|  |
| --- |
|  |
| ONR Technical Assessment Guide  Limits and Conditions for Nuclear Safety (Operating Rules) |



ONR Technical Assessment Guide (TAG)

Limits and Conditions for Nuclear Safety (Operating Rules)

Authored by – Fault Studies Specialist Inspector

Approved by – Professional Lead for Fault Analysis

Issue No.: 7

Publication Date: Mar-23

Next Major Review Date: Mar-28

Doc. Ref.: NS-TAST-GD-035

Record Ref. No.: 2020/262101

Revision Commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| Issue 7 | Updated to provide greater readability, ensure alignment with extant international guidance and reflect current regulatory permissioning approach. |

Contents

[1. Introduction 4](#_Toc121986315)

[2. Purpose and Scope 4](#_Toc121986316)

[3. Relationship to Licence and other Relevant Legislation 4](#_Toc121986317)

[4. Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides 6](#_Toc121986318)

[5. Advice to Inspectors 10](#_Toc121986319)

[References 21](#_Toc121986320)

[Glossary and Abbreviations 23](#_Toc121986321)

[Appendix 1 – Tests for Operating Rules 24](#_Toc121986322)

[Appendix 2 – Common Misconceptions 25](#_Toc121986323)

[Appendix 3 – WENRA Safety Reference Levels of Relevance 27](#_Toc121986324)

[Appendix 4 – Technical Specifications for Nuclear Power Plants 29](#_Toc121986325)

[Appendix 5 – Operating Rules and Defence in Depth 31](#_Toc121986326)

[Appendix 6 – Criticality Safety Operating Rules 34](#_Toc121986327)

# Introduction

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

# Purpose and Scope

1. This TAG provides advice to inspectors when considering the 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 and assists in judging the adequacy of safety case implementation and Licence Condition (LC) 23 related compliance inspections. It also provides guidance to aid regulatory decision making when assessment includes consideration of whether limits and conditions have been adequately derived and underpinned in the safety case.
2. Licensees use a range of terminology for limits and conditions such as operating rules (OR), technical specifications, key safety management requirements, etc. This guide focusses on the methods used by licensees to derive such limits and conditions. ONR’s Technical Inspection Guide [2] also provides further guidance. Both guides complement one another in helping ONR inspectors exercise their regulatory judgment.
3. A summary of the key principles discussed in this guide is presented in Appendix 1 and guidance on common LC23 misconceptions is provided in Appendix 2.

# Relationship to Licence and other Relevant Legislation

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

**Licence Condition 23 – Operating Rules**

**Licence Condition 24 – Operating Instructions**

1. 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 and in accident conditions. LC23(1) further states that such limits and conditions shall be referred to as operating rules, therefore within this TAG the term ORs is used consistently with this definition.
2. LC23(3) requires the operator to ensure that operations at the facility comply with these constraints at all times. Compliance inspection guidance is provided in [2]. Inspectors should note that the intent of LC23 is to link the analysis, assumptions and boundary conditions documented in the safety case with actual operational limits and conditions in force at the facility. The limits and conditions derived in the safety case therefore need to be stated in a way 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. This will be discussed in more detail in Section 5.
3. LC23(3) also requires the licensee to take appropriate action in the event of exceeding these limits and conditions. Such incidents should be recorded, investigated, and reported in accordance with arrangements made under LC7. Hence, licensees’ safety cases should include detailed planning and analysis to cater for potential incidents and utilise learning from experience to prevent repeat events.
4. The requirements of LC23 apply to any condition or limit appearing (explicitly or implicitly) in the licensee's safety case. This requirement applies 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).
5. LC24(2) requires licensees to implement instructions to ensure that the limits and conditions identified under LC23(1) are complied with. Hence, the licensee should be able to demonstrate that its administrative controls and procedures are designed and implemented such that they support reliable human performance of actions that keep the plant within the safe operating envelope.
6. In addition, LC27 (Safety Mechanisms, Devices and Circuits) places a duty on the licensee not to operate, inspect, maintain and test its facility unless sufficient safety mechanisms etc., are properly connected and in working order. It follows that this should be in accordance with limits and conditions relating to the design (suitability and sufficiency), availability (connectedness) and condition (working order) of such 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 discussed in [2].
7. 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 (such as HSWA (specifically ALARP requirements), MHSWR Regulations 3 and 5, REPPIR, IRRs etc).

