

LIMITS AND CONDITIONS FOR NUCLEAR SAFETY (OPERATING RULES)

T/AST/035 - Issue 3

Issue Date:

23-08-2011

Review Date:

23-08-2014

Open Government Status:

Fully Open

Approved by :

A N Hall

- 1. [Purpose and scope](#)
- 2. [Relationship to the licence and other relevant legislation](#)
- 3. [Relationship to SAPs, WENRA safety reference levels and IAEA safety standards](#)
- 4. [Advice to assessors](#)
 - [Terminology](#)
 - [Operating Rule Tier Hierarchy](#)
 - [Operating Rules and Defence in Depth](#)
 - [Types of Operating Rules](#)
 - [Derivation of Operating Rules](#)
 - [Criticality Limits and Conditions](#)
 - [Examples of Typical Operating Rules](#)
- [References](#)
- [Annex 1 – Tests for an Operating Rule](#)
- [Annex 2 – Common LC23 Misconceptions](#)
- [Annex3 – Examples of Operating Rules](#)

1. Purpose and scope

1.1 This guide provides advice to inspectors on operational safety limits and conditions implemented at nuclear facilities and their relationship with the underlying safety case. It is intended for use during ONR's assessment of safety cases to assist when judging the adequacy of safety case implementation and for LC23-related compliance inspections. It also provides guidance to aid regulatory decision making in the nuclear permitting process when assessment includes consideration of whether limits and conditions applied at, or proposed for nuclear facilities have been adequately underpinned in the safety case.

1.2 Licensees use a range of terminology for the limits and conditions necessary for nuclear safety, e.g. Operating Rules, Technical Specifications,

Key Safety Management Requirements, etc. This guide is concerned principally with the methodologies used by licensees to derive such limits and conditions, and so has been written as a reference document to provide a detailed theoretical overview of appropriate approaches. In view of the level of detail in this guide, a short Overview section has been provided summarising the key content, together with an Annex listing key aspects and providing cross-references to the detailed advice in the main text. *Familiarity with the content of the Overview and Annex 1 will be sufficient for the needs of most inspectors.* In addition, further specific guidance on the implementation of safety case limits and conditions is provided in [1], which complements this guide. Both guides have been provided to advise and inform ONR inspectors in the exercise of their regulatory judgment.

Overview

1.3 LC23(1) requires the “adequate safety case” that licensees must produce “in respect of any operation that may affect safety” should “identify the conditions and limits necessary in the interests of safety”. LC23(1) calls such conditions and limits “operating rules”. LC23(3) further requires licensees to ensure that their operations “are at all times controlled and carried out in compliance with [these] operating rules”. This updated and expanded Technical Assessment Guide and its accompanying Technical Inspection Guide [1] have been produced in tandem following extensive surveys of guidance and practice on the derivation and application of limits and conditions at nuclear facilities both across UK licensees and internationally. The advice herein draws extensively from, and is consistent with, ONR’s SAPs [2], IAEA Safety Guide NS-G-2.2 [4], other relevant IAEA guidance (e.g. [13] to [15]) and the WENRA Safety Reference Levels [3].

1.4 A fundamental aspect of this guidance is that operating rules (abbreviated hereinafter as ORs) are by definition *conditions and limits* identified by the licensee in its *safety case*. The requirement in LC23(3), to ensure operations are “at all times” compliant with these ORs, therefore places duties on the licensee to link the theoretical analysis documented in its safety case with actual operational limits and conditions in force at the facility and through these, to operate in accordance with its safety case. These duties apply to any condition or limit appearing (explicitly or implicitly) in the licensee’s safety case, not just to the subset of limits and conditions that the licensee may choose to designate as “Operating Rules” (or whatever the licensee chooses to call its highest level limits and conditions). In other words, what is (or is not) an OR is defined by LC23, rather than by the terminology that the licensee employs. The definition of OR used here is therefore wider than the concept used historically by some UK licensees in that ORs are not only the limits of the normal safe operating envelope for the facility, but should also include any other limit or condition needed for safety.

1.5 That said, although any limit or condition identified in the licensee’s safety case is an OR for the purposes of LC23, it needs to be stressed that ONR expects both inspectors and duty holders to focus (target) their attention on those ORs that have the greatest bearing on safety. This guide thus sets out a hierarchy of ORs and suggests explicit criteria for ONR to judge which ORs should be regarded as most important. These criteria draw from SAPs Target 4 (Design Basis Fault Sequences). They have thus been set in terms of the unmitigated consequences and initiating event frequencies of individual fault sequences, though other aspects of the fault analysis (e.g. Probabilistic Safety Assessment, PSA) will also be important. In general, inspectors should target their attention predominantly on

ORs relating to faults falling broadly within Tiers 2 or 3 of Figures 1a and 1b (below), subject to the more detailed guidance on the hierarchy in paras 4.2 to 4.7 of this guide. The guide refers to such ORs as *High Hazard Operating Rules (HHORs)*, and those in Tier 1 as *Low Hazard Operating Rules (LHORs)*. As part of this hierarchy, ONR will not normally Approve ORs under LC23(4) unless the OR falls broadly within Tier 3 and will not normally expect the LC7 reporting arrangements deriving from LC23(3) to include an OR unless it resides broadly within Tiers 2 or 3 (i.e. it is an HHOR).

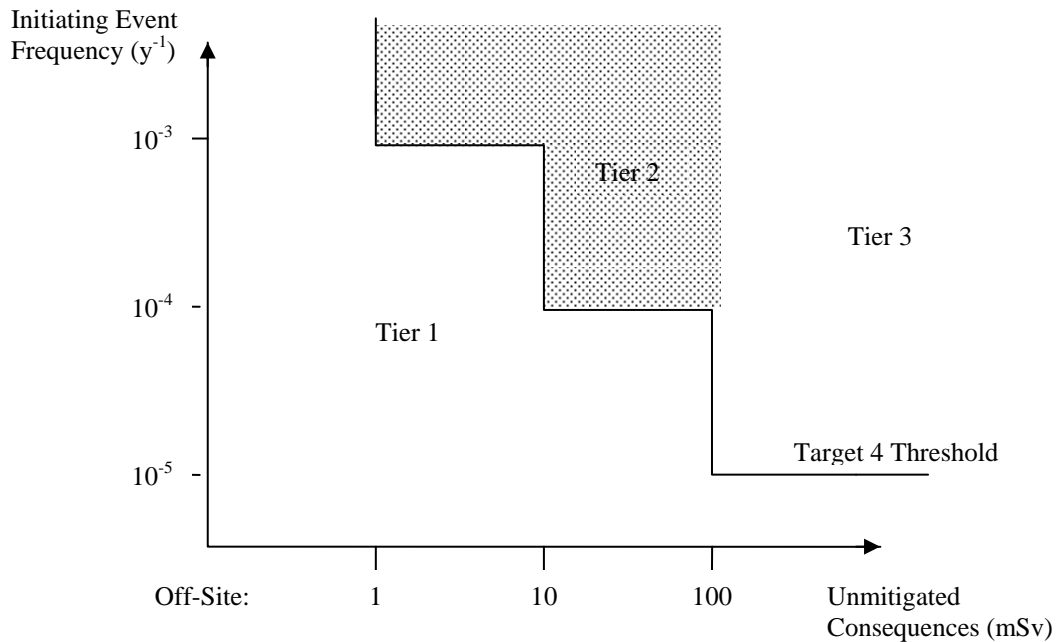


Figure 1a: Operating Rule Tiers for Off-Site Faults

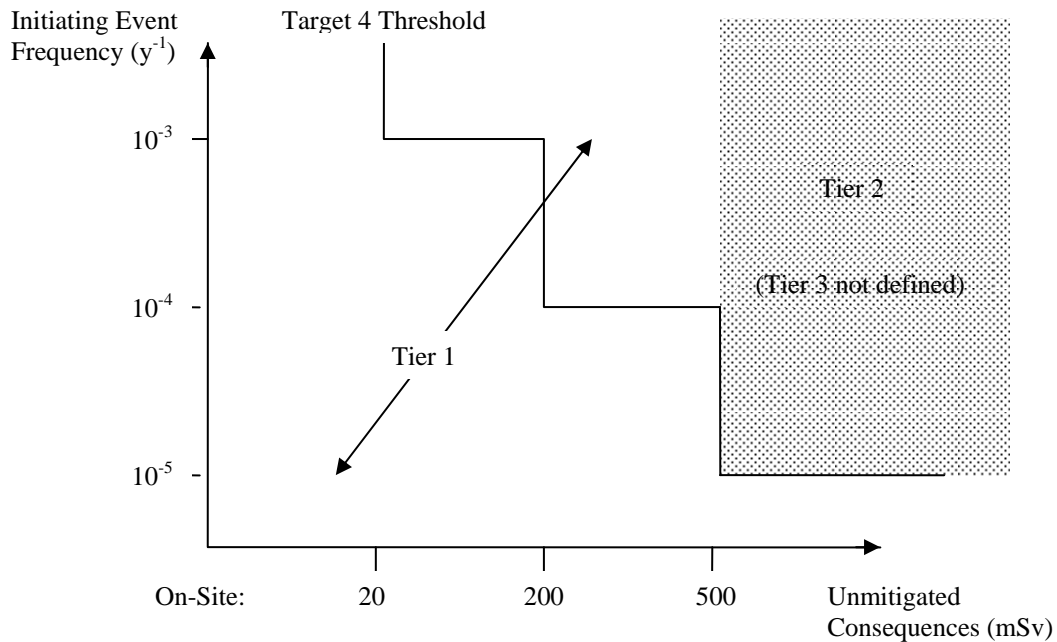


Figure 1b: Operating Rule Tiers for On-Site Faults

1.6 Similarly, it is ONR's expectation that licensees will adopt some form of OR hierarchy to assist with the targeting of their attention on limits and conditions that have the greatest bearing on safety. The technical details of such hierarchies must necessarily be a matter for individual licensees to decide upon as they should depend, for example, on the individual approaches to Design Basis Analysis (DBA) (see paras 4.2 and 4.3).

1.7 ORs link the theoretical safety case analysis with actual operational limits and conditions in force at the facility. It is imperative therefore that the ORs are written to be used by the operators who will need to apply them (and not for example, for the fault analysts, design engineers or even the regulators). To achieve this, the ORs should be set in terms that are meaningful to the operators. Additionally, they should permit a straightforward demonstration of compliance (e.g. avoid, where possible, complicated off-line calculations) and keep the number and nature of compliance checks to manageable levels (e.g. by combining similar limits and conditions into a single OR, or adopting a bounding approach where practicable). Qualitative guidance on how to derive appropriate ORs is provided in para 4.33.

1.8 In addition to these aspects, the wording used for LC23 leads to a number of high-level principles governing the scope and nature of ORs:

- ORs must be *conditions* or *limits* (and not for example, instructions) that may be readily checked by the operators to ensure the facility is being operated in accordance with its safety case. *This is a more powerful form of safety management than an instruction-based approach, as it leads to precise definitions of what is (or is not) verifiably safe, rather than trying to prohibit all the means through which an unsafe state might potentially arise.* (The implementation of ORs should nevertheless be covered by operating instructions as required by LC24(2));
- The requirement for compliance *at all times* implies the need for ORs to be identified for all permitted operating modes (e.g. start-up, shutdown as

well as in normal operation); for the OR to be set taking into account how quickly a non-compliant state could theoretically develop; and for any temporary ORs to be regarded as equally important as permanent ORs;

- The licensee's duties apply to *any operation that may affect safety* and so the ORs' coverage, like that of the safety case, needs to be complete, i.e. address all important aspects of the facility's operation.

1.9 Expanding on this last bullet, SAPs Key Engineering Principle EKP.3 seeks a defence in depth approach to safety leading to the provision of several (as far as possible independent) layers of protection against potentially significant faults or failures. This analysis should normally result in the identification of ORs for each of the Levels of the Defence in Depth hierarchy described in para 143 of SAPs, as illustrated in Figure 2 (but dependent on the type of fault under consideration, e.g. there may be no practical Level 4 response for some fast-acting faults).

