequency that exists whilst those activities are taking place. This is discussed more in Appendix 5.

Natural External Hazards

8.3.20 Natural external hazards (e.g. weather, flood and seismicity) can be described by a hazard curve of frequency of exceedance versus severity. The 'exceedance' in exceedance frequency means that at any given point of the hazard curve, the frequency of the indicated hazard severity should be interpreted as the frequency of realising an event of severity greater than the one indicated. If the DBA can demonstrate robustness against an external hazard of a particular exceedance frequency with a high degree of confidence, there can be even higher confidence that a less severe but more likely hazard can be tolerated.

8.3.21 Instead of trying to calculate the frequency of a hazard with a specific severity, the issue is usually tackled from the 'opposite direction'; an estimate of the severity of a natural hazard that will occur at a specific exceedance frequency is made. Further evaluations then need to be made for the plant response (e.g. building acceleration, flood heights etc), against which DBA can demonstrate the effectiveness of identified safety measures.

8.3.22 Given the lack of data available for very infrequent natural hazards, the established GB position is to set a limit on the natural hazards considered by DBA techniques at 1×10^{-4} pa but then determine the severity of the hazard and the resulting plant response on a conservative basis, rather than make a best estimate prediction of the severity of a 1×10^{-5} pa hazard.

8.3.23 Further guidance on the assessment of external hazards (including as part of DBA) is provided in NS-TAST-GD-013 (Ref. 6).

8.4 APPENDIX 4: SINGLE FAILURE CRITERION IN DBA

8.4.1 The single failure criterion is applied in two separate ways in safety cases:

- As a design attribute that is typically achieved through redundancy in the system architecture of high classification SSCs (in accordance with SAPs EDR.2 and EDR.4)
- As a conservative assumption made in DBA, in addition to the initiating fault and any consequential failures, included to demonstrate a high degree of confidence that acceptance criteria will be met (in accordance with SAP FA.6).

8.4.2 Both applications are important and should be considered by ONR, but it could be that different specialists take the lead on the two aspects (for example, a C&I inspector may look at the architecture of a protection platform, whilst a fault studies specialist looks at the transient analysis assuming a single failure in the protection platform). Guidance to inspectors on the properties of safety systems, including single failure tolerance is provided in NS-TAST-GD-003 (Ref. 8) and therefore is not repeated here. Instead, this Appendix is focused on the assumptions made in DBA. In practice, a design would develop iteratively with DBA demonstrating the effectiveness of deterministic design rules, and design rules for a facility being informed by the DBA.

8.4.3 The IAEA guide SSG-2 (Ref. 17) states that the following should be assumed in deterministic analysis of AOOs and design basis accidents:

> *In accordance with the single failure criterion, a single component failure should be assumed to occur in the operation of the safety groups required for the initiating event, in addition to the initiating failure and any consequential failures. Depending on the selected acceptance criterion, the single failure should be postulated in a system or component that leads to the greatest challenge to the safety systems.*

8.4.4 To support its DBA, unless the design in question is simple or there is an obvious limiting single failure, the licensee should be able to provide evidence of a systematic review of single component failures to identify those which have the potential to degrade or challenge the delivery of safety functions required following an initiating event. Good design in accordance with EDR.4 and Ref.8 has the potential to significantly minimise vulnerability to single failures. This should be recognised by the ONR inspector as part of a holistic review of the design and safety case. However it is rarely practicable to completely eliminate all single failures which have some impact on the successful delivery of safety functions, particularly those introduced by manufacturing, installation, or maintenance errors.

8.4.5 PSA can be a useful tool for the licensee to utilise to identify single failures for consideration in the DBA (as well as being a complementary means of demonstrating the insensitivity of the facility's design to single failures).

8.4.6 Both active single failures (for example, a valve fails to change state or a pump fails to start on demand) and passive failures (for example, a break or blockage in a pipe or failure of a non-return valve to operate correctly) should be considered for their potential to challenge the delivery of safety functions. Consistent with the deterministic nature of DBA, an identified single failure should be applied without any assumptions on the probability of it occurring. However, there may be occasions where the licensee can make arguments that it is grossly disproportionate to consider a particular single failure within the DBA because the sequence frequency will be beneath the 1×10^{-7} pa threshold established by SAP FA.6.