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

## Safety Assessment Principles

1. The principal SAPs [1] with direct relevance to this guide are summarised below.
2. SAP SC.6 seeks safety cases that identify operating conditions and limits to ensure the facility is kept in a safe condition. SC.6 para 106 also expects that safety cases justify how any requirements will be implemented effectively. It follows that the conditions and limits therein must be usable by the operators to be effective. FA.9 (para 643) provides guidance on how to identify conditions and limits in practice, suggesting that these should be derived from the design basis analysis (DBA). Para 643 identifies three types of limits and conditions: safety 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 152), 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. FA.14 also states that appropriate use of Probabilistic Safety Analysis (PSA) should be made in the setting of ORs, and FA.16 states that Severe Accident Analysis (SAA) should be used to identify any further reasonably practicable preventative or mitigating measures beyond those derived from DBA and PSA.
3. The Engineering SAPs provide detailed guidance on the measures that should be taken in the design and operation of the facility. 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 (ESR.4). The engineering SAPs also recognise the vital role played by the operators in ensuring the safe operating envelope is maintained; and the need for systematic analysis to identify and design such administrative controls (EHF.4).
4. SAP SC.8 states that ownership of the safety case, including any limits and conditions derived from it (para 112), should reside with those in the duty-holder’s organisation who have direct responsibility for safety. In practice, responsibility for compliance with limits and conditions falls to the duly authorised persons (DAPs) who are responsible under LC12 for plant safety.
5. Other SAPs[[1]](#footnote-2) refer to safety limits and conditions. These references are of secondary or duplicated relevance to this assessment guide, and so are not discussed directly. In principle, many SAPs relate to limits or conditions within the safety case, and thus to an operational limit or condition on the plant.

## WENRA Reference Levels

1. The objective of the Western European Nuclear Regulators Association (WENRA) harmonisation programme is to develop a common approach to nuclear safety in Europe. They achieve this by comparing national approaches to the application of IAEA safety standards. The 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 SRLs. Hence, inspectors should consider them relevant good practice (RGP) in keeping with ONR’s guidance on the demonstration of ALARP [3].
2. This guide has drawn from the WENRA SRLs for existing reactors 2020 [4]. In particular Issue H which addresses operational limits and conditions at civil nuclear reactors. It has also drawn from the decommissioning and storage reference levels [5 & 6]. A tabular summary of how WENRA Safety Reference Levels covered in this TAG is presented in Appendix 3.
3. SRLs related to the implementation of limits and conditions, rather than to their derivation, have been identified in [2], rather than this TAG.

## IAEA Safety Standards

1. The IAEA safety standards (requirements and guides) were used as a benchmark for the SAPs in both the 2006 and 2014 Editions and are recognised by ONR as RGP. This guide has similarly been written to reflect IAEA safety standards and requirements. The General Safety Requirements publication “Safety Assessment for Facilities and Activities” Requirement 4 [7], defines the purpose of safety assessment (undertaken by the licensee) and includes the statement:

The safety assessment has to include an assessment of the provisions in place for radiation protection, to determine whether radiation risks are being controlled within specified limits and constraints, and whether they have been reduced to a level that is as low as reasonably achievable.

1. It goes on to provide further detailed guidance, including on the need to determine whether:

* the procedures and safety measures necessary for implementation of the operational limits and conditions ensure an adequate level of safety (Requirement 11); and
* adequate provisions have been made at each level of Defence in Depth (Requirement 13).

1. The Specific Safety Requirements publication “Safety of Nuclear Power Plants: Design” [8], states the expectation that the design shall establish a set of operational limits and conditions for safe operation (Requirement 28), whilst “Safety of Nuclear Power Plants: Commissioning and Operation” [9], states the expectation that the plant is operated in accordance with those operational limits and conditions (Requirement 6). The parallel Specific Safety Requirements publications “Safety of Research Reactors” [10] and “Safety of Nuclear Fuel Cycle Facilities” [11] have similar expectations. The guidance for inspectors provided by the relevant SAPs and this TAG is consistent with these IAEA requirements.
2. The IAEA has a Specific Safety Guide “Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants” (SSG-70) [12], which provides more detailed guidance on how limits and conditions should be derived and implemented. Strictly speaking, SSG-70 [12], applies only to Nuclear Power Plants; however, the guidance it contains should be recognised as being applicable to other types of nuclear facilities (noting reference to NS-G-2.2[[2]](#footnote-3) in IAEA’s radioactive waste store guidance (WS-G-6.1) [13]). SSG-70 is also consistent with the approaches set out for spent fuel facilities in SSG-15 [14]. It also underpins the fundamental structure for limits and conditions implied within IAEA’s Safety Glossary [15]. SSG-70 has therefore been used in this TAG as a source of general guidance applying to all types of nuclear facilities.
3. Guidance regarding limits and conditions is also provided in other IAEA safety guides and standards, with respect to specific types of facility and situation. This guide has therefore been written with due cognisance of, and consistent with, those safety standards listed in Table 1, below. Whilst inspectors should be aware of these other sources of guidance, consideration of specific guides is likely to be of most benefit when applied to the specific type of facility and situation they relate to.