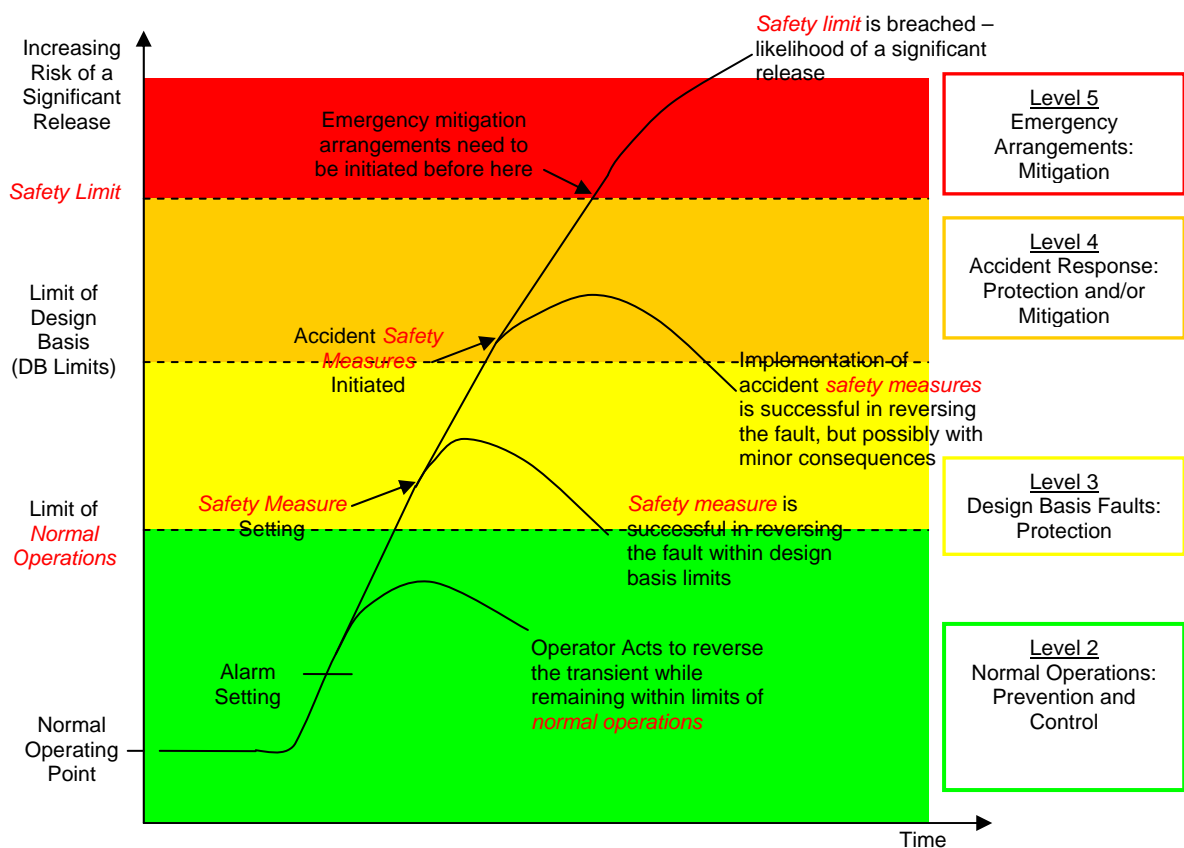


Figure 2: Schematic Illustration of Defence in Depth Approach to Operating Rules

1.10 Following this approach, the ORs should identify the boundaries between the SAPs' Defence in Depth Levels 2 to 5 in order to trigger the relevant fault / accident management arrangements at each stage of a fault's progression. They should also identify any further limits or conditions (e.g. identifying the plant and equipment that needs to be kept available and specifying any associated set points) necessary to put these management arrangements into effect. Here it is stressed that where the hazard is high, inspectors should expect to see ORs at all these Defence in Depth Levels, and not just for the one / few that the licensee considers the most important. However, since not all these layers of protection will be equally important, the licensee should seek to grade its ORs to assist focussing attention

on key safety matters. Further guidance on this aspect is provided at paras 4.8ff. Usually, the licensee's safety analysis should identify the most important ORs to be:

- (i) those defining / supporting the limit of normal operations (as these are the first barrier to fault progression);
- (ii) those associated with the safety measures needed to protect against design basis faults and
- (iii) those covering the availability of emergency equipment needed within short timescales to respond to an accident (e.g. tertiary hold-down systems on certain nuclear power plants).

1.11 Following the above approach should lead to the licensee identifying several types of ORs from its safety case. These would normally include, but not necessarily be limited to:

- Parametric limits and conditions to trigger an operator response in the event of a pre-defined condition or circumstance being reached;
- Operational limits and conditions defining minimum levels and permitted configurations of plant, equipment and associated supplies needed to enact safety measures;
- Set point limits and conditions to define where safety measures are intended to be activated or initiated in order to protect against or mitigate fault consequences;

Para 4.24 provides a more complete list of the types of ORs that a licensee might derive.

1.12 The licensee's process for deriving ORs should recognise that ORs are only part of what is required to keep risks as low as reasonably practicable (ALARP). In particular, complying with ORs will not necessarily imply that the facility's risks are duly ALARP, just acceptably low. This is because ORs are conditions and limits necessary in the interests of safety, defining compliant operation (e.g. a safe operating envelope) within which risk levels have been shown to be acceptable, rather than the optimal point residing within that envelope. The safety case should therefore not only seek to determine a suitable and sufficient set of ORs for the purposes of ensuring compliance, but should also determine how operations will minimise risks. For example, the ORs should define the minimum levels of plant and equipment needed for safety, whereas the safety case should also determine what further plant and equipment it is reasonably practicable to provide / have available. Similarly, the ORs will define limits for safe operation, which should be set some margin away from the normal (ALARP) operating point, so that contravening the OR would necessitate a significant loss of control.

1.13 Further details expanding on all the above aspects are provided in the main body of this document. Complementary guidance on implementation aspects is also provided in the TIG [1]. In addition, a summary of the key principles employed here (with cross-references to the main body of the guide) is set out in Annex 1, guidance on common LC23 misconceptions is provided in Annex 2 and a set of illustrative examples is provided in Annex 3.

2. Relationship to the licence and other relevant legislation

2.1. The following Licence Conditions are of direct relevance to this guide:

Licence Condition 23: OPERATING RULES

(1) 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.

(2) The licensee, where the Executive so specifies, shall refer the operating rules arising from paragraph (1) of this condition to the relevant nuclear safety committee for consideration.

(3) The licensee shall ensure that operations are at all times controlled and carried out in compliance with such operating rules. Where the person appointed by the Licensee for the purposes of condition 26 identifies any matter indicating that the safety of any operation or the safe condition of any plant may be affected that person shall bring that matter to the attention of the licensee forthwith who shall take appropriate action and ensure the matter is then notified, recorded, investigated and reported in accordance with arrangements made under condition 7.

(4) The licensee shall submit to the Executive for approval such of the aforesaid operating rules as the Executive may specify.

(5) The licensee shall ensure that once approved no alteration or amendment is made to any approved operating rule unless the Executive has approved such alteration or amendment.

(6) Notwithstanding the preceding provisions of this condition the Executive may, in its opinion circumstances render it necessary at any time, agree to the temporary suspension of any approved operating rule.

Licence Condition 24: OPERATING INSTRUCTIONS

(1) 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.

(2) 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) The licensee shall, if so specified by the Executive, furnish to the Executive copies of such operating instructions and when any alteration is made to the operating instructions furnished to the Executive, the licensee shall ensure that such alteration is furnished to the Executive within such time as may be specified.

(4) The licensee shall make and implement adequate arrangements for the preparation, review and amendment of such operating instructions.

(5) The licensee shall submit to the Executive for approval such part or parts of the aforesaid arrangements as the Executive may specify.

(6) The licensee shall ensure that once approved no alteration or amendment is made to the approved arrangements unless the Executive has approved such alteration or amendment.

2.2 LC23(1) requires the licensee to produce an adequate safety case to demonstrate the safe operation of the facility. One purpose of the safety case is to identify all of the limits and conditions necessary so that the plant is kept within constraints that ensure the safety of the facility during normal operation, fault and accident conditions. These constraints 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).

2.3 LC23(3) requires the operator to ensure that operations at the facility comply with these constraints at all times. Compliance aspects are addressed in greater detail in T/INS/023 [1]. For the purposes of this guide, inspectors should note that the intent of LC23 is to link the theoretical analysis documented in the safety case with actual operational limits and conditions in force at the facility [H1.1]. The limits and conditions derived in the safety case therefore need to be couched in terms that will be usable and relevant to the operators (e.g. measurable, verifiable), and

set so that the operators can be sure that having complied with these limits and conditions, they will also be compliant with the safety case.

2.4 LC23(3) additionally requires the licensee to take appropriate action in the event of exceeding these limits and conditions and also to investigate (etc) such incidents. This implies that licensees' safety cases should include detailed planning and analysis to cater for foreseeable incidents and utilise learning from experience to prevent repeat events [H10.2]. Guidance on learning from experience is addressed in detail in [17].

2.5 LC24(2) requires licensees to implement instructions to ensure that the limits and conditions identified under LC23(1) are complied with. Here inspectors should note the distinction made between limits and conditions, which are constraints on how the facility must be operated, and instructions, which relate to how operators should carry out safety-related activities. A key implication of this distinction is that the conditions and limits derived under LC23(1) need to be set in terms of verifiable operational states rather than in procedural terms. For example, a limit on the maximum number of cans allowed in a Pu glovebox would be appropriate for the purposes of LC23(1), but a rule prohibiting operators from adding more than a certain number of cans would not (as this is an instruction to people rather than a limit/condition for the plant). The reasoning for such distinctions is that the operator needs to ensure the facility is in a safe state, compliant with the safety case, irrespective of how any unsafe state might have arisen. Defining the safe state in terms of operational instructions places a focus on the operators rather than on the facility. This is not to say that licensees should avoid providing instructions in the interests of safety, particularly when the possibility of reaching an unsafe state through operator action has been identified; only that the limits and conditions identified in the safety case should preferably relate to the facility/plant/equipment and not to its operators.

2.6 The points made in the above paras will be expanded upon in later sections of this guide.

2.7 In addition LC27 (Safety Mechanisms, Devices and Circuits) is of indirect relevance, as it places an explicit duty on the licensee to operate (etc) its facility in accordance with limits and conditions relating to the design and number (suitability and sufficiency), availability (connectedness) and condition (working order) of the safety equipment. These limits and conditions are necessary in the interests of safety and so need to be derived in the safety case. There is thus an overlap in the duties deriving from LC27 and LC23. The implications of this overlap for implementation are set out in the companion TIG [1].

2.8 No other legislation has been identified as directly relevant to the present guidance. However, ORs will be of indirect relevance to several other LCs (e.g. LC7 and LC26 through their mention in LC23(3) and LC14 as this will govern the procedures for their derivation). Duties deriving from LC23 also overlap with other legislation (e.g. HSWA (specifically ALARP requirements), MHSWR Regulations 3 and 5, REPPIR (whose duties in this regard may be met through compliance with LC23 [18]), IRRs etc).

3. Relationship to SAPs, WENRA reference levels and IAEA safety standards

SAPs

3.1 The principal SAPs [2] with direct relevance to this guide are SC.6 plus supporting paras 96 and 97b; SC.8 and para 101 EKP.3 plus paras 140 to 143 and Table 1; EMC.21; EMC.24; ESS.1; ESS.4 and para 339; ESS.13; ESS.24; EHF.4; ECR.2 and para 474; and FA.9 plus para 526. In addition, other SAPs (e.g. para 186, EHA.5, EPS.4, para 252i, para 273, EGR.3, EGR.12, para 424b, para 439, ERC.3, para 447-8, 451, ERC.4, EHT.2, para 464b, para 465, para 498, para 667) make reference to safety limits and conditions, but these are of secondary or duplicated relevance in the context of this assessment guide and so have not been referenced in it.

3.2 In brief, guidance in the SAPs pertinent to this guide is broadly as follows: SAP SC.6ff seeks safety cases that identify operating conditions and limits to ensure the facility is kept in a safe condition. SC.6 (para 96) also looks for safety cases that are “easy to implement”, implying the conditions and limits therein must be usable. FA.9 (para 526) then provides guidance on how to identify conditions and limits in practice, suggesting that these should be derived primarily from the Design Basis Analysis (DBA). Para 526 identifies three types of limits and conditions: trip settings and performance requirements; configuration and availability conditions; and the need to define the safe operating envelope for the facility. These three types of limits and conditions are key measures for achieving the objectives of Levels 2 and 3 of the SAPs’ Defence in Depth hierarchy (EKP.3, para 143), i.e. they are needed to prevent and control abnormal operations and, if this cannot be achieved, to control faults so that these remain within the design basis.

3.3 The Engineering SAPs provide detailed guidance on the measures that should be taken in the design and operation of the facility to achieve these objectives. This includes, for example, the need to operate so that structures, systems and components remain within defined limits (EMC.21) and to monitor that this is the case (EMC.24, ESS.13); the need for safety systems to maintain a defined safe state (ESS.1, ESS.4); and the need to identify minimum levels of equipment needed for safe operation (ESS.24). In addition to the engineering, the SAPs also recognise the vital role played by the operators in ensuring the safe operating envelope is maintained and the need for systematic analysis of such controls (EHF.4). Finally, the SAPs also say (SC.8) that ownership of the safety case, including any limits and conditions derived from it (para 101), should reside with those in the duty-holder’s organisation who have direct responsibility for safety. In practice, this ownership falls to the Duly Authorised Persons (DAPs) who are responsible under LC12 for plant safety.

3.4 Over and above these direct linkages, there is a significantly broader indirect linkage deriving from the need for safety cases to be implemented at the facility: In principle, many SAPs could give rise to an expectation of a limit or condition within the safety case, and thus to an operational limit or condition on the plant. The guidance provided here thus sets out a framework linking safety cases and their implementation in support of the whole suite of ONR’s technical safety case guidance (i.e. all SAPs and TAGs).

WENRA Reference Levels

3.5 The objective of the Western European Nuclear Regulators Association (WENRA) harmonisation programme is to develop a common approach to nuclear

safety in Europe by comparing national approaches to the application of IAEA safety standards. Their Safety Reference Levels (SRL), which are based on the IAEA safety standards, represent good practices in the WENRA member states and provide a consensus view of the main requirements to be applied to ensure nuclear safety. The UK is committed to aligning its regulatory guidance with the WENRA safety reference levels and in keeping with ND's guidance on the demonstration of ALARP [10], inspectors should consider the WENRA Reference Levels to be Relevant Good Practice for civil nuclear reactors.

3.6 This guide has drawn from the WENRA Reactor Harmonisation Working Group's Safety Reference Levels [3], particularly Appendix H which addresses Operational Limits and Conditions at civil nuclear reactors (N.B. Decommissioning and Storage Reference Level D68 is also relevant). To assist cross-reading between these guides, instances where the present guidance is linked to a particular Reference Level, e.g. Level m of Part n in Appendix H, will be denoted by the notation [Hn.m]. In the interests of brevity, where a Reference Level could have been linked many times over, only the key linkages have been provided. Moreover, certain of these Reference Levels relate to the implementation of limits and conditions, rather than to their derivation, and so have been linked to the companion TIG [1], rather than to this guide.

IAEA Safety Standards

3.7 The IAEA Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2006 and are recognised by HSE as relevant good practice. The assessor should therefore consult them, where relevant.

3.8 This guide and companion TIG [1] have been written to reflect IAEA safety standards and requirements. Here, the principal guidance NS-G-2.2 [4] applies strictly only to Nuclear Power Plants. However, NS-G-2.2 is increasingly being applied to other types of nuclear facilities (e.g. cross references to NS-G-2.2 in radioactive waste store guidance [16]), is consistent with the approaches set out for spent fuel facilities in [14] and [15] and it underpins the fundamental structure for limits and conditions implied within IAEA's Safety Glossary [12]. NS-G-2.2 has therefore been used in this Technical Assessment Guide as a source of general guidance applying to all types of nuclear facilities.