8.4.7 Qualitatively, reasoning that a single active failure during the initiating of a complex safety system is more likely than a random break in a pipe that had been in sound working order prior to a demand being placed on it and does not need to change state can have some merit. Before accepting such arguments, the ONR inspector should consider if passive failures are as unlikely as claimed or indeed random. For example, whilst a high quality length of pipe (with associated high quality welds) is unlikely to fail randomly when a demand is placed on it, if the condition of the pipe has become degraded over its operational life, experiences a thermal shock or water hammer when utilised, or could have been left isolated or blocked following construction or maintenance activities, then the chances of failure will be increased. Any claim that a particular single failure is not credible within the DBA therefore needs to be substantiated and perhaps supported by additional oversight during operations and maintenance. There may also be merit in the licensee analysing the fault sequence with a degraded safety measures as a DEC-A scenario to demonstrate some tolerance to the failure.

8.4.8 It is only necessary to consider one single (limiting) failure in a design basis fault sequence. However, it may be necessary for the licensee to analyse several variations of the same initiating event with different single failure assumptions to demonstrate that the design is tolerant to the most challenging fault sequence. It is important to consider if a change in operating state, power level or maintenance configuration could result in a different single failure being limiting.

8.4.9 To achieve its objectives of showing the fault tolerance of a design and the effectiveness of the various safety measures, it is not unusual for DBA results to be compared against several acceptance criteria, potentially with different calculations. Conservative DBA to demonstrate the effectiveness of a reactor trip system may need to include a different single failure to conservative DBA demonstrating the effectiveness of the containment structure. Similarly, DBA to determine the off-site radiological consequences to the public may need to consider a different limiting single failure to DBA undertaken to establish the dose to workers from the same fault. If it is not clear in a safety case submission, challenging the licensee on why it believes its chosen single failure is limiting for demonstrating the effectiveness of all safety functions and acceptance criteria can be a powerful way for the ONR inspector to gain confidence in the conservatism of the DBA.

8.4.10 In response to such a challenge, the licensee may point to multiple conservative assumptions in the DBA for a particular fault sequence to simultaneously show tolerance to multiple single failures whilst minimising the analytical burden. For example:

- With a 2 out of 4 voting system for reactor protection system, a trip signal is only generated when the 2nd and 3rd channels reach their setpoints
- The control rod with the highest worth is assumed not to insert
- Only a single train of post-trip cooling operates.

8.4.11 Such an approach is acceptable if justified and the results support the safety claims being put forward.

8.4.12 When demonstrating the effectiveness of safety measures that are diverse from the principal (typically Class 1) SSCs, whether that is for frequent design basis faults or for DEC events, it is not usually necessary to assume a single random failure in the SSCs under consideration. The expectation is that a demand will only be placed on a diverse safety measure following a failure of principal safety measure which should already have been designed to have been single failure tolerant. For the principal safety measure to have failed, multiple failures or a major CCF must have already occurred,

so it is not appropriate to further penalise the fault sequence with additional single random failures. This is consistent with the expectations set out in SAP EDR.4.

8.5 APPENDIX 5: TIME AT RISK ARGUMENTS AND PERMITTED MAINTENANCE STATES

8.5.1 SAP NT.2 states that there should be sufficient control of radiological hazards at all times. This includes all operating modes, maintenance activities, throughout the operating life of a facility (not just when it is new), and at end of life during decommissioning. Both deterministic and probabilistic analyses have roles to play to ensure there is adequate control for all periods of operation provided within the design and to support ongoing demonstrations through life.

8.5.2 From a deterministic perspective, SAP FA.6 states that design basis fault sequences should include:

- The worst normally permitted configuration of equipment outages for maintenance, test and repair; and
- The most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.

8.5.3 Therefore, facilities should include design provision for faults occurring in all planned operating modes and configurations, even if such a position would only exist for a short period of time or occur infrequently during the operational life of the facility. The effectiveness of this provision should be demonstrated through suitable DBA.

8.5.4 Most safety measures will require some maintenance, inspection or replacement during their lifetime. DBA can play an important role in demonstrating that these activities can be undertaken without a detriment to safety and establishing the best time to undertake these activities.