Table 1 - Summary of Relevant IAEA Safety Standards

|  |  |  |
| --- | --- | --- |
| Document | Title | Published |
| GSR Part 4 | Safety Assessment for Facilities and Activities (Rev. 1) | 2016 |
| SSR-2/1 | Safety of Nuclear Power Plants: Design (Rev. 1) | 2016 |
| SSR-2/2 | Safety of Nuclear Power Plants: Commissioning and Operation | 2016 |
| SSR-3 | Safety of Research Reactors | 2016 |
| SSR-4 | Safety of Nuclear Fuel Cycle Facilities | 2017 |
| SSG-70 | Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants | 2022 |
| SSG-15 | Storage of Spent Nuclear Fuel (Rev. 1) | 2020 |
| SSG-20 | Safety Assessment for Research reactors and Preparation of the Safety Analysis Report | 2012 |
| SSG-25 | Periodic Safety Review for Nuclear Power Plants | 2013 |
| SSG-27 | Criticality Safety in the Handling of Fissile Material | 2014 |
| WS-G-6.1 | Storage of Radioactive Waste | 2006 |

# Advice to Inspectors

## Introduction

1. As discussed in section 3 above, LC23 requires the licensee to produce an adequate safety case and identify all the limits and conditions necessary to ensure the safety of the facility during normal operation and in accident conditions.
2. Here the term ‘safety case’ should be interpreted as per the SAPs Glossary and not just how the licensee defines this term, i.e.:

“The totality of a licensee’s (or dutyholder’s) documentation to demonstrate safety …”.

1. Inspectors should be aware that the terminology employed in a licensee’s safety case for limits and conditions may refer to both ORs and LC24 operating instructions, without specific distinction between them. It is therefore important to recognise that what is (or is not) an OR is defined by LC23, rather than by the terminology that the licensee employs.

## Types of Operating Rules

1. Inspectors should expect to see a variety of types of limits and conditions arise from a dutyholder’s safety cases[[3]](#footnote-4). These would normally include, but not necessarily be limited to:

* **Parametric**: Defining the boundaries between Defence in Depth Levels (e.g., normal operations, fault conditions, etc.) in terms accessible to the operators. This may include notification and reporting arrangements if breached (see LC23(3)).
* **Operational**: Defining minimum levels, and permitted configurations, of plant and equipment (including associated supplies). This also covers the minimum staffing levels identified by the safety case to ensure adequate protection and monitoring in all permitted modes of operation.
* **Protective**: Set point limits and conditions defining where safety measures are intended to be activated / initiated to protect against or mitigate fault consequences.
* **Time-based**: Defining surveillance requirements such as frequencies and circumstances. For monitoring compliance against each OR, the allowed time-periods when safety measures are permitted to be unavailable or temporarily substituted by other measures, and the time periods within which operators need to complete identified activities.
* **Theoretical**: Physical or safety limits based on the prevention of unacceptable releases of radioactive materials from the plant through the application of ultimate limits (such as temperatures, coolant pressure, pressure boundary integrity or other operational characteristics influencing the release of radioactive material from its place of confinement).
* **Underlying**: Ensuring that other assumptions made in the safety case are captured.

1. This guide has not included lists of examples of typical types of limits and conditions for various types of facility. This is because it is judged that such lists are of limited value given the wide range of ORs that may be applicable to the facility in question. However, inspectors should still consider whether the coverage of a licensee’s ORs reflects RGP at comparable facilities (both nationally and internationally). A recommended starting point for nuclear power plants is to compare with the examples provided in [12].

## Derivation of Limits and Conditions

1. Many ORs are derived from the facility’s deterministic safety analysis, and inspectors should focus regulatory attention on those identified via DBA as they are likely to be the most significant (see FA.9 and supporting text). Use of DBA should ensure that there will be sufficient margins of conservatism between the limits applied and the point where there is a threat to safety. In particular, DBA should:

* determine limits of normal operation, safety settings, design basis limits and (in conjunction with the engineering analysis) safety limits.
* inform the required availability of safety measures; and
* provide significant insight against the expectations of the Defence in Depth framework.

1. However, the safety case should not limit the derivation of ORs to DBA. ORs should also be derived from PSA (if it exists for the facility), the engineering substantiation[[4]](#footnote-5) and other parts of the safety case (such as SAA for example) as appropriate. PSA will be particularly important in determining ORs governing the availability of safety measures and be a key input to holistic reviews of ORs. Consideration should also be given to PSA outputs in determining Examination, Inspection, Maintenance and Testing (EIMT) related ORs and proof test intervals for example. In addition, the PSA will normally be the principal source for deriving time-based ORs, those relating to allowed substitution periods and the unavailability of safety measures, so that any periods of elevated risk may be suitably justified.
2. The engineering substantiation is a prime input to the DBA (in determining safety limits). It is also a source of ORs in its own right. For instance, the engineering substantiation should (among other things) 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 activities; cater for plant ageing and corrosion effects; and set ORs relating to equipment qualification.
3. 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. Recognising that management discretion may be part of a licensee's safety management systems, Inspectors should nonetheless encourage the licensee to a position where its safety case and ORs are in full alignment.
4. ORs link the safety case analysis and assumptions with actual operational limits and conditions in force at the facility. Hence, ORs should be written for use by the operators. It is the operators who will need to apply them, rather than other interested parties (e.g., fault analysts, design engineers or regulators) and be worded so that the operators can easily demonstrate compliance.
5. The set of ORs should include limits and conditions on the minimum availability of safety measures. Such ORs should be provided to ensure that for each fault addressed in the safety case, there are identified lines of protection in place. These should be shown by analysis to be suitable and sufficient to protect against the fault and be covered by explicit arrangements to ensure that they are being delivered or will be available when needed.
6. The safety case should explain any availability constraints on identified safety measures and justify any substitution arrangements that may be proposed. Where any such substitution arrangements provide a reduced degree of protection than the normal arrangements, the ORs should limit the maximum duration over which these may be applied. ORs that relate to the availability of safety measures should also specify when activities need to be stopped in the event of unavailability. The duration should be as short as reasonably practicable, taking account of the risks of shutting down the process and be justified in the safety case via PSA or other appropriate analysis. The OR should be worded so that enacting any such substitution arrangements or stopping the process within the respective justified timeframes would not breach the OR. Civil nuclear power plants adopt this approach by applying Technical Specifications (Tech Spec), which are discussed in more detail in Appendix 4.
7. 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. For example, 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. Here the implementation arrangements need to reflect the nature of the OR, and what the licensee would do in the event of non-compliance. Inspectors should therefore be alert to the need to capture underlying safety case assumptions as ORs. Inspectors should also consider whether the manner in which such ORs are implemented is commensurate with the risks arising if they were to be exceeded.
8. Inspectors assessing the adequacy with which ORs have been identified in a safety case submission or inspecting how they have subsequently been implemented on the facility should consider the breadth of their sample and whether adequate account has been taken of:

* all the permitted operating states of the facility;
* all identified sources of hazard;
* all identified fault sequences;
* all levels of Defence in Depth listed in SAPs paras 152ff. (The ORs should form a sufficiently complete set such that it is not possible to pass from one level of the Defence in Depth hierarchy to another without contravening at least one OR);
* all the types of ORs listed at para 29;
* all the plant and equipment claimed in the safety case, including the range of operability within which they will need to perform safety functions, and the resources and services required; and
* all human-related claims made in the safety case (e.g., minimum staffing requirements such as numbers, specific Suitably Qualified and Experienced Persons (SQEP) and locale.

1. It is vital that, when deriving ORs, licensees pay attention to how they will be implemented to ensure clarity. When considering the adequacy of what the licensee has proposed, inspectors should judge the proposed ORs against the following considerations:

* **Meaningful**: The ORs need to be defined in terms meaningful to the facility operators. For instance, a reactor safety case may analyse 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 then translate these limits into appropriate 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.
* **Unambiguous**: Clear presentation and avoidance of ambiguity are important contributors to reliability in the use of ORs. Hence, human factors advice should be sought at an early stage in the development of the documentation in which the ORs will be presented to the operating personnel. The meaning of terms should be explained to help prevent misinterpretation and there should be no debate as to what compliance means for a given OR.
* **Simple**: Licensees should seek to define ORs that are as simple as possible for the operators to comply with. Complicated ORs involving multiple parameters should normally be avoided. For instance, a criticality limit may be a function of several factors such as enrichment, moderator, reflector, mass and configuration. While it may be legitimate for the OR to be written to cater for all the various 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 Type *X* container may be located in Glovebox *Y* at any time”, rather than a more complicated limit involving mass and proximity.
* **Constraints**: Inspectors should note the distinction between limits and conditions, and instructions. Limits and conditions are constraints on how the facility must be operated. Instructions 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 an instruction prohibiting operators from adding more than a certain number would not.
* **Practicable**: The safety case should demonstrate that all the management controls associated with OR compliance are achievable. Where safety measures are enacted / initiated by the operators, it should be substantiated with sufficient evidence that they can be undertaken to the quality and within the timescales assumed in the safety case. Licensees should therefore ensure early consultation between the safety case authors, operators and HF experts, and continued iteration as the case is developed.
* **Holistic**: To avoid an unreasonably large number of ORs, a least common denominator approach should be applied. If one OR can provide a reasonably practicable bounding limit or condition that can cover 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 flasks, 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 flasks handled. In such cases it is important that the safety case demonstrates that the universal OR is bounding for all the relevant fault scenarios.
* **Manageable**: The personnel responsible for ensuring compliance with the OR should be identified. ORs should be within the capacity and capability of those who are responsible for maintaining them and avoid complexity so far as is practicable. Safety cases should therefore include suitable and sufficient human factors analysis to demonstrate that there will be sufficient resource available at all times to maintain compliance with the applicable ORs. This should take account of the timescales required for operator action) and then set ORs to ensure these staffing levels are maintained. Specific ONR guidance on these aspects is provided in NS-TAST-GD-060 [16].

1. 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). Changes to ORs required by the safety case should be implemented as soon as is reasonably practicable. If the extant ORs no longer represent the revised safety case for a period of operation, this position should be justified i.e., it should be shown that stopping operation is not reasonably practicable in the interim. It may be the case that a facility cannot be shut down, for example a waste store. However, in such cases, appropriate additional temporary ORs and suitably robust controls which are substantiated proportionately may be reasonably practicable.
2. It may occasionally be necessary for a licensee to modify ORs on a temporary basis. For example, to perform physics tests on a new reactor core. In such circumstances particular care should be taken by the licensee to ensure that the effects of the change are appropriately analysed, and to demonstrate the controls are adequate. Should the risk from the modification be significant (for example, if categorised as such by the licensee), inspectors may choose to consider whether the modified state is justified by at least the same level of licensee analysis, substantiation and approval as a permanent modification. When a reasonable alternative approach is available to the licensee, this should be preferred to a temporary modification of an OR. Probabilistic methods or reliability analysis may provide inspectors with valuable insights for the purpose of making judgements in such situations.
3. The licensee's process for deriving ORs should recognise that compliance with ORs is only part of what is required to keep risks as low as reasonably practicable (ALARP). This is because ORs are conditions and limits necessary in the interests of safety. These ORs define compliant operation (e.g., a safe operating envelope) within which risk levels have been shown to be acceptable. Inspectors should recognise that they do not define the optimal point residing within that envelope (e.g., the normal operating point)[[5]](#footnote-6). The safety case should therefore not only seek to determine a suitable and sufficient set of ORs defining the safe operating envelope 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 employ.