4. Advice to inspectors

Terminology

4.1. A key difficulty in regulating LC23 has been that there is no single, universally accepted, terminology. Misunderstandings in this regard often caused confusion in discussions with licensees. For instance, the term "Operating Rule" has been interpreted variously as: any limit or condition derived under LC23; an important safety limit requiring ONR Approval and Safety Committee endorsement; or a high-level limit or condition needed to define protection system settings in order to prevent doses in excess of legal limits. There is a similarly wide variety of interpretations to the term "Safe Operating Envelope". In view of this, from this point onwards, this guide will adopt a self-consistent terminology, in which terms with a specific technical meaning will be highlighted in *red italics*. The following definitions will be used:

- ❖ *Operating Rule (OR)*: Any condition or limit in place at a nuclear facility through which, a licensee demonstrates compliance with its safety case. *ORs* can embody any limit or condition necessary in the interests of

safety derived from the licensee's safety case, provided they relate to nuclear, radiological or radwaste safety (i.e. where the relevance to safety lies within the remit of the Nuclear Installations Act (as amended) 1965). In this guide, the term *OR* also includes temporary *ORs*, e.g. those used to control one-off or short-term operations.

- ❖ *High Hazard Operating Rule (HHOR)*: Any *OR* important to nuclear safety, i.e. an *OR* relating to risks and consequences residing broadly within Tiers 2 and 3 of the hierarchy defined in the next section, or graded as such by the licensee. In view of their importance, *HHORs*¹ are the prime focus of this guide and represent the subset of *ORs* to which inspectors should be applying their greatest attention.
- ❖ *Low Hazard Operating Rule (LHOR)*: Any *OR* appearing in the licensee's safety case that is not a *HHOR*, i.e. an *OR* relating to risks and consequences residing broadly within Tier 1 of the hierarchy defined in the next section, or graded as such by the licensee. Although licensees have a legal duty to derive, implement and comply with *LHORs*, they should not be the prime focus of its safety management system, nor of ONR's attention.
- ❖ *Normal Operations*: Operation within specified operational limits and conditions². *Normal operations* are intended to embody all the modes of operation permitted at the facility, e.g. including start-up and shutdown states and temporary situations arising due to maintenance and testing [H4.1] and to include so-called Anticipated Operational Occurrences³.
- ❖ *Fault Conditions*: Operation beyond *normal operations* arising from an unplanned departure from the specified mode of operation of a structure, system or component due to a malfunction or defect within the structure system or component or due to external influences or human error. This is based on the SAPs' definition of "Fault". *Fault conditions* include faults with consequences that have not (or cannot) be justified to be Anticipated Operational Occurrences in the safety case.
- ❖ *Normal Operations Operating Rule (NOOR)*: Any *HHOR* used to denote the boundary between *normal operations* and *fault conditions*⁴.
- ❖ *Safety Measure*: A safety system, or a combination of procedures, operator actions and safety systems that prevents or mitigates a

¹ *HHORs* are the UK equivalent of the IAEA's "Operating Limit and Conditions" (OLCs), which are used (see e.g. [4], [12]) for those limits and conditions in place at nuclear power plants that have been approved (in the general English sense of the word) by the regulatory body, i.e. the most important limits and conditions.

² Although this is the same definition as used by both IAEA [12] and the SAPs [2], there is a subtle, but important, distinction in meaning between the two sets of guidance. As noted above, IAEA's definition of OLCs equates broadly to *HHORs*, implying a narrower definition of *normal operations* than intended in the SAPs. In this document however, the intended meaning of *normal operations* is as per the SAPs, i.e. operations compliant with any identified limits and conditions, not just those *ORs* graded as *HHORs*.

³ An IAEA term for foreseeable, but undesired deviations from planned operation justified in the safety case to not result in any significant detriment to safety.

⁴ The term *NOOR* has been introduced for consistency with the IAEA concept of "limits and conditions for normal operations" – a subset of OLCs in [4]. As noted above, the SAPs definition of *normal operations* is broader than in the IAEA's approach and hence a separate term is needed to express the IAEA concept, which applies only to high hazard situations rather than to cases of lower hazard where applying such controls would be disproportionate. Hence the term *NOOR* is used for *ORs* that mark the boundary between *normal operations* and *fault conditions* in cases where the unmitigated risks and consequences lie broadly within Tiers 2 and 3 of the hierarchy defined in the next section.

radiological consequence⁵. Such safety systems will be safety mechanisms, devices and circuits for the purposes of LC27.

- ❖ **Safety Setting:** The point at which a *safety measure* is intended to activate or initiate during *fault conditions*.
- ❖ **Safety Limit:** A limit on operational parameters within which the operation of the facility has been shown to be safe⁶. *Safety limits* are thus the outermost *ORs*, beyond which the safety case has not, or cannot, demonstrate safety, e.g. in an operating reactor, the lowest conceivable temperature beyond which the fuel clad could melt.

N.B. This terminology has been adopted in the interests of consistency and clarity within the present guide. Its use is not intended to suggest that Licensees should be encouraged to change their own terminologies. Inspectors seeking to change the terminology used by a licensee need to consider, inter alia, the possible safety disadvantages from so doing.

Operating Rule Tier Hierarchy

4.2. Although LC23(1) requires licensees to identify all conditions or limits necessary in the interests of safety, ONR expects a targeted and proportionate (graded) approach in which the greatest attention and care is applied to the identification and implementation of conditions and limits with the greatest importance to safety. Licensees' safety case methodologies should therefore employ a hierarchical approach to deriving *ORs* that is appropriate to the risks and hazards addressed. The hierarchy needs also to ensure that, when implemented, all *ORs* will be given a suitable and sufficient degree of attention, avoiding a situation in which the importance of *HHORs* becomes lost in a sea of lesser *LHORs*.

4.3. Clearly a number of hierarchies could be employed; licensees need to select an approach that is appropriate to their situation and in particular is consistent with their DBA methodology. In general, individual approaches should resemble the following hierarchy, which is consistent with ONR's DBA guidance in the SAPs:

- ❖ **Tier 1:** This addresses limits and conditions which, if exceeded, could at worst contribute to only a low/medium level of realised hazard relative to the fault Initiating Event Frequency (IEF). Here, "low/medium level" should be interpreted to mean assessed unmitigated off-site consequences (based on a conservative assessment) below the levels where SAPs Target 4 suggests DBA should be applied (see Figure 1a above) or below 500mSv for on-site DBA faults. In view of their likely (large) number and nature, such *LHORs* should normally be identified to operating personnel within LC24 Operating Instruction type (or possibly IRR-related) documentation and need not be subject to the safety management processes set out in T/INS/023 [1].
- ❖ **Tier 2:** This addresses limits and conditions, which if exceeded, could at worst, contribute to a high level of realised hazard relative to the fault IEF. Here, "high level" should be interpreted to mean the assessed unmitigated consequences (based on a conservative

⁵ This is part of the definition used in the SAPs (the omitted part relates to passive *safety measures* and is not relevant here).

⁶ This is essentially the IAEA definition but modified for style and generalised to all nuclear facilities.

assessment) are where SAPs Target 4 indicates DBA should be applied for off-site faults, but fall short of Tier 3 criteria (see Figure 1a above), or are more than 500mSv for an on-site fault. Such *HHORs* should be:

- Identified to operating personnel in separate documentation;
 - Subject to the implementation arrangements set out in T/INS/023 [1], and
 - Controlled via safety cases categorised at a level in the licensee's safety management process that requires ONR's formal *agreement* (or equivalent, depending on the detail of the local LC Arrangements / procedures) to the associated activities.
- ❖ **Tier 3:** This addresses limits and conditions which, if exceeded, could contribute to a very high level of realised off-site hazard. This should be interpreted to mean:
- An off-site fault whose unmitigated consequences exceed 100mSv (based on a conservative assessment) (see Figure 1a above); or
 - An off-site fault whose unmitigated consequences exceed 30mSv (based on a best-estimate assessment); or
 - Where either ONR has specific concerns or international precedents suggests additional regulatory control to be appropriate.

N.B. In line with international best practice, no specific Tier 3 criteria have been set for on-site faults.

HHORs in Tier 3 should be controlled and managed to at least the same standards as those for Tier 2, and preferably via safety cases categorised at the highest level in the licensee's safety management process. Based on international best practice, ONR should consider Tier 3 *HHORs* to be candidates for *approval* under LC23(4). However, decisions on which *HHORs* should be *approved* are a matter for Divisional regulatory policy. For instance, candidates for *approval* would not normally include *HHORs* where:

- ONR already has adequate control under existing arrangements and to add further controls would be disproportionate; or
- The *HHOR* makes only a small contribution to avoiding the hazard being realised, e.g. in view of the time available to the operators to reverse a non-compliance before serious consequences could materialise.

4.4. Following SAPs para 504, *ORs* relating to the potential for "significant quantities" of radioactive material to escape from their designated place of confinement (see SAP FA.2) should be categorised according to the dose that could be realised if the material were to be released. However, *ORs* relating to faults leading to a "substantial" relocation (as defined in SAPs para 543) with potential off-site consequences should normally be categorised in Tier 3.

4.5. Since the aim of these Tiers is to facilitate a targeted approach so that the *HHORs* have greatest prominence, consideration needs also to be given to the contribution that each individual *OR* makes to overall defence in depth (see following section). The set of *ORs* derived from a high hazard fault sequence will not be of equal importance and so they should not all necessarily be classed as *HHORs*. Indeed to do so could lead to an unmanageable number of *HHORs*. For example, an *OR* associated with the mitigation of the consequences of an accident following the earlier failure of the prevention and protection measures might make only a relatively small contribution. It is legitimate within the scheme set out here to demote such *ORs* to a lower Tier, so that focus is applied to the preventative / protective *ORs* contributing most to safety. However, it should be rare to demote those *ORs* providing the fault prevention or protection (see following section) on this basis, since these would normally form the prime defences. Equally, it should be rare to demote *ORs* requiring the availability of plant, systems, equipment or supplies needed within short timescales (even at Levels 4 and 5), where a delay in deployment could fundamentally undermine the required safety function. Equally, *ORs* might be promoted to higher Tiers if for example, the PSA or Severe Accident Analysis (SAA) suggests that these are particularly important limits or conditions needed for nuclear safety.

4.6. Demoting or promoting *ORs* to different Tiers needs necessarily to be a matter of judgement. However, licensees' schemes for setting Tiers should normally apply the following general rules:

- Demoting to *LHOR* status should only take place because the number of *HHORs* is considered unmanageable to an extent that safety performance could realistically be compromised. In such cases, demoting may still not be the appropriate remedy, since a plethora of *HHORs* could well indicate a more fundamental problem with the design, e.g. an over-reliance on operational rather than automatic *safety measures*, or a failure to group similar *HHORs* appropriately into single bounding *HHORs*;
- An *HHOR* should only be demoted if the *HHORs* remaining in the original Tier continue to constitute a suitable and sufficient, independent barrier to the fault's progression, preferably at earlier Levels in the Defence in Depth hierarchy;
- Any *HHOR* that is demoted is judged to make only a minor contribution to nuclear safety, e.g. the demoted *OR* supports other *HHORs*, such as a surveillance / monitoring criterion or an underlying assumption; or it relates to barriers at Level 4 or above in the Defence in Depth hierarchy; or it has only indirect relevance to how the operators would operate the facility;
- Promoting *ORs* is solely on the basis of their importance to safety, e.g. based on the PSA or the engineering assessment.
- Preventative and protective *HHORs* (i.e. those defined for Levels 2 and 3, including *NOORs*) should rarely be demoted. When this is proposed, the *HHORs* remaining need to continue to form a suitable and sufficient preventative and protective barrier, i.e. the demoted *OR* makes only a relatively small contribution to safety compared to the remaining Level 2/3 *HHORs*.
- It should be rare to demote *ORs* requiring the availability of plant, systems, equipment or supplies needed within short timescales, even

at Levels 4 and 5. Where such demotions are proposed, the safety case should justify that implementing as a **LHOR** will not undermine the required safety function.

- The re-grading of **ORs** should ideally be part of a holistic review aimed at providing confidence in the overall manner in which the safety case will be implemented.

Example 1 (Annex 3) includes a practical illustration of how to apply the above methodology.

4.7. When applying **OR** tiering it needs to be kept in mind that DBA is not an exact science and hence the designations in Figures 1a and 1b should be regarded as indicative, rather than fixed criteria. In particular, the approach applied should take account of analysis uncertainties. For example, it would be legitimate, within the approach set out above, for a (Tier 1) **LHOR** that lies just outside the Tier 2 region, to be categorised as a Tier 2 **HHOR** unless the analysis placing the **OR** in Tier 1 was grossly conservative. Furthermore, it should be recognised that Figures 1a and 1b are a simplification of the SAPs' criteria, which are multi-faceted and so cannot be presented simply (e.g. different IEF criteria apply for natural hazards). In general, the SAPs (particularly para 514) and the Technical Assessment Guide on external hazards [6] should be used to determine definitive designations of the Tier regions consistent with wider ONR guidance.