8.5.5 The IAEA guide SSG-2 (Ref. 17) states that deterministic analysis for design extension conditions does not need to consider unavailability of claimed safety systems (on the basis that they would be only be called upon following a failure of the independent Class 1 SSCs credited within DBA that are designed for planned maintenance). However, there will need to be some controls on the unavailability of these systems; if there are no constraints on their unavailability in the safety case, they are not a credible line of defence in depth. In addition, given that they will need to be maintained at some time, in the context of reducing risks ALARP, it will usually be appropriate to plan to undertake necessary maintenance cognisant of the operating state of the facility, the availability of other SSCs delivering the same safety function (notably the Class 1 DBA safety measures) and the time it will take to bring the SSC back into service.

8.5.6 Even with the best, most-forward looking design approaches and maintenance strategies, unplanned or urgent maintenance states at some point during the operational life of facility will be hard to avoid. Similarly, ageing effects and degradation of safety measures can be difficult to predict during the initial design phase, and short term periods of increased risk may be required to allow essential tasks to be undertaken to facilitate continued operation. It is not necessary for every conceivable (unplanned) scenario to be considered in the DBA. However, the requirements of SAP NT.2 still apply for the radiological hazards to be controlled and the ONR inspector should consider if adequate probabilistic arguments have been put forward by the licensee to demonstrate safety. Further guidance on dealing with time at risk situations is provided in the SAPs (associated SAP NT.2) and NS-TAST-GD-005 (Ref. 28).

8.5.7 The distinction between a planned maintenance state (which needs to be explicitly considered in the DBA) and an unplanned or urgent maintenance state (which does not require DBA consideration) should be established by the licensee and is a potential area for assessment by the ONR inspector. Typically, a planned maintenance state will

be permissible through operating rules for an extended period of time (perhaps weeks), whilst urgent states will normally be limited to a very narrow time window (hours or days) such that a period of operation at elevated risk does not have a significant impact on the annualised risk from the facility.

8.5.8 As with many finely balanced judgements, a combination of deterministic and probabilistic considerations is likely to be required to reach the optimal outcome:

- A deterministic view that operations should stop because of the degraded ability of safety systems to respond to a future random event may need to be risk informed by considering the potential of stopping operations to increase the likelihood of a demand on the unavailable system (as opposed to continuing in the same operating state whilst the system is returned to service).
- Probabilistic arguments that the annualised risk from an operational state is small need to be complemented by a deterministic consideration of whether potential faults are in fact independent from the state. For example, raising a reactor to power, a batch operation, or a filter change may only be done relatively infrequently, but it is only during those activities that certain faults would occur and place demands on safety systems.
- Arguments that it is grossly disproportionate to provide the full expectations of DBA for a random initiating event occurring in an operating or maintenance state that lasts for a very short period during the life time of the facility may be acceptable if supported by appropriate probabilistic arguments. However, it may be practicable to provide effective safety measures that are not substantiated to the extent expected for DBA, and robust administrative controls should be put in place to minimise the frequency of entering such conditions and thereby reduce the period of higher risk to ALARP.

8.6 APPENDIX 6: WENRA SAFETY REFERENCE LEVELS AND SAFETY OBJECTIVES RELEVANT TO THIS TAG

Note, this TAG is not necessarily the only place the identified Safety Reference Levels and Safety Objectives are reflected in ONR guidance.

WENRA Safety Reference Levels for Existing Reactors (Ref. 18)