## Operating Rule Hierarchy

1. 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 should be applied to the identification and implementation of conditions and limits with the greatest importance to safety. A licensees’ safety case methodologies may therefore employ a graded approach to categorising ORs. Such grading should be appropriate to the risks and hazards present if the relevant OR was to be breached. The grading also needs to ensure that, when implemented, all ORs will be given a suitable and sufficient degree of attention by the licensee. As such, the licensee’s safety case methodology should provide sufficient information to allow the ORs that are most important to safety to be readily identified.
2. This guidance does not prescribe a method for how ORs should be graded; licensees need to employ an approach that is appropriate to their situation, and which should be consistent with a robust DBA methodology cognisant of ONR’s design basis target (Target 4). The position within the hierarchy should be assigned considering:

* the unmitigated consequence of non-compliance with the OR;
* the overall likelihood that the OR will be challenged; and
* the extent to which the OR is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults.

1. As such, the position of the OR within the licensee’s grading structure is likely to be closely linked to the categorisation of the safety function which the OR is delivering. ONR’s expectations for determining the categorisation of safety functions and classification of SSCs is described within NS-TAST-GD-094 [17], which proposes a three-tier approach to the categorisation of safety functions. Inspectors should be aware that alternative approaches to safety function categorisation may be developed and demonstrated to be fit for purpose.

## Operating Rules and Defence in Depth

1. SAP EKP.3 and its supporting guidance states that the design and operation of nuclear facilities should adopt a Defence in Depth approach. That is, a series of defences aimed at ensuring faults do not escalate into significant consequences. As far as is practicable, these defences should be independent of one another. SAPs paras 149 - 153 and Table 1 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.
2. Figure 1 illustrates the Defence in Depth approach to ORs with the transient response of a typical parametric limit during a fault scenario (temperature, system pressure etc). 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 (noting that Level 1 of the SAPs’ hierarchy relates to how the facility is designed rather than how it is operated). Indeed, at some facilities it may not be possible for the licensee to set ORs at all levels. Further guidance on appropriate ORs at each level is provided in Appendix 5.
3. Previous issues of this TAG provided specific guidance with regards to criticality limits and conditions, recognising that faults of this nature rely purely on preventative measures (i.e., Levels 2 and 3). Guidance on the application of criticality safety considerations to ORs has been retained, to demonstrate how they may be derived and implemented. This is presented in Appendix 6.