Operating Rules and Defence in Depth

4.8. The prime purpose of **ORs** is to translate requirements and assumptions identified in the safety case into a form that allows the operators to carry out their activities while controlling the facility in a safe manner compliant with the safety case (see LC23(1 and 3)) [H1.1]. Based on SAP EKP.3 and its supporting guidance, the safety case should adopt a defence in depth approach, i.e. a series of defences aimed at ensuring faults do not escalate into significant consequences. As far as is practicable, these defences should be made as independent of one another as possible. SAPs paras 142 and 143 set out the objectives of a defence in depth approach and the "essential means" needed to ensure faults do not progress from one "Level" to the next. Adopting this approach and terminology, the safety case should therefore provide **ORs** so that essential means are identified against each of these objectives [H1.2] (other than for Level 1 of the SAPs' hierarchy, which relates to how the facility is designed rather than how it is operated – see below). In detail:

- Level 2 – prevention and control of abnormal operation and detection of failure: Here the safety case should, where appropriate, define two types of **OR** namely:
 - (i) a precise definition of each permitted mode of **normal operation** so that it will always be clear what operating mode the facility is in, what **fault conditions** need to be prevented while in this mode and what exactly needs to be controlled and
 - (ii) what equipment (e.g. indications, alarms) needs to be in place to detect any excursions from the permitted mode of **normal operations**, together with any associated settings.
- Level 3 – control of faults within the design basis: Here the safety case should, where appropriate, identify **ORs** to:

- (i) ensure the availability of suitable and sufficient *safety measures* that need to be in place to provide protection, together with their associated *safety settings*;
 - (ii) define the limit of the design basis; and
 - (iii) state what equipment will be needed to monitor conditions during design basis faults.
- Level 4 – control and mitigation of accident conditions: Here the safety case should, where appropriate, identify *ORs* to:
 - (i) trigger the implementation / activation of the accident mitigation / protection *safety measures* and other accident management arrangements;
 - (ii) ensure the availability of these *safety measures* and define their associated *safety settings*;
 - (iii) state what equipment will be needed to monitor accident conditions;
 - (iv) define relevant *safety limits*.
- Level 5 – mitigation of significant radiological releases: Here the safety case should, where appropriate, identify *ORs* to:
 - (i) trigger the implementation of the on- and off-site emergency response; and
 - (ii) identify what equipment and personnel need to be available to confirm whether or not a significant release has occurred, to monitor conditions and to address the emergency response (e.g. site boundary / fence radiation monitors).

4.9. The absence of Level 1 (prevention of abnormal operation and failures by design) in the above list needs to be expanded upon. The duty in LC23(1) to identify conditions and limits necessary in the interests of safety clearly extends to the engineering design process. However, provided this process has worked effectively, the conditions and limits needed for passive safety aspects will not result in any need for operational compliance checks post-commissioning (other than perhaps occasionally, e.g. as part of a Periodic Safety Review). For example, a shield wall may be subject to a maximum load (weight) limit imposed by design constraints in adjacent parts of the structure. Once the wall has been designed and installed compliant with these constraints, these limits, though part of the safety case, are no longer of any active concern to the operators, and hence should not give rise to any *ORs*. Other non-passive aspects of the design will nevertheless result in limits and conditions that the operators will need to comply with, e.g. constraints on the temperatures, pressures etc within which plant and equipment can perform their safety functions or to minimise the likelihood of initiating events; maintenance frequencies etc. Such *ORs* will however need to be derived specific to the predicted (fault) conditions where they apply and will thus be assigned to one or more of the Levels 2 to 5 of the Defence in Depth hierarchy, rather than to Level 1. Moreover, the nature of such *ORs* will depend more on the underlying branch of engineering than on matters addressed in this guide. In view of these considerations, no detailed advice will be provided here on Level 1 (design) *ORs* other than in general terms where these relate clearly to one of the Levels.

4.10. The extent to which the *ORs* at Levels 2 to 5 need be identified will vary according to the type of facility, the range of its design basis faults and reasonable

practicability considerations. Further guidance on appropriate *ORs*, Level by Level, is provided in the following paragraphs:

Level 2

4.11. Where the hazard is sufficiently high, the safety case should always identify *NOORs*. This is because prevention will necessarily be the first line of defence against faults and operators often provide a flexible and effective means of avoiding an escalating fault condition at initiation. The *NOORs* should include definitions of all the operating modes that will normally be permitted at the facility; these permitted operating modes in sum then define the totality of *normal operations*. However, in instances where the risks / consequences are in Tier 1, the approach to Level 2 (prevention) limits and conditions set out in the following paragraphs may not be reasonably practicable.

4.12. The *NOORs*, should be set some margin away from the conditions where the facility is intended to be operated since contravening a *NOOR* should be regarded as a serious matter. In cases where a *NOOR* can be gradually approached (e.g. the limit is set in terms of a continuous parameter such as pressure or temperature, rather than as a conditional state such as System X is available for duty), the safety case should identify further supporting limits and conditions. These *ORs* should be set before the *NOOR* so that operator action and / or engineered means may be used to return conditions back to normal without contravening any *NOOR*. Normally, these supporting limits and conditions would be defined in the (LC24) instructions used by the operators to restore normality, and be linked to indications and alarms. Operational fluctuations between these supporting *ORs* and the *NOOR* should be regarded as part of *normal operations*. Exceeding these supporting *ORs* should nevertheless be considered by the licensee within its Learning from Experience arrangements in order to minimise the likelihood of repeat events. Margins should also be sought where reasonably practicable in cases where the *NOOR* can only be approached in discrete steps, e.g. by providing redundant / diverse equipment that can be substituted-in in the event of equipment unavailability. Further guidance on substitution arrangements is provided below.

4.13. The safety case should consider how the facility would be brought back within *normal operations* following a *NOOR* being exceeded, and then identify further *ORs* specifying maximum timescales within which normality must be restored. These timescales should be as short as reasonably practicable taking account of the speed at which conditions can safely be changed and the risks from operating in unfamiliar territory [H6.2].

4.14. A key aspect of identifying *NOORs* is the need to ensure that *normal operations* are controlled in a manner which keeps all safety-related components and structures within defined limits (see EMC.21). The safety case analysis here should identify potential failure modes, determine how these might be affected by the manner in which the facility is operated, and then define appropriate *NOORs* / *LHORs* so that failures are then minimised. There will normally be two such classes of failure to be considered: failures that lead to initiating events (e.g. breaches of primary containment due to stress cycling, corrosion etc) and failures that could prevent delivery of a safety function when called upon (e.g. reactor graphite cumulative damage prejudicing control rod insertion).

Level 3

4.15. *ORs* should always be defined to specify the availability of *safety measures* (see also SAPs ESS.1 and ESS.24) [H6.1]. Similarly there should always be *ORs*

in place to define the corresponding *safety settings*, together with any provisions that the *safety measures* will need in order to operate, e.g. power supplies, fuel stocks, chemical stocks. The *ORs* defining the required *safety measures* will normally be amongst the most important safety limits and conditions (see para 1.10) and so their derivation should be a key focus of the safety case. The *safety settings* should be located with an adequate margin to *normal operations* to avoid inadvertent initiation/activation of the *safety measures* [H5.1]. The safety case should include deterministic analysis (which should be DBA for *HHORs*) to show that these *safety measures*, *safety settings* and provisions will be sufficient to return the facility, if it were to suffer a fault while operating at the limit of its permitted *normal operations*, back to a safe and stable state (and preferably back to within *normal operations*) without entailing serious consequences. Here it should be emphasised that the term *normal operations* embodies all the operating modes permitted at the facility. Hence the *ORs* governing minimum *safety measures* should not be limited to just the principal operating mode for which the facility was designed, but address all permitted operating modes.

4.16. A key aspect of the deterministic analysis will be to evaluate the extent to which it remains safe for faults to develop before they can be turned around, i.e. kept within the design basis (see ESS.4 and supporting text). The safety case needs to establish that, even at the worst point during a design basis fault, conditions will remain within *safety limits* with as large a margin as reasonably practicable. To achieve this, *safety settings* should be set against design basis limits that are as low as reasonably practicable and, where reasonably practicable, the design basis should incorporate substantiated operational margins to any relevant *safety limit*. Achieving reasonable practicability in these aspects will normally require a balance to be struck between the operational (etc) benefits of relatively loose design basis limits compared to the safety dis-benefits of more restrictive operation. Such balances should be determined with due regard to uncertainties so that the safety case provides a robust underpinning for the design basis.

4.17. Such margins may not be possible for every design of plant, nor for every fault (e.g. it may not be reasonably practicable to define them for certain at-power faults on nuclear power plants). However, in cases where separate design basis limits can sensibly be set, the licensee may elect to use these as part of its *normal operations* safety management processes. Relying too heavily on this type of *OR* has significant disadvantages however, since it places the operational safety focus on fault protection rather than on prevention, and thus the compliance demonstration can become far removed from the operator's day-to-day reality. Thus, where such an approach is followed, the safety case needs also to derive suitable and sufficient *NOORs*, so that the full suite of *ORs* provides adequate coverage of fault prevention as well as protection.

Level 4

4.18. Setting design basis *ORs* within the safety case is considered to be good UK practice and goes beyond what is formally required by IAEA for nuclear power plants [4]. To reach Level 4 implies that the Level 3 *safety measures* protecting against the fault must have failed. The design basis *ORs* may thus be used to trigger the implementation / activation of the facility's accident mitigation *safety measures* and other accident management arrangements identified in the licensee's safety case. Inspectors should not however expect to see design basis *ORs* at all types of facility, or indeed for every fault sequence. For instance, the

speed at which some fault sequences could progress from Level 3 (control of faults within the design basis) to Level 5 (mitigation of significant radiological releases) at nuclear power plants might make it impracticable to identify mitigation *ORs* within Level 4. Equally, the magnitude of the hazard potential presented by the facility could mean that Level 4 aspects are not addressed in great detail within the safety case. Conversely, it will be the case for many types of facility (particularly at nuclear chemical plants, where the concept of design basis *ORs* was first developed) that fault progression through Level 4 will be slow enough to make the implementation of beyond design basis mitigation measures reasonably practicable. Where this applies, the safety case should also identify corresponding *ORs*. These *ORs* should be set so that operators can return the facility back to a safe and stable state, and preferably back to within *normal operations*, minimising adverse consequences of the fault and without exceeding any *safety limits*.

Level 5

4.19. The suite of *ORs* should always include a suitable and sufficient set of *safety limits*, defined conservatively so that no significant consequences (which in radiological terms should be interpreted as exceeding IRR dose limits) can arise without at least one *safety limit* being exceeded [H5.2]. N.B. IAEA guidance [4] suggests that *safety limits* on operational nuclear power plants should be set with sufficient conservatism so that exceeding any single *safety limit* alone will not lead to unacceptable consequences. The *safety limits* should be identified through conservative (normally engineering substantiation) analysis, taking due account of uncertainties and couched in terms that are meaningful to the facility operators. From an operational perspective, the prime application of these *ORs* is to inform (and potentially to act as triggers within) the emergency arrangements and accident management strategies.

Aspects applying at all Levels

4.20. In the above paragraphs, little mention has been made (in the interests of avoiding tedious repetition) of the need for *ORs* to cater for plant monitoring (surveillance) arrangements (e.g. indications and alarms). The safety case should nevertheless define the *ORs* necessary to implement all reasonably practicable monitoring arrangements identified in the safety case at all Levels of the defence in depth hierarchy [H9.1]. In particular, where equipment (including *safety measures*) is needed to operate, or has a limited qualification range, there should be *ORs* to ensure the operators have a suitable means of confirming its status (see EMC.24, ESS.13c).

4.21. In addition to defining the *ORs*, the safety case should also include proportionate analysis to determine the circumstances and frequencies where compliance with each *OR* needs to be confirmed (and recorded). This analysis is particularly important for *NOORs*. Here, the compliance confirmation requirements should be drawn up taking into account the quickest speed at which adverse conditions (e.g. operational drift) or faults could develop, so that there is a margin of confidence that prevention measures will be initiated quickly enough to be successful. The deterministic analysis (or DBA for Tier 2 and 3 *HHORs*) should therefore make pessimistic assumptions in regard to the timing of the checks (e.g. assume a fault occurs immediately following a positive compliance confirmation), utilising the results of transient analysis where necessary. The resultant circumstances and frequencies should normally be designated as *LHORs*, even if they relate to surveillance arrangements for a *HHOR*.

4.22. Modern power reactors adopt a Tech. Spec approach to **ORs**, whereby limits and conditions include specific time periods etc so that non-compliance is only deemed to have occurred when the limit has been exceeded for longer than a prescribed time interval, or on more than a specific number of occasions within a given time period etc. This approach, where appropriately justified within the safety case, provides a graded method of OR compliance that seeks to avoid situations where returning immediately to *normal operations* induces greater risks than a slower, but more considered return. For example, tripping a power reactor immediately following the loss of a back-up pump could well incur greater risks than running for a limited period without that pump available. Provided provision is made to shut down if the non-availability extends beyond prescribed limits, pre-justified in the safety case, then setting **ORs** in this manner should be encouraged. Indeed the Tech. Specs approach, through which **ORs** provide operators with a suitable but well-defined degree of operational flexibility, is considered to align with internationally accepted best practice and meet the requirements of LC23.

4.23. The set of **ORs** should also include and cater for any underlying assumptions made in the safety case. Such **ORs** are needed to ensure that theoretical arguments put forward will continue to remain valid in practice. **ORs** of this type often arise out of PSA, e.g. where it is assumed that a certain activity is carried out no more than N times per year, or a piece of equipment is available X% of the time. Although these **ORs** will rarely make a prime contribution to overall safety (and so will likely be denoted **LHORs**) they nevertheless require implementation. Here the implementation arrangements need to reflect the nature of the **OR**, and what the licensee would do in the event of a non-compliance. For example, where exceeding an annual limit would only entail an update of the numerical risks (i.e. not leading to any change in the safety provisions applied), quarterly or annual retrospective checks will likely be sufficient. Inspectors should nevertheless be alert to the need to capture underlying safety case assumptions as **ORs** and consider whether the manner in which such **ORs** are implemented is commensurate with the risks arising if they were to be exceeded.

Types of Operating Rules

4.24. Based on the above, inspectors should expect to see a variety of types of limits and conditions arising from licensees' safety cases, including (where relevant) the following broad types of **ORs**:

- ❖ **Parametric**: defining the boundaries between Defence in Depth Levels (e.g. *normal operations*, *fault conditions*, etc) in terms accessible to the operators to trigger associated responses in the event of non-compliance, including notification and reporting arrangements (see LC23(3)).
- ❖ **Operational**: defining minimum levels of, and permitted configurations for, plant, equipment and associated supplies, together with staffing levels that the safety case says need to be available, Level by Level, to ensure suitable and sufficient protection and monitoring in all permitted modes of operation.
- ❖ **Protective**: defining the *safety settings*, i.e. the point at which *safety measures* are intended to activate or be initiated during *fault conditions*.
- ❖ **Time-based**: defining the surveillance requirements (i.e. frequencies, circumstances) for monitoring compliance against each **OR**, allowed time-periods when *safety measures* etc are permitted to be

unavailable and the time periods within which operators need to complete identified activities.