Reference Level	Description	Relevant SAP(s)	Coverage in this TAG
Issue E: Design Basis Envelope for Existing Reactors			
E1	Objective [*of design basis]*	FA.4, FA.7	Sections 5.5 & 5.8
E2	Safety Strategy *[defence-in-depth*]	EKP.3, FA.7	Sections 4 & 5.8
E3	Safety functions	ECS.1,	Sections 4 & 5.7
E4	Establishment of the design basis	FA.2 & FA.5	Sections 5.3 & 5.6
E5	Set of design basis events	FA.2 & FA.5	Sections 5.3 & 5.6
E6	Combination of events	FA.6	Sections 5.7 & 5.11
E7	Definition and application of technical acceptance criteria	FA.6 & FA.7	Section 5.7 “Grouping of Fault Sequences for Analysis” Section 5.8 “Acceptance Criteria”
E8	Demonstration of reasonable conservatism and safety margins	FA.6 & FA.7	Section 5.7 “Design Expectations for DBA Safety Measures” Section 5.8 “Fault Sequence Analysis” Appendices 3 & 4
E9	Design of safety functions *Note, this TAG is technology neutral and therefore does not provide design guidance specifically for nuclear power plants*	Multiple engineering SAPs FA.6	Section 5.7 “Design Expectations for DBA Safety Measures”
E11	Review of the design basis	SC.7	Sections 3, 5.3, 5.8 & 5.10
Issue F: Design Extension of Existing Reactors			
F1	Objective	FA.1	Sections 4 & 5.11
F2	Selection of design extension conditions	FA.1, FA.2, FA.3 & FA.15	Sections 4 & 5.11
F3	Safety analysis of design extension conditions	FA.1 & FA.15	Sections 4 & 5.11
F4	Ensuring safety functions in design extension conditions *Note, this TAG is technology neutral and therefore does not provide design guidance*	ECS.1 & FA.16	Sections 4 & 5.11

	specifically for nuclear power plants		
F5	Review of the design extension conditions	SC.7	Sections 3, 5.3, 5.8 & 5.10
Issue G: Safety Classification of Structures, Systems and Components			
G1	Objective	ECS.2	Sections 5.7 “Design Expectations for DBA Safety Measures” and 5.9
G2	Classification Process	ECS.2, FA.8, FA.9	Sections 5.7 “Design Expectations for DBA Safety Measures”, 5.9 & 5.10
G3	Ensuring Reliability	ECS.2, FA.8, FA.9	Sections 5.7 “Design Expectations for DBA Safety Measures” and 5.9
Issue H: Operational Limits and Conditions			
H1	Purpose	FA.9	Sections 3 & 5.10
H2	Establishment and Review of OLCs	FA.9	Section 5.10
H4	Scope of OLCs	FA.6	Section 5.3
H5	Safety limits, safety system settings and operational limits	FA.9	Section 5.10
H6	Unavailability Limits	FA.6 & FA.9	Appendices 3 & 5

WENRA Safety Objectives for New Nuclear Power Plants (Ref. 19)

Safety Objectives	Description	Relevant SAP(s)	Coverage in this TAG
O1	Normal operation, abnormal events and prevention of accidents	FA.4	Section 5.5
O2	Accidents without core melt	FA.7	Sections 5.8 & 5.11
O4	Independence between all levels of defence in depth	EKP.3	Sections 4 & 5.7

WENRA Waste and Spent Fuel Storage Safety Reference Levels (Ref. 37)

Reference Level	Description	Relevant SAP(s)	Coverage in this TAG
Safety Area: Design			

S-19	The storage facility shall be designed to fulfil the fundamental applicable safety functions during normal operation, anticipated operational occurrences and design basis accident conditions	ECS.1, FA.8	Sections 4, 5.7 & 5.9
S-23	The radioactive waste and spent fuel storage facility shall be designed on the basis of assumed conditions for its normal operations and assumed incidents or accidents.	FA.4	Section 5.5
S-24	The licensee shall identify and classify structures, systems and components important to safety applying a graded approach.	ECS.2, FA.8, FA.9	Sections 5.7 “Design Expectations for DBA Safety Measures”, 5.9 & 5.10
S-26	The licensee shall establish operational limits and conditions (OLCs) in order to maintain the storage facility and waste and spent fuel packages or unpackaged spent fuel elements in a safe state during facility operation.	FA.9	Section 5.10
S-28	The design of the facility shall take into account all relevant postulated initiating events (PIEs), depending on the storage characteristics.	FA.2, FA.5	Sections 5.3 & 5.6

WENRA Decommissioning Safety Reference Levels (Ref. 38)

Reference Level	Description	Relevant SAP	Coverage in this TAG
Safety Area: Safety Verification			
DE-50	The licensee shall provide a safety case, which addresses all issues relevant for safety during decommissioning. *Note links to Appendix A on Example for a safety case for decommissioning & Appendix B on Postulated initiating events*	FA.2, FA.5, FA.7	Sections 5.3, 5.6, 5.8 & 5.11