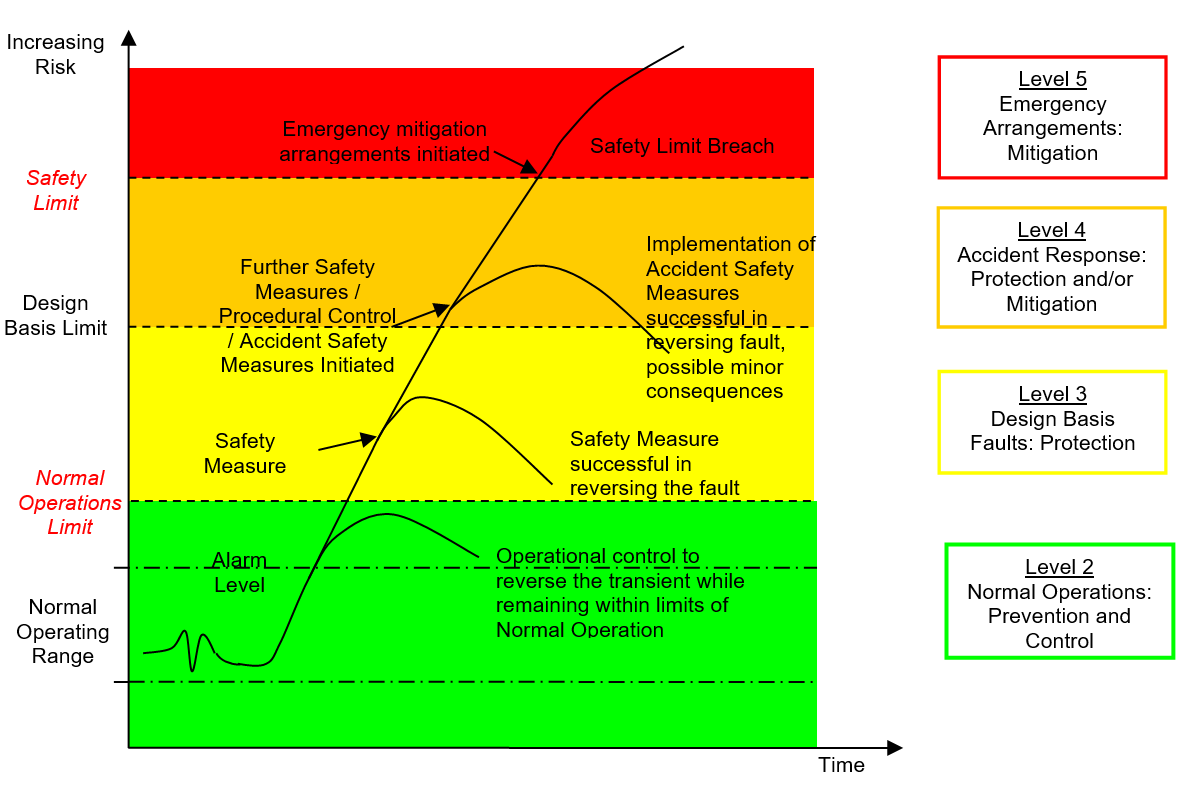


Figure 1 – Schematic Illustration of Defence in Depth Approach to Operating Rules

## Operating Rule Surveillance / Compliance

1. To ensure that limits and conditions are met at all times, the licensee should have an appropriate surveillance programme in place that supports operating personnel in ensuring compliance with the relevant ORs. This surveillance programme should include required inspections, checks, calibration, testing, etc. Further guidance to inspectors on OR surveillance and compliance is provided in [2].
2. Surveillance requirements, or their equivalent, should be identified and linked to ORs. These requirements should include the nature and frequency of the surveillance activities that are required to show compliance with the ORs. Further advice to Inspectors regarding EIMT is provided in [18].
3. ORs should be written with regard to the instrumentation available to the operators. Supporting methods such as pre-calculated compliance tables, diagrams, or on-line monitors programmed to perform the necessary calculations should be provided. Alternatively, if calculations cannot be avoided, then the safety case should show that these calculations can be performed within the timescales over which adverse conditions could develop; and that the risk of human error when undertaking / checking these calculations is minimised. However, inspectors should seek means of real-time (on-line) rather than retrospective compliance.
4. The safety case should identify the ORs necessary to ensure that all reasonably practicable surveillance arrangements identified in the safety case may be implemented, at all Levels of Defence in Depth. In particular, where an SSC 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). In instances where an SSC may be rendered unable to respond to a future demand ORs should allow for this to be detected, and rectified, before any demand is placed upon it.
5. The safety case should consider the nature of the instrumentation and/or administrative control that will be used to demonstrate OR compliance. Licensees should use proportionate analysis, such as PSA (where available) and experience gained from previous activities, to determine the frequency of any surveillance activities to demonstrate OR compliance. Surveillance requirements should also be determined considering the shortest time by which adverse conditions (e.g., operational drift) or faults could develop, so that there is a sufficient margin of confidence that prevention measures will be initiated before the OR is challenged. The deterministic analysis should therefore conservatively assume the timing of surveillance activities, utilising the results of transient analysis where necessary. Importantly, the OR should be set with sufficient margins so that measurement uncertainty or timing cannot cause an apparently compliant situation to be an un-revealed non-compliance with the safety case.

## Periodic Review of Operating Rules

1. The systematic review and update of ORs, in light of operational events and experience, should form a key part of a licensee’s LC15 periodic safety case reviews. This guidance is consistent with that provided in the IAEA Specific Safety Guide “Periodic Review for Nuclear Power Plants” [19], which states that operational limits and conditions should be reviewed as part of periodic safety reviews.
2. When considering the adequacy of a licensee’s periodic review inspectors should consider whether it has been demonstrated that ORs remain applicable for their intended purpose and can be complied with. Where necessary, a licensee’s review may lead to changes in ORs as a result of operating experience, technological development and RGP. Probabilistic assessment methods may similarly inform the justification for changes to ORs.
3. Further advice to inspectors regarding the assessment of periodic reviews is provided in [20].

## Operating Rule Reporting

1. 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. In cases where a licensee wishes to use an OR at the design basis or safety limit for this purpose (see figure 1); this should be justified explicitly, demonstrating that an appropriate margin of safety remains. Nevertheless, inspectors should seek a sufficient margin of safety between ORs used for event reporting and any safety limit. This ensures that there is a very low likelihood that exceeding a reporting level will lead to initiating any emergency arrangements.
2. In general, licensees should set ORs related to reporting arrangements at the earliest point where non-compliance would entail a significant loss of control. However, they should be set at a suitable level so that the burden from reporting frequent non-compliance is not disproportionate to the consequence.
3. Loss of control could take many forms. Inspectors should therefore recognise that ONR’s degree of interest in, and follow up to, an OR being exceeded should be proportionate to the following:

* the degree to which control was lost;
* the potential consequence of the loss of control;
* the extent to which the licensee was responsible for that loss of control;
* the length of time that the breach was undetected; and
* whether similar events have occurred previously, and whether any learning had been taken.