- ❖ Theoretical: to capture the success criteria used in the safety case, e.g. design basis limits, *safety limits*.
- ❖ Underlying: to capture other assumptions made in the safety case of lesser importance to safety.

Derivation of ORs

4.25. The *ORs* are the means by which the theoretical analysis set out in the safety case is translated into practical terms that ensure the facility will be operated safely. As such, and as stressed already in this guide, it is imperative that all *ORs* (including any temporary *ORs*) are derived from the facility's safety case [H1.1]. Limits and conditions derived for other reasons (e.g. solely from economic or performance considerations) should not be included in the *ORs*. Here the term 'safety case' should be interpreted as per the SAPs – “the totality of a licensee's (or dutyholder's) documentation to demonstrate safety ...” – and not just how the licensee defines this term. That said, inspectors should be alert to cases where an *OR* has resulted from the licensee's due process, but the due process has not included appropriate written justification that risks have indeed been reduced to ALARP. For example, some UK licensees determine substitution arrangements for instances when the *safety measures* identified in the formal 'safety case' are temporarily unavailable as part of 'safety case implementation'. These substitution arrangements (which are themselves written documents) are considered by the appropriate safety committee and documented in the committee minutes. Such an approach will normally be acceptable provided the decisions reached are supported by an appropriate analysis that justifies the relevant risks are ALARP – this analysis then forms part of the safety case. In general, inspectors should beware of instances where plant limits and conditions have arisen solely through some form of management decision, and are not reflected in the safety case, since this draws into question the adequacy of the licensee's LC14 arrangements for producing safety cases. Here, recognising that management discretion can be an important part of a licensee's safety management systems, inspectors should encourage the licensee to determine why its formal processes have not required an *OR*, and then seek to move the licensee to a position where its safety case and *ORs* are in full alignment.

4.26. The converse of the previous situation also applies – inspectors should consider whether the limits, conditions and assumptions present in the safety case have actually resulted in *ORs* at the facility. SAP SC.6 and its supporting paragraphs are particularly relevant here – the safety case needs to identify all important aspects of operation and management required for maintaining safety and set out operating limits and conditions in a manner that is easy to understand and allows them to be implemented.

4.27. In deciding whether the *ORs* cater for all important aspects of operation and management, i.e. whether the list of *ORs* derived in the safety case is complete, inspectors should consider, in view of the type and magnitude of the hazards involved, whether the *ORs* take adequate account of:

- (i) All the permitted operating states⁷ of the facility;

⁷ For a nuclear power plant, the permitted operational states should include power operation, shutdown and refuelling, any intermediate conditions between these states and temporary situations arising due to maintenance and testing [H4.1].

- (ii) All identified sources of hazard;
- (iii) All identified fault sequences;
- (iv) All Levels of defence in depth listed in SAPs paras 140ff (see paras 4.8ff). (The *ORs* should form a sufficiently complete set so that it is not possible to pass from one Level of the SAPs' Defence in Depth hierarchy addressed by the safety case to another without contravening at least one *OR*);
- (v) All the types of *ORs* listed at para 4.24⁸;
- (vi) All the plant and equipment claimed in the safety case, including the range of operability within which these will need to perform safety functions and the resources and services these require;
- (vii) All human-related claims made in the safety case, e.g. minimum staffing requirements.

4.28. Most *ORs* should be derived from the facility's deterministic analysis (see FA.9 and supporting text). Where the hazard potential is great enough, this should be DBA (and so result in *HHORs* for off-site / significant on-site faults). Use of DBA ensures that there will be good margins of conservatism between the limits applied and reality. In particular DBA should be the prime source for determining *NOORs*, *safety settings*, design basis limits and, in conjunction with the engineering analysis, *safety limits*. The DBA will also provide a significant input in regard to the availability of *safety measures* and provide the backbone to the Defence in Depth framework. However, it is important that the safety case does not limit the derivation of *ORs* to deterministic analysis; *ORs* should also be derived from the PSA, the engineering substantiation and other parts of the safety case (e.g. the Severe Accident Analysis, overarching reviews) as appropriate. The PSA will be particularly important in determining *ORs* governing the availability of *safety measures*, will be a key input to holistic reviews of *ORs* and will normally be the principal source for rules relating to allowed substitution periods and the non-availability of safety measures (see below) so that any periods of elevated risk may be suitably justified. The engineering substantiation will be both a prime input to the DBA (e.g. in determining *safety limits*), and a source of *ORs* in its own right. For instance, the engineering substantiation should (inter alia) provide limits on operation to prevent fault initiation or escalation; ensure design assumptions and intent are met; set conditions on appropriate plant and equipment configurations; specify the timing of maintenance and testing activities⁹; cater for plant ageing and corrosion effects; and set *ORs* relating to equipment qualification [H2.1].

4.29. The safety case should identify a subset of the *ORs* that will be used by the licensee for event reporting under LC23(3). In line with international good practice, LC23(3) event reporting should normally be initiated at the limit of *normal operations*, i.e. using the *NOORs*. In cases where a licensee wishes to use an *OR* at a deeper Level in the Defence in Depth hierarchy for this purpose, then this should be justified explicitly taking into account the remaining margins of safety between the reporting level and relevant *safety limits*. In general there should be a substantial margin of safety between *ORs* used for event reporting and any *safety*

⁸ In addition, statutory and other general requirements (e.g. site licence conditions) should not be duplicated in the *ORs*. Equally, limits which physically cannot be exceeded (e.g. because of fundamental constraints inherent in the plant design) should not be included.

⁹ N.B. PSA may also be relevant here, e.g. through reliability analyses.

limit so that there is a very low likelihood that exceeding a reporting level will entail initiating any emergency arrangements.

4.30. Inspectors should beware of instances where the licensee sets its *ORs*, and in particular those used for LC23(3) reporting, too loosely (i.e. further into the fault progression sequence than is reasonably practicable), for instance in fear of the reporting and regulatory consequences that might follow a non-compliance. Here it needs to be recalled that the prime purpose of *ORs* is not event reporting etc, but to ensure that the facility is operated in accordance with its safety case. Nevertheless, reporting (etc) considerations are important, and thus need to be factored into where the *OR* is set, e.g. to avoid unnecessary over-reporting. In general, *ORs* related to reporting arrangements should be set at the earliest point where non-compliance would entail a significant loss of control (c.f. the wording of LC23(3) which requires operations be controlled in compliance with the *ORs*), but loose enough so that the burden from reporting frequent non-compliance is not disproportionate to the risks / consequences. Where appropriately justified in the safety case, the approach taken in certain Tech. Specs may be useful here, i.e. the limit is set in conjunction with a time period so that non-compliance is only deemed to have occurred when the limit has been exceeded for longer than a prescribed time interval, or on more than a certain number of occasions in a given time period.

4.31. Losses of control could take many forms, e.g. it may involve plant or equipment being operated outside the range for which it has been qualified; or it may be because of an external event over which the licensee has no direct control. The manner in which the licensee sets its *ORs* should reflect a responsible safety culture in which non-compliances (or near non-compliances) are viewed as opportunities to learn from experience to ensure the event is not repeated rather than one focussed on placing blame and on possible enforcement action. Consistent with this, inspectors should emphasise that ONR's attitude to, and regulation following, an *OR* being exceeded will be proportionate to (inter alia) the degree to which control was lost, the extent to which the licensee was responsible for that loss of control and whether similar events have occurred previously (see Annex 2).

4.32. The licensee's safety case should provide sufficient information to allow the *ORs* that are most important to safety to be readily identified. In particular, the fault analysis, etc, and methodologies employed need to be compatible with the approach taken to categorise *ORs*. Ideally, this categorisation should take place within the safety case. However, it is sufficient for the safety case to provide the necessary information so that categorisations can be assigned later through another process. Such an approach has particular merit, since it facilitates a holistic view of the barriers. In considering whether the licensee's overall approach is fit for purpose, inspectors should consider the extent to which the criteria used to categorise *ORs* resembles the Tiered process defined in paras 4.3ff.

4.33. The derivation of *ORs* should pay particular attention to how they will be implemented. There are several important considerations here. For instance:

- The need for *ORs* to be defined in terms meaningful to the facility operators. For instance, a reactor safety case might be concerned with fuel heat transfer and thus derive thermal-hydraulic limits within which the fuel needs to be operated, e.g. in terms of dimensionless constants. The resultant *ORs* should however be a translation of these limits into amenable (surrogate) parameters, such as

measurable pressures and temperatures. The safety case should demonstrate that the theoretical limits or conditions cannot be exceeded provided the surrogate limits or conditions are complied with.

- The need for a straightforward demonstration of **OR** compliance. **ORs** should be written with regard to the instrumentation etc available to the operators. As such, the safety case needs to consider matters such as redundancy and diversity to cater for circumstances when the normal (frontline) instrumentation is unavailable. In addition, **ORs** should avoid requiring the operators to undertake involved calculations to determine compliance. Instead, methods such as pre-calculated compliance tables, diagrams, or on-line monitors programmed to perform the necessary calculations should be provided to assist the operators. Alternatively, if calculations are absolutely necessary, then the safety case should demonstrate that these calculations can reasonably be performed within the timescales over which adverse conditions could develop (i.e. inspectors should seek means of real-time (on-line) rather than retrospective compliance). Further guidance on the use of programmable etc systems is provided in [7].
- The need for simple **ORs**. The limits and conditions derived in safety cases will often involve several input parameters. For instance, a criticality limit may be a function of enrichment, moderator, reflector, mass and configuration. While it is legitimate for the **OR** to be written to cater for all the multiple aspects (provided these are measurable), it might be better to set the limit in alternative terms that are equally effective for ensuring safety. For instance, a criticality limit could be simplified to “no more than one full Type X container may be located in Glovebox Y at any time”, rather than say a more complicated limit involving mass and minimum proximity. Licensees should seek to define **ORs** that are as simple as possible for the operators to comply with; complicated **ORs** involving multiple parameters should in general be avoided.
- The need for practicable **ORs**. Here, the safety case needs to provide appropriate evidence that all operator actions associated with **OR** compliance, and in particular where *safety measures* are enacted / initiated by the operators, will be carried out to the quality and within the timescales assumed in the safety case.
- The need for a holistic approach to avoid an unreasonably large number of **ORs**, particularly **HHORs**. Here a least common denominator approach should be applied, i.e. if one **OR** can provide a reasonably practicable bounding limit or condition catering for several separate fault sequences then this should be used in place of several separate but similar limits. For example, the safety case for a fuel flask handling facility might consider fault sequences involving several types of flask, deriving separate limits and conditions for each type. However, the **OR** recommended by the safety case might be a single limit catering for all the various types of flask handled. In such cases it is important that the safety case demonstrates that the universal **OR** is bounding for all the relevant fault scenarios.

- The need to consider who will be responsible for ensuring compliance with the **OR**. This is strongly related to the previous point. The key question inspectors should ask here is whether the totality of the **ORs** that individual (or groups of) operators will be required to apply is manageable, given the totality of their duties, their likely capabilities and the training with which they have been provided. Safety cases should thus include suitable and sufficient human factors analysis to address these and related matters (e.g. the monitoring arrangements – see EHF.4). This is particularly pertinent in cases where there are many **ORs**, or where these appear potentially complicated to implement and/or monitor. In deciding whether there are “too many **ORs**”, inspectors need also to consider how frequently these will need to be applied, e.g. the presence of many **LHORs** applying to one-off tasks and set out in the relevant Operating Instructions would not normally be a matter of concern. Overall the safety case should justify that there will always be enough suitably qualified and experienced staff available, both in *normal operations* and in all *fault conditions* analysed, to maintain compliance with the **ORs** (taking account e.g. of the timescales for operator action claimed) and then set **ORs** to ensure these staffing levels are maintained [H8.1].
- The need for robust ORs. Here the safety case should consider the nature of the instrumentation / procedures that will be used to demonstrate **OR** compliance taking into account factors such as instrument drift / uncertainty, or the frequency at which the operators will check compliance. The **OR** should be set with sufficient margins so that measurement uncertainty, timing etc cannot cause an apparently compliant situation to in reality be an un-revealed non-compliance with the safety case.

Overall, the safety case should provide adequate justification that the **ORs** can be implemented with a good degree of confidence, e.g. through detailed human factors / task analysis. Further details are provided in [17]; other implementation aspects are addressed in [1].

4.34. The set of **ORs** should include limits and conditions on the minimum availability of safety equipment, and in particular of *safety measures*. Such **ORs** should be provided to ensure that for each fault addressed in the safety case, there is an identified “basket” of measures which are shown by analysis to be enough to protect against the fault, and which are covered by explicit arrangements to ensure that they will be available when needed. Here:

- “Sufficient” means able, as a group, to perform the required safety function without other *safety measures*;
- “Available” (for equipment) means:
 - (a) not known to be unavailable to function on demand as described in the safety case, either to address the fault directly or (where this is required by the safety case) to act as a standby measure in the event of the unavailability of other equipment; or
 - (b) having an appropriate form of substitute protection when known to be unavailable, justified in the safety case.

As such, the safety case should identify:

- pre-planned contingencies (substitution arrangements) to deal with potential equipment unavailability including timescales within which these arrangements need to be enacted;
 - regular testing and maintenance requirements necessary to keep the equipment in good condition and reveal failures;
 - all resource and service requirements necessary for the equipment to perform its safety function(s) (e.g. fuel stocks, power supplies); and
 - limitations on the usable lifetime of the equipment and / or its components taking account of prevalent cumulative wear / damage mechanisms.
- "Available" (for procedures) means:

Having a sufficiently high profile that implementation (as defined in the safety case) is assured with appropriately experienced and trained personnel available to perform the necessary tasks. Where operator actions are claimed to provide *safety measures*, the safety case should specify the actions that need to be completed by the operators and the timescales for so doing.

4.35. The safety case should set out and justify any substitution arrangements. Where the substitution arrangements afford a reduced degree of protection than the normal arrangements, the *ORs* should limit the maximum duration over which these may be applied (e.g. in terms of per demand or maximum duration per year). The *ORs* identifying the availability of *safety measures* etc should also specify allowed timeframes within which relevant operations / activities must be stopped in the event of non-availability. These timeframes should be as short as reasonably practicable, taking account of the risks of shutting down the process and justified in the safety case (e.g. through PSA). The *OR* should be worded so that enacting the formal substitution arrangements or stopping the process within the respective justified timeframes would not constitute exceeding the *OR* [H6.1, H6.2, H6.3].

4.36. The *ORs* should reflect the extant safety case for the facility and be kept up to date to incorporate any changes (either to the facility or its safety justification). Where a licensee relaxes a safety case, e.g. in the light of operational experience or a better understanding of prevailing uncertainties, it is legitimate for the *ORs* to remain unchanged provided that so doing is justified explicitly in the new safety case. Here the case needs to weigh the operational benefits from applying looser limits with the disadvantages arising from e.g. operator training requirements, re-calibration of equipment and the costs of updating operational documentation. Conversely, where a safety case requires that the *ORs* be tightened, the case should also consider the reasonable practicability of not operating the facility pending implementation of the new *ORs*. In cases where shutting down the facility or process is not a reasonably practicable option (e.g. at waste storage facilities), it is imperative that the revised *ORs* are implemented at the facility as soon as is reasonably practicable, with appropriate temporary means of control put in place during the interim. In general, the systematic review and update of *ORs*, e.g. in the light of operational events and experience, should form a key part of LC15 periodic safety case reviews, see [9] [H2.2, D68].

Criticality Limits and Conditions

4.37. SAP ECR.2 sets out ONR's expectation that a double contingency approach should be applied to guard against unintended criticality events. In other words, at least two unlikely, unintentional, independent and concurrent changes in condition ought to be required before such an event could occur. Here it should be emphasised that licensees' approaches to criticality safety should not differ in principle from how other aspects of nuclear safety are managed. In particular, criticality *ORs* should not be regarded as any different to other *ORs* in how they are derived or implemented. They should therefore, normally be considered as *HHORs* in view of the major hazard potential involved. In terms of the SAPs' Defence in Depth Framework (see above), the safety case should seek to identify at least two successive faults worth of margin between *normal operations* and exceeding the *safety limit*. Failing to prevent / protect against the first of these faults (i.e. move from Level 2 to Level 3 in the Framework) should necessitate exceeding at least one *NOOR*. By default these *NOORs* should also be used for event reporting, unless the safety case can provide a suitably robust argument that looser reporting arrangements are appropriate, e.g. there is triple or higher contingency, or other significant margins (see also paras 4.29 and 4.30). Beyond this, where practicable in line with the double contingency principle, the safety case should identify at least one further fault that must occur for the *safety limit* to be breached, together with the protection measures necessary to prevent this. Whether the double contingency principle can be satisfied or not, the DBA principles of fault tolerance and other relevant SAPs will still apply. The *safety limit* should in turn be determined with a suitable margin to the conditions where criticality could actually occur (Level 5).

4.38. It is noted that in many applications, criticality safety is achieved through *safety measures* that prevent an unsafe change being initiated (e.g. checking a permitted limit prior to moving fissile material or a moderator). The advice provided in this guide is equally valid and applicable to these scenarios. However, when considering such cases, Figure 2 (above) can helpfully be modified to show the fault progression as step changes (see Figure 3).

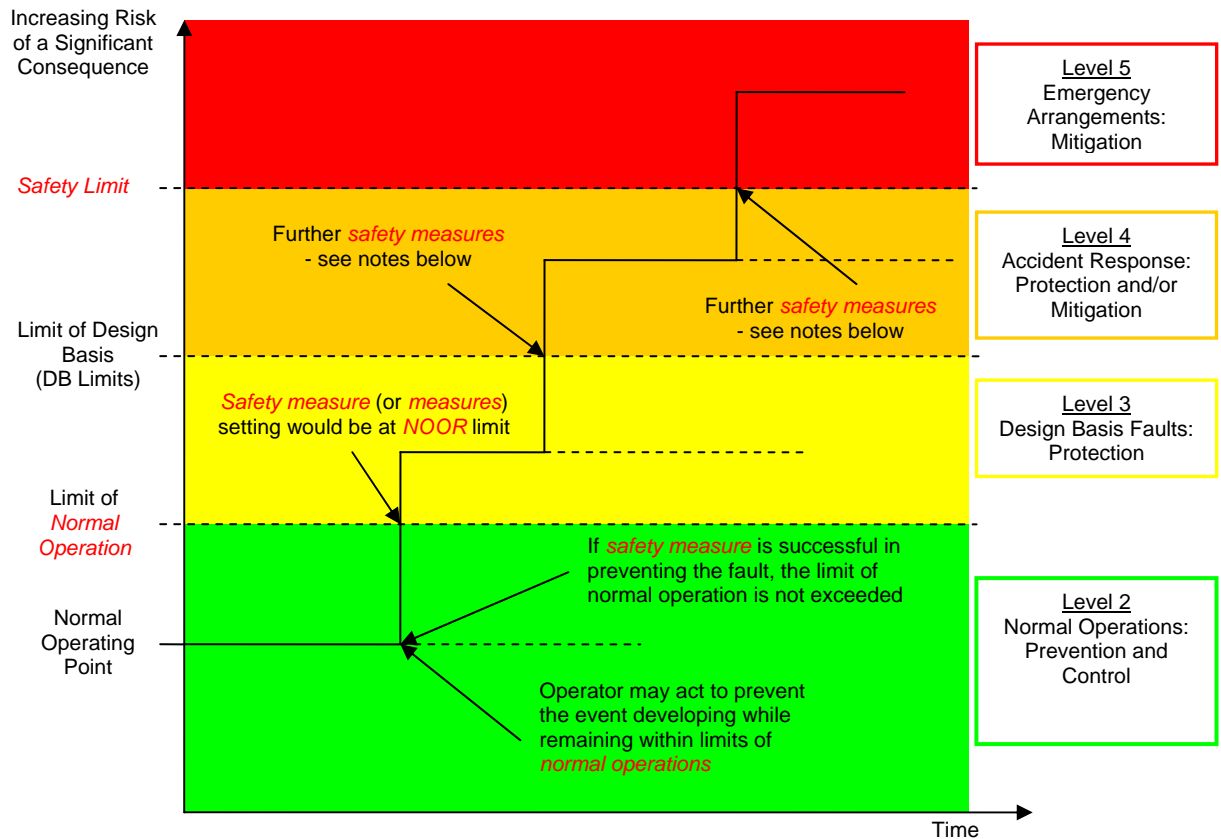


Figure 3: Schematic Illustration of Defence in Depth Approach to Operating Rules for Operations Subject to Step Changes and Preventative Safety Measures

Notes: 1) Where the double contingency principle is applied, there will be limits on at least two independent parameters (e.g. fissile mass and moderator mass). Such limits would both be *NOORs*. The fault progression to exceed both limits is illustrated above as two changes leading to a beyond design basis event. In reality however, both *safety measures* should normally be set at the *NOOR* level.

2) Where the fault progression is measured in terms of a single parameter (such as multiple over-batching of fissile mass) there may be multiple *safety measures* acting at the same point to prevent the progression. Although there may be a further opportunity to prevent the fault being repeated, this would generally take the progression beyond the design basis (e.g. in the example in para 4.38).

4.39. As an example, the analysis of Pu cans in a glovebox might show, with due margin for calculation uncertainties, that four cans may be accommodated, but a fifth can cannot be demonstrated to be safe from unintended criticality. Assuming there is no operational need to process more than one can at a time, a *NOOR* should specify that no more than one can is permitted to be present in the glovebox at any time – this is the first line of defence. The safety case should also identify physical and/or administrative (detection) *safety measures* to protect against multiple cans being present in the glovebox. The *safety limit* should however, be set at four cans, since this is the last point that may be demonstrated to be safe. In this example, the fault of inserting an extra can would need to occur three times-over between *normal operations* and the *safety limit* (so demonstrating fault tolerance – though noting these faults may not be independent). The design basis is that *safety measures* should protect against two cans being present, whilst demonstrating that a failure to do so would be safe (i.e. the DB Limit is two cans).

The DB limit is set to maximise the margin to the *safety limit* whilst allowing the *safety measures* to act without it being exceeded (see para 4.16). *ORs* would be set at Levels 2 (the *NOOR* – one can, defining *normal operations*), 3 (to ensure the availability of *safety measures* which protect against multiple cans being present) and 4 (four cans – the *safety limit*, set relative to the realised hazard). Of these, the *NOOR* (at one can) and the *OR(s)* requiring *safety measures* to protect against multiple cans should be designated as *HHORs*, as these provide the prime (most important) means of fault prevention and protection. The *safety limit* would however be a *LHOR* as it is only indirectly relevant to the operators (e.g. it would only be monitored against in extreme circumstances). Further advice on criticality aspects of safety cases is provided in [8]. The overall picture is illustrated in Figure 4.

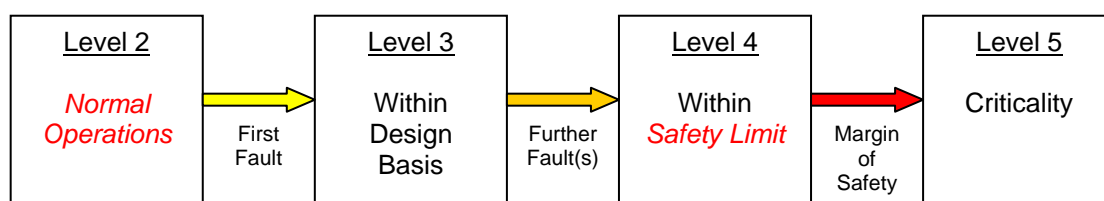


Figure 4: Inter-relationship between the Double Contingency Approach to Criticality and the Defence in Depth Framework

4.40. In some cases, it may not prove reasonably practicable to maintain the margins described in the example above. If the analysis had shown instead that although two cans may be accommodated, a third can cannot be proven suitably safe then, assuming the operation is necessary, and risks demonstrated to be ALARP, the DB limit and *safety limit* would need to be the same. Such a situation would require a robust demonstration of sufficient defence-in-depth, e.g. diverse, independent *safety measures* to protect against multiple cans being present. The *ORs* would be defined in the same way as previously, but the *safety limit* and the DB limit would both be at two cans.

Examples of Typical Operating Rules

4.41. Unlike its predecessors, this guide has not included lists of examples of typical types of limits and conditions for various types of facility. This is because such lists have proved to be of limited value to inspectors while at the same time generating challenges that they are incomplete, e.g. when compared to other guides prepared by other regulators. Inspectors should nevertheless consider whether the coverage of a licensee's *ORs* reflects readily accessible good practice at comparable facilities in other countries. For example, the coverage of the *ORs* identified for nuclear power plants should be compared with the lists provided in [4].

REFERENCES

- 1) Technical Inspection Guide, LC23 Operating Rules, T/INS/023
- 2) "Safety Assessment Principles for Nuclear Facilities", 2006 Edition (Rev 1), HSE, January 2008
- 3) Reactor Harmonisation Working Group Safety Reference Levels. WENRA, 2008, <http://www.wenra.org/extra/pod>

- 4) IAEA Safety Guide: Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants. NS-G-2.2, IAEA, November 2000, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1100_scr.pdf
- 5) Not Used
- 6) Technical Assessment Guide, External Hazards, T/AST/013.
- 7) Technical Assessment Guide, Computer based safety systems, T/AST/046
- 8) Technical Assessment Guide, Control, storage handling and transport of nuclear matter including fissile material, T/AST/041
- 9) Technical Assessment Guide, Periodic Safety Reviews, T/AST/050
- 10) Technical Assessment Guide, Demonstration of ALARP, T/AST/005
- 11) Not Used
- 12) IAEA Safety Glossary; Terminology used in Nuclear Safety and Radiation Protection; 2007 Edition. IAEA, June 2007, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1290_web.pdf
- 13) IAEA Safety Requirement: Safety of Nuclear Power Plants: Operation Safety Requirements; IAEA Safety Standards Series No. NS-R-2, October 2000, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1096_web.pdf
- 14) Safety Series No. 117, Operation of Spent Fuel Storage Facilities, IAEA, 1994, http://www-pub.iaea.org/MTCD/publications/PDF/Pub977e_web.pdf
- 15) Safety Series No. 118, Safety Assessment for Spent Fuel Storage Facilities, IAEA, 1994, http://www-pub.iaea.org/MTCD/publications/PDF/Pub981e_web.pdf
- 16) Safety Guide WS-G-6.1, Storage of Radioactive Waste, IAEA, 2006, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1254_web.pdf
- 17) Technical Assessment Guide, Leadership and Management for Safety, T/AST/078, currently draft
- 18) A guide to the Radiation (Emergency Preparedness and Public Information) Regulations 2001 (L126; ISBN 0 7176 2240 1), HSE Books

ANNEX 1 – Tests for an Operating Rule

The following is a summary of some of the key principles for *ORs*. It has been provided as a quick checklist to aid inspectors' assessment. The content is neither exhaustive nor fulsome – inspectors requiring more detailed guidance should refer to the indicated paragraphs within the main body of this guide.