1. In situations where an OR is not being met or an administrative control cannot be followed, then this should be reported, and the duty holder should have appropriate arrangements to achieve this, in accordance with LC23(3) and LC7. The causes should be analysed by the duty holder, and this may lead to the modification of that rule or procedure, or potentially the methodology used for deriving ORs, in accordance with established arrangements. The licensee’s arrangements should allow for changes to be made in a controlled manner.

## Regulatory Permissioning of Operating Rules

1. The basis of ONR’s regulatory strategy with regards to LC23 is provided in [21]. In line with this approach Inspectors should consider approval of limits and conditions to such an extent and degree of prescription that secure:

* the availability of a suitable hierarchy of safety measures, utilities and resources that are necessary to safeguard nuclear safety and prevent accident progression within the design basis.
* appropriate regulatory oversight and control of changes to operating rules of higher significance in accordance with LC23(5). In practice all high hazard facilities would have accident sequences with the potential to give rise to offsite consequences. Inspectors should therefore seek to apply a regulatory footprint to the operating rules on all high hazard sites in Great Britain.
* a proportionate regulatory footprint against licensee’s arrangements for modifying numerical values of parametric limits and conditions, considering the maturity of existing arrangements for control of modifications under LC22. ONR will not generally approve such parametric limits and conditions where there is sufficient evidence that a licensee’s arrangements, for controlling such changes, are adequate with respect to arrangements made under LC22; nor where ONR has judged that doing so would require disproportionate use of internal resource.

1. All licensees should have suitable arrangements to ensure that modifications on existing plant and processes are reviewed to determine the impact on existing ORs. Any required changes to the ORs should be subject to appropriate due process, commensurate with the classification of the modification and in line with the licensee’s arrangements for LC22.
2. When considering licensee submissions under LC22, inspectors should typically select changes to ORs of the highest categorisation in the licensee’s grading structure as candidates for assessment. Licensee arrangements made under LC22(1) typically provide for a hold-point that prevents implementation of such changes until ONR has agreed for it to be lifted. This aligns to the broader principles of flexible permissioning.

# References

1. ONR, "*Safety Assessment Principles for Nuclear Facilities*", 2014 Edition, Revision 1 (January 2020) [www.onr.org.uk/saps/saps2014.pdf](http://www.onr.org.uk/saps/saps2014.pdf).
2. ONR, “*LC23: Operating Rules*”, NS-INSP-GD-023 Issue 6.1, March 2021.
3. ONR, “*Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)*”, NS-TAST-GD-005 Revision 10, December 2019.
4. WENRA, “*WENRA Safety Reference Levels for Existing Reactors 2020*”, February 2021, [WENRA Safety Reference Levels for Existing Reactors Revision 2020 | WENRA](https://www.wenra.eu/node/86).
5. WENRA, “*Decommissioning Safety Reference Levels*”, Version 2.2, April 2015, [Microsoft Word - WGWD Report\_Decommissioning SRLs\_V2 2.doc (wenra.eu)](https://www.wenra.eu/sites/default/files/workinggroups/wgwd/wgwd_report_decommissioning_srls_v2_2.pdf).
6. WENRA, “*Waste and Spent Fuel Storage Safety Reference Levels*”, Version 2.2, April 2014, [wgwd\_storage\_report\_final.pdf (wenra.eu)](https://www.wenra.eu/sites/default/files/publications/wgwd_storage_report_final.pdf)
7. IAEA General Safety Requirements GSR Part 4, “*Safety Assessment for Facilities and Activities*” (Rev. 1), February 2016 [Safety Assessment for Facilities and Activities | IAEA](https://www.iaea.org/publications/10884/safety-assessment-for-facilities-and-activities)
8. IAEA Specific Safety Requirements SSR-2/1, “*Safety of Nuclear Power Plants: Design*” (Rev. 1), February 2016 [Safety of Nuclear Power Plants: Design | IAEA](https://www.iaea.org/publications/10885/safety-of-nuclear-power-plants-design).
9. IAEA Specific Safety Requirements SSR-2/2, “S*afety of Nuclear Power Plants: Commissioning and Operation*” ( Rev. 1), February 2016, [Safety of Nuclear Power Plants: Commissioning and Operation | IAEA](https://www.iaea.org/publications/10886/safety-of-nuclear-power-plants-commissioning-and-operation).
10. IAEA Specific Safety Requirements SSR-3, “S*afety of Research Reactors*”, September 2016 [Safety of Research Reactors | IAEA](https://www.iaea.org/publications/11031/safety-of-research-reactors).
11. IAEA Specific Safety Requirements SSR-4, “*Safety of Nuclear Fuel Cycle Facilities*”, October 2017 [Safety of Nuclear Fuel Cycle Facilities | IAEA](https://www.iaea.org/publications/12216/safety-of-nuclear-fuel-cycle-facilities).
12. IAEA Specific Safety Guide SSG-70, “*Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants*”, September 2022 [Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants | IAEA](https://www.iaea.org/publications/14901/operational-limits-and-conditions-and-operating-procedures-for-nuclear-power-plants)
13. IAEA Safety Guide WS-G-6.1, “*Storage of Radioactive Waste*”, 2006, <http://www-pub.iaea.org/MTCD/publications/PDF/Pub1254_web.pdf>.
14. IAEA, Specific safety Guide SSG-15, “*Storage of Spent Nuclear Fuel*” (Rev. 1), 2020, [20-03179E\_PUB1882\_14.12.20-Print-PDF.indd (iaea.org)](https://www-pub.iaea.org/MTCD/Publications/PDF/P1882_web.pdf).
15. IAEA Safety Glossary: Terminology used in Nuclear Safety and Radiation Protection; 2018 Edition. IAEA, June 2019, [PUB1830\_web.pdf (iaea.org)](https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf).
16. ONR, “*Procedure Design and Administrative Controls*”, NS-TAST-GD-060 Issue 4.1, December 2021.
17. ONR, “*Categorisation of safety functions and classification of structures, systems and components*”, NS-TAST-GD-094 Revision 2, July 2019.
18. ONR, “*Examination, Inspection, Maintenance and Testing of Items Important to Safety*”, NS-TAST-GD-009 Revision 6, May 2019.
19. IAEA Specific Safety Guide SSG-25, “*Periodic Review for Nuclear Power Plants*”, 2013 [Periodic Safety Review for Nuclear Power Plants | IAEA](https://www.iaea.org/publications/8911/periodic-safety-review-for-nuclear-power-plants).
20. ONR, “*Periodic Safety Review*”, NS-TAST-GD-050 Revision 8, October 2020.
21. ONR, “*Proposal to reform the use of primary powers under Licence Condition 23*”, January 2016 CM9 Ref. 2015/322669.
22. ONR, “*Criticality Safety*”, NS-TAST-GD-041 Revision 7, June 2019