- *ORs* should be a **condition or limit** and not an instruction [2.2 - 2.5];
- *ORs* (including temporary *ORs*) should be **derived from the safety case** and not from other sources [2.2, 2.3, 4.25];
- The set of *ORs* should be **complete**, so that failing to comply with the safety case entails exceeding at least one *OR* [4.27, 4.26, 4.17];
- The *ORs* should be consistent with the **current, extant safety case** and **systematically reviewed** in the light of operational experience [4.36];
- *ORs* should be **written for the operators** so that compliance can be clearly demonstrated and any non-compliance readily identified [2.3, 2.4, 4.33, 4.20, 4.21];
- *ORs* should be specified in **directly measurable / checkable terms taking account of measurement uncertainties** [4.33];
- *ORs* should be **graded / classified** so that the most important limits and conditions have greatest prominence (i.e. *HHORs*) [1.5 - 1.6, 4.2 - 4.7, 4.32];
- The number of *ORs* (especially *HHORs*) should be **minimised** where possible **by combining similar limits and conditions** [4.6, 4.33 bullet 5];
- *ORs* should be **derived for all Levels of the Defence in Depth Framework** including *normal operations* [4.8, 4.9, 4.10ff];
- The *ORs* should provide **unambiguous definitions of each permitted mode of operation**, which in sum define the extent of *normal operations* [4.11, 4.8, 4.12];
- *ORs* should be provided to ensure the safety of the facility in all its **permitted operating modes**, including start-up, shutdown and temporary situations arising due to maintenance and testing [4.1 (definition of *normal operations*), 4.11, 4.15, 4.24, 4.27];
- The set of *ORs* should **include limits and conditions for plant and system operability, safety settings and the availability of safety measures** [2.7, 4.35, 4.15 - 4.16, 4.9, 4.8, 4.24];
- Compliance with *ORs* **does not necessarily mean risks will be ALARP**; *ORs* will normally be set with a margin to the ALARP operating point [1.12, 4.12, 4.16, 4.29];
- *HHORs* should be **determined primarily through DBA**, but should also include limits and conditions as necessary from all parts of the safety case analysis, and in particular from **engineering analysis, PSA** and (where relevant) **severe accident analysis** [4.28, 4.3, 4.16, 4.9, 4.5, 4.7, 4.23, 4.35];

- *ORs* should include identified **safety limits**, denoting extreme conditions within which the facility can still be shown to be safe [4.19, 4.8, 4.1];
- A subset of the *HHORs* should be identified **for event reporting** purposes. These should ideally reside at the limit of **normal operations** and if not, be chosen with a significant margin to any **safety limit** [4.29 - 4.31, 1.5, 4.37].

ANNEX 2 – Common LC23 Misconceptions

The following list has been compiled to assist inspectors when providing high-level advice in regard to ONR's regulation of LC23. The list is intended to help avoid past misunderstandings and mixed messages from being repeated in future. Each misconception is given in italics, followed by the corrected view:

- *The prime purpose of LC23 is to identify serious adverse circumstances for the purposes of event reporting and notification.* Reality: The prime purpose of *ORs* is to capture requirements and assumptions identified in the safety case in a form that allows the operators to carry out their activities and to control the facility in a safe manner, compliant with the safety case (see LC23(1 and 3)).
- *ONR will normally prosecute following non-compliance with an OR.* Reality: ONR's enforcement decisions will be based upon its Enforcement Management Model (EMM). Key considerations following non-compliance with an *OR* will include the level of hazard, the degree to which the licensee lost control of the facility / process and the extent to which it was culpable for this.
- *ONR will not normally prosecute in the event of non-compliance with a limit or condition identified in the safety case that has not been designated formally as an OR.* Reality: See the previous bullet. Although how the licensee has designated the *OR* will be a factor, especially given that *LHORs* are supposed to guard against lesser hazards, ONR will take appropriate enforcement action commensurate with the circumstances of the non-compliance, irrespective of whether and how the *OR* has been designated.
- *ORs are derived exclusively from the facility's DBA.* Reality: While most *ORs* will likely be derived from the facility's deterministic analysis (which for medium / high risks and hazards should be DBA leading to *HHORs*), the licensee should also seek to identify *ORs* from all parts of its safety case, including the PSA, engineering analysis and (where appropriate) severe accident analysis.
- *Criticality ORs need to be treated differently to other LC23 limits and conditions.* Reality: *ORs* for criticality should be derived and implemented using precisely the same principles as are used for all other *ORs*.
- *Once an operating reactor has been finally shutdown and defuelled, it no longer needs ORs, nor LC23 adequate arrangements.* Reality: ONR expects licensees to identify and implement all the conditions and limits necessary for the safety of their facilities and to classify these accordingly. While defuelling the reactor will remove a significant proportion of the site's hazard potential, *LHORs* will still be needed for the remaining hazards – and potentially *HHORs* too. The licensee's LC23 arrangements need to be

suitable and sufficient for the prevailing risks and hazards at the site so that all necessary **ORs** are identified in the safety case and implemented.

- *ONR would like to see a single approach to **ORs** applied at all UK nuclear facilities.* Reality: This guide sets out ONR's view of good practice following extensive surveys of guidance and application on the derivation and implementation of limits and conditions at nuclear facilities both across UK licensees and internationally. Not all of this guide will be relevant to all types of faults at all facilities. However, licensees will need to justify electing not to apply key aspects of the approach set out here in terms of ALARP. Overall licensees should adopt an approach to **ORs** that serves the best interests of safety at their facilities, uses appropriate terminology that is meaningful to their staff (especially operators) and takes into account international guidance and best practice at similar facilities elsewhere.

ANNEX 3 – Examples of Operating Rules

This annex has been provided to illustrate some of the key concepts described within this guide. It should be stressed that these examples (including the data therein) are entirely hypothetical and have been designed to be illustrative rather than realistic or complete, and to be complementary to one another, e.g. different aspects are stressed in the different cases. Furthermore, no attempt has been made to format these **ORs** into a style meeting good human factors / ergonomic practice.

Example 1 – Power Reactor Loss of Feed

Total loss of feed to boilers is an identified fault within a power reactor safety case with an initiating frequency of more than $10^{-3}y^{-1}$. If no action were taken, the fault could escalate to a major offsite release exceeding 100mSv. Hence applying Figure 1a, **ORs** relating to this fault should be classed provisionally as Tier 3 **HHORs**.

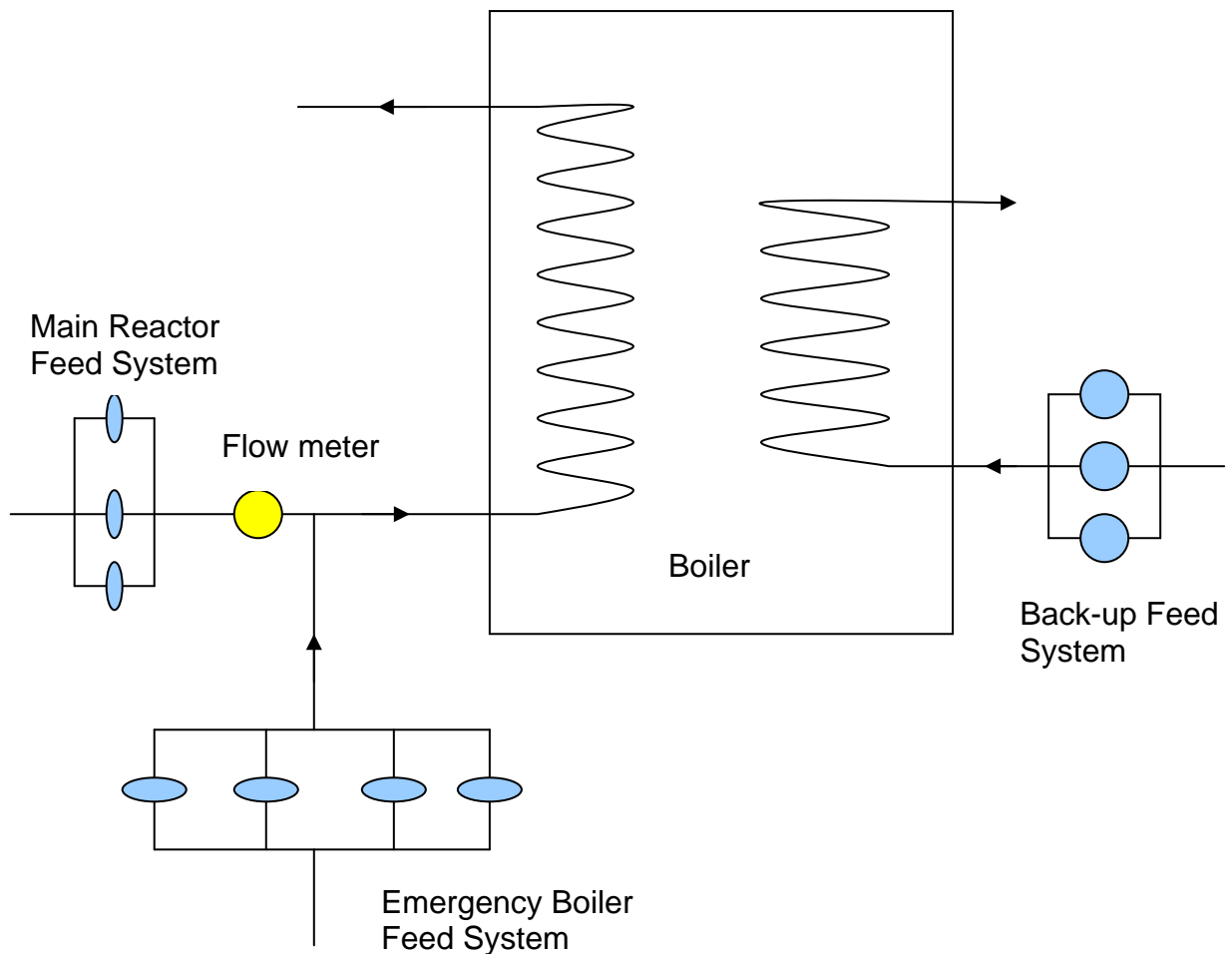
To protect against such faults, reactor trip and emergency feed systems are included within the design (see figure below). The safety case identifies the availability of these systems as necessary for normal operation. **ORs** should therefore be defined governing system settings and plant / equipment availability for these systems to function. For example:

OR-1: For reactor powers above P MW, as measured by equipment XX:

- a) Boiler feed must be maintained above x kg/sec, as measured at flow meter CC, or the reactor tripped within t s.
- b) At least 3 out of 4 Emergency Boiler Feed Pumps must be available.
- c) At least 1 out of 3 Back-up Cooling System Pumps must be available.
- d) No more than 1 out of 3 Back-up Cooling System Pumps may be unavailable for any period exceeding 8 hours.

OR-2: Following a reactor trip, the feed system must be configured to provide at least w kg/s of feed to the reactor within h hours.

OR-3: Fuel temperatures must be maintained below T°C to prevent fuel melt.



Notes

- These **ORs** name the specific equipment. This may however cause the **ORs** to be difficult to read / interpret. Good practice would instead be to set out the limit or condition in plain English, with accompanying clarification of the key terms (e.g. how to measure flows, powers, defining precisely which equipment needs to be maintained available etc) provided in supporting Operating Instructions.
- OR-1 d) is an (admittedly simplistic) example of the Tech. Spec approach to **ORs**. A realistic Tech. Spec would have a cascade of (usually worsening) time-constrained conditions based on PSA, providing operators with definitive limits for how long the safety case considers it safe to remain in a given operational state.
- Analogous additional **ORs** should also be provided for other power conditions, e.g. for when the reactor is shutdown.
- OR-1 a) is an example of a **NOOR**, as it defines part of the boundary between **normal operations** and **fault conditions** for a fault residing in Tier 3 of our hierarchy.
- OR-1 b) to d) form part of the Level 3 defence in depth design basis fault protection. OR-1 thus marks part of the normal safe operating envelope.

- OR-2 is an **OR** forming part of the Level 4 (Accident Response Protection and/or Mitigation) defence in depth. Applying the advice in para 4.6 (assuming that the situation here meets the general criteria stipulated in that para), this **OR** may be demoted to a **LHOR** because: a) OR-1 is a **HHOR** providing an independent barrier to the fault's progression; b) OR-2, as a Level 4 **OR**, makes only a minor contribution to overall safety; c) OR-2 is not in Levels 2 or 3; and d) timescales (at 8 hours) are long here.
- OR-3 is an example of a **safety limit**. As with OR-2, this **OR** may be downgraded to a **LHOR** because it meets the criteria set out in para 4.6.
- Other **ORs** should specify low flow alarm settings designed to alert the operator to possible feed problems in advance of any need to trip the reactor. Such Level 2 **ORs** may also be downgraded to **LHOR** status as they support OR-1.

Example 2 – Dissolving Fuel

Dissolving spent (irradiated) fuel is a continuous operation. For normal operation, a scrubber system, which depends on a sufficient supply of necessary chemicals, notably caustic soda, provides the first line of defence against a release to atmosphere. A filter bank provides a second, independent line of defence. The idealised plant layout is shown schematically below.

A failure, or unavailability of the scrubber system, in tandem with a failure or unavailability of the filter bank could result in offsite releases exceeding 10mSv. The safety case assesses the probability of initiating events leading to such losses or unavailability as exceeding $10^{-4}y^{-1}$, making **ORs** relating to this fault provisionally Tier 2 **HHORs**.

The safety case states that in order to avoid an off-site release, the scrubber system should always be available:

OR-1: The scrubber system must be available and operational while fuel is being dissolved.

The safety case also addresses what “available and operational” means in practice:

- There needs to be a suitable supply of essential chemicals; explicit quantities and types are given based on an assessment of demand in possible fault scenarios;
- The various system components needed for the scrubber to operate are listed;
- The alarm system designed to indicate whether these scrubber system components are fully operational needs also to be in service.

These requirements are defined in a series of supporting **ORs**: **OR-1.1** to **OR-1.n**

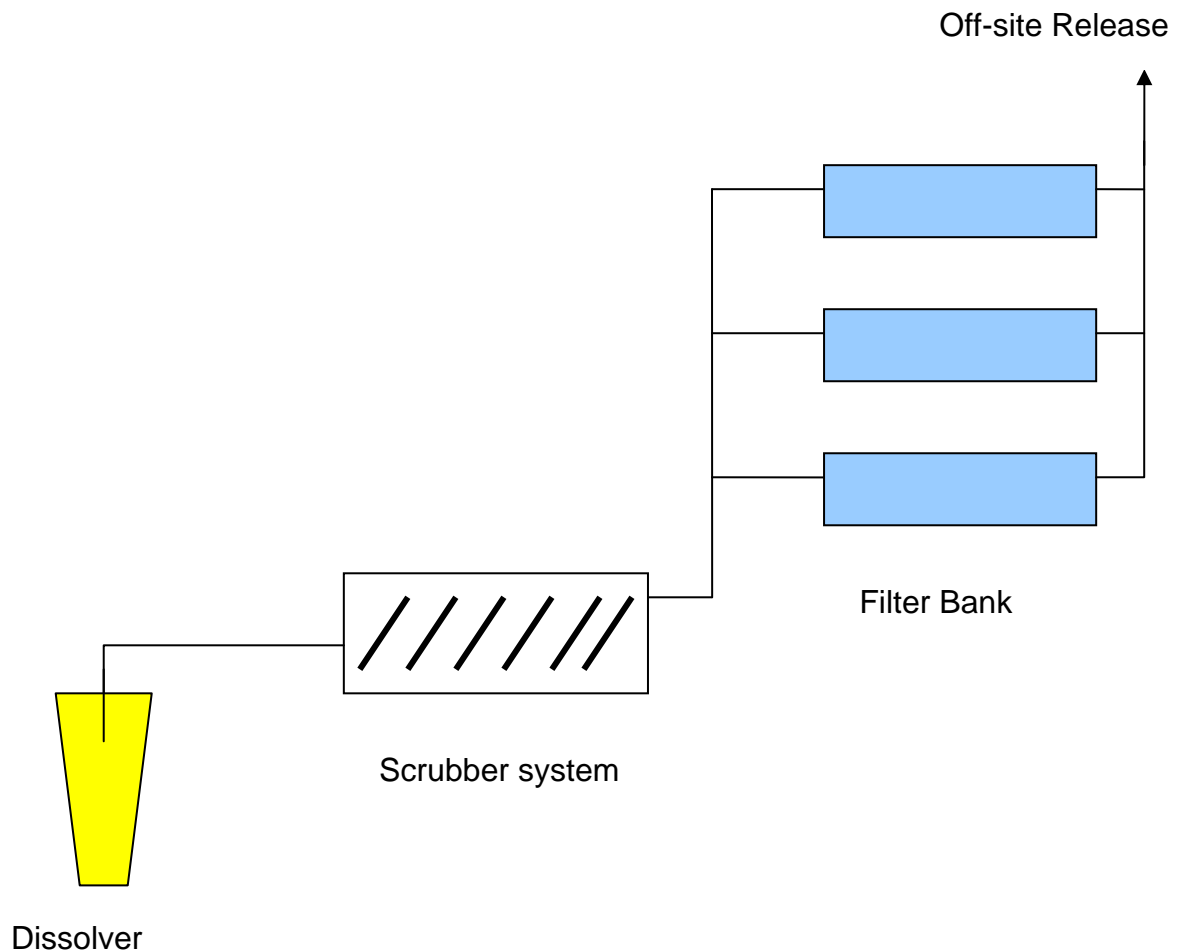
The safety case's PSA assesses that in view of the magnitude of the hazard and the likelihood of initiating events, a second line of protection (the filters) should also always be available. These filters are in a bank; only one needs to be in service to fulfil the design safety function:

OR-2: At least one filter must be available and operational while fuel is being dissolved.

The safety case addresses what “available and operational” means in practice, noting that an accumulation of more than x kg of dust would limit flows to an extent

that its safety function would no longer be fulfilled. Conservative assessments are then used to show that provided the filters are replaced at least every Y operational years (i.e. years in flow operation), this quantity of dust cannot accumulate.

OR-2.1: Filters in system ZZ must not remain in service for more than Y operational years.



Notes

- The fault sequences that these **ORs** relate to make these candidates for Tier 2. However, OR-1.1 to OR-1.n and OR-2.1 are supporting limits and conditions to the parent rules OR-1 and OR-2. Following the guidance in para 4.6, and applying the other criteria therein, these **ORs** may be demoted to Tier 1 (**LHORs**), and should be placed in the OIs “necessary to ensure any **ORs** are implemented” (LC24) – see para 4.3. OR-1 and OR-2 would however remain Tier 2 **HHORs** in view of the risks and hazards they protect against.
- Even though OR-1.1 to OR-1.n and OR-2.1 would only appear in OIs, there is still a need for further instructions to show how compliance with these **LHORs** will be demonstrated, either in the same OI or in other OIs.
- OR-2.1 could have been phrased in terms of the mass of dust in the filters, or the minimum “Decontamination Factor” (DF) that the filters need to provide. However, neither of these alternatives would be particularly meaningful to the operators, and would present challenges in the demonstration of compliance, i.e. they would not be “straightforward” – see para 4.33.

- Similarly OR-2.1 could have been written as an instruction to change the filters at a certain frequency. A state-based **OR** is preferred for the reasons given in paras 2.5 and 1.8.
- Unavailability of the scrubber system might occur faster than dissolving operations could reasonably and safely be shutdown. Hence, a more sophisticated **OR** to OR-1, as per the Tech. Spec example above, setting a maximum time to shut down the system might be preferable. However, such an approach would only be appropriate if supported by suitable analysis of dissolver shutdowns within the safety case.
- Likewise a Tech. Spec approach could be followed for OR-2, i.e. an **OR** setting maximum times that a dissolver may be operated with just one, or just two available filter banks without the need to initiate a controlled shutdown.
- The need for two lines of protection is an example of how PSA can lead to **HHORs**, rather than just through DBA. The criteria for identifying which **ORs** should be considered to be **HHORs** should nevertheless be consistent with the licensee's DBA methodology – para 4.3. Alternatively, the licensee's DBA rules (e.g. in terms of redundancy) might also have led to the safety case seeking two independent lines of protection.

Example 3 – Glovebox for Sampling Plutonium-Bearing Liquors

A leak within a glovebox handling a continuous flow of Plutonium Nitrate (PuN) liquor could lead to a build-up of liquor that, if not stopped, could result in a criticality event with fatal doses to any operators nearby. In view of this, the safety case identifies the need for two **safety measures**: a flow shut-off control valve linked to liquor monitoring devices in a sump and an overflow to divert leaking liquor to a geometrically safe holding tank (i.e. a predominantly passive safety system). The glovebox layout is shown schematically below.

In view of the likelihood of leaks, and the consequences of a criticality (which would exceed 500mSv), the **ORs** relating to this fault should provisionally be classed as Tier 2 **HHORs**.

Other processes undertaken in the glovebox mean that small volumes of other liquids could also accumulate in the sump without posing a safety concern. The safety case thus defines a non-zero sump level X mm, below which liquor levels will be deemed part of **normal operations**:

OR-1: Liquor levels in Sump ZZ will be maintained below X mm.

Accumulations of liquor above X mm are thus classed as a **fault condition** in the safety case. The shut-off valve protecting against this fault is set to trigger if the liquor level increases to Y mm.

OR-2: While Glovebox XX is receiving PuN liquors, Flow Control Valve YY must be maintained available to shut-off the PuN flow whenever liquor levels exceed Y mm as measured in Sump ZZ.

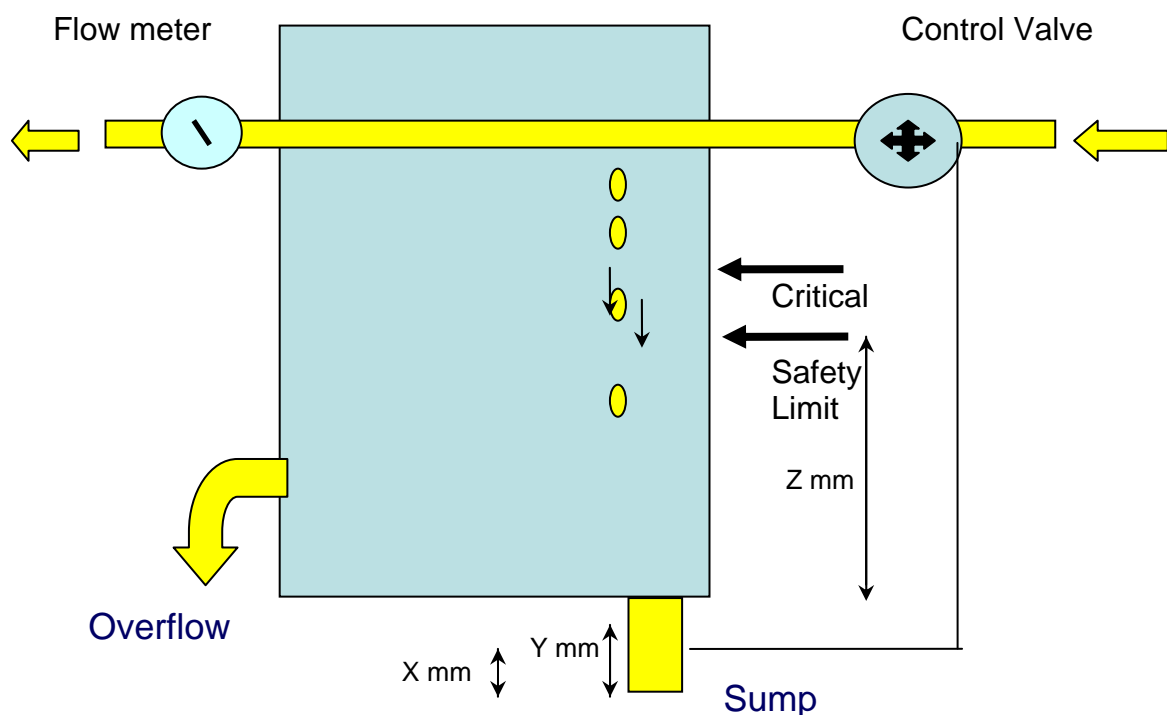
The safety case argues that the protection offered by the flow shut-off system provides suitable and sufficient protection to meet the licensee's DBA and PSA criteria. However, it is deemed reasonably practicable and in line with good practice to install a second **safety measure** – the overflow. The overflow is a predominantly passive system, and so need not be subject to an availability **OR**. However, the safety case notes the overflow is of limited size and so can only be

substantiated to perform its safety function if the process liquor flow is maintained below $W \text{ m}^3/\text{s}$:

OR-3: Flow of PuN measured at Flow meter WW must be no greater than $W \text{ m}^3/\text{s}$.

Conservative criticality calculations within the safety case demonstrate that a criticality cannot occur for liquor levels below $Z \text{ mm}$ above the base of the glovebox:

OR-4: To ensure adequate margins to criticality limits, liquor levels in Glovebox XX must be maintained below $Z \text{ mm}$, measured from the glovebox base.



Notes

- The phrase “predominantly passive” has been used since the overflow’s safety function relies on the process flow being kept below $W \text{ m}^3/\text{s}$.
- Despite the large doses that could arise, these **ORs** are classified provisionally as Tier 2 (and not Tier 3) **HHORs** as there is no Tier 3 criterion in Figure 1b or para 4.3 for on-site consequences.
- OR-1 is a **NOOR**, i.e. at Level 2 in the SAPs Defence in Depth hierarchy (SAP EKP.3ff), and defines where **normal operations** end and **fault conditions** begin. Normally the **NOOR** would be supported by an alarm set so that the operators could respond manually in the event of liquor accumulating in the sump before the automatic **safety measure** responded. The level $X \text{ mm}$ should be set ALARP taking account of the likelihood and magnitude of non-Pu bearing liquors being present in the sump.
- OR-2 defines a Level 3 **safety measure** needed to protect against leakage faults. The wording of the **OR** allows the control valve system to be out-of-

service without contravening the **OR** provided glovebox flows are already stopped. The wording also permits the equipment to be set to operate lower than Y mm; indeed setting lower is good practice to cater for possible instrument drift (another way of contravening this **OR**).

- The choice of Y should include a margin above the **NOOR** (X mm) in order to avoid inadvertent initiation/activation of the control valve (see para 4.15), but also ALARP to minimise the extent of any unintended leaks.
- OR-3 in this example is a Level 4 **safety measure**, as the licensee decided, based on its DBA, PSA criteria and engineering standards, not to claim this within the (design basis) Level 3 protection. The overflow is however, a predominantly passive system and so resides higher in the SAPs EKP.5 hierarchy than the control valve. Hence, the safety case should justify that this (and not the valve) is appropriate as the prime defence for Level 3.
- No **OR** has been set to denote the design basis limit (i.e. marking the transition between Levels 3 and 4) in this example since there is no suitable means of measuring liquor levels above the sump. Y mm could potentially have been used for this purpose, but for the delay between shutting off the process flow and stopping the leak, which the safety case assesses could take liquor levels beyond Y. **ORs** should, in general, only be specified in directly measurable / checkable terms (para 4.33, but see also next bullet). It may not always be reasonably practicable to set design basis limits that will be useful to the operators.
- OR-4 could have been specified in terms of the volume of Pu build-up, or the number of mN (milli-Niles) to criticality. However, neither of these would have been meaningful to the operators. OR-4 is an example of a **safety limit** (see paras 4.1 and 4.19) and marks the limit beyond which the safety case has not, or cannot, demonstrate safety. Such **ORs** can rarely be measured or checked directly with any degree of confidence; their presence in the safety case is usually to specify a success criteria that earlier defences need to achieve. From an operational perspective, the prime application of **safety limits** is to inform (and potentially to act as triggers within) the emergency arrangements and accident management strategies. In this instance, the licensee's emergency arrangements should be triggered if there was concern that a continuing leakage flow might overwhelm the overflow.
- Following the guidance in para 4.6, OR-3 and OR-4 could be downgraded to Tier 1 **LHORs** since they make only a minor contribution to nuclear safety compared to other (Level 2 and 3) barriers. This is because both are deep into the Defence in Depth hierarchy (Levels 4 and 5) and OR-4 has only indirect relevance to how the operators operate the glovebox.