# Glossary and Abbreviations

ALARP As low as reasonably practicable

DBA Design Basis Analysis

EIMT Examination, Inspection, Maintenance and Testing

EMM Enforcement Management Model

HSE Health and Safety Executive

HSWA The Health and Safety at Work etc. Act 1974

IAEA International Atomic Energy Agency

IRR Ionising Radiation Regulations

LC License Condition

MHSWR Management of Health and Safety at Work Regulations

NOOR Normal Operations Operating Rule

OR Operating Rule

PSA Probabilistic Safety Analysis

PSR Periodic Safety Review

REPPIR Radiation (Emergency Preparedness and Public Information) Regulations

RGP Relevant Good Practice

SAA Severe Accident Analysis

SAP Safety Assessment Principle(s)

SFAIRP So far as is reasonably practicable

SEPA Scottish Environment Protection Agency

SQEP Suitably Qualified and Experienced Persons

SRL Safety Reference Level

SSC Structure, System and Component

TAG Technical Assessment Guide(s)

TIG Technical Inspection Guide(s)

WENRA Western European Nuclear Regulators’ Association

# Appendix 1 – Tests for Operating Rules

The following is a summary of some key principles for deriving *ORs*. It has been provided as a quick checklist to aid inspectors’ assessment and is not intended to be exhaustive.

* *ORs* should be a condition or limit and not instructions;
* *ORs* (including temporary *ORs*) should be derived from the safety case and not from other sources;
* The *ORs* should be consistent with the extant safety case and systematically reviewed in light of operational experience;
* *ORs* should be written for operators so that compliance can be clearly demonstrated, and any non-compliance readily identified
* *ORs* should so far as is reasonably practicable (SFAIRP) be specified in directly measurable / checkable terms taking account of measurement uncertainties;
* *ORs* should be graded / classified so that the most important limits and conditions have greatest prominence;
* The number of *ORs* should be minimised where possible by combining similar limits and conditions;
* *ORs* should SFAIRP be derived for all Levels of the Defence in Depth framework including *normal operations*;
* Linking should be provided between the *ORs* and the surveillance requirements required to demonstrate compliance, including expectations for frequency and nature of surveillances.
* The *ORs* should provide unambiguous definitions of each permitted mode of operation, which together define the extent of *normal operations*;
* *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;
* The set of *ORs* should include limits and conditions for plant and system operability, *safety settings* and the availability of *safety measures*;
* Compliance with *ORs* does not necessarily mean risks will be ALARP; *ORs* will normally be set with a margin to the operating point at which risk have been demonstrated to be reduced SFAIRP by the safety case;
* *ORs* 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;
* *ORs* should include identified *safety limits*, denoting extreme conditions within which the facility can still be shown to be safe;
* A subset of the *ORs* 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*.

# Appendix 2 – Common 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 misunderstandings and mixed messages from being repeated in future. Each misconception is given, followed by the correct view in **bold text**:

* The main purpose of LC23 is to identify serious adverse circumstances for the purposes of event reporting and notification.

**Reality: The main purpose of ORs is to define a suite of limits and conditions which capture the requirements and assumptions identified in the safety case. They should be 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 if an OR is breached.

**Reality: ONR’s enforcement decisions will be based upon its Enforcement Management Model (EMM). Key considerations following breach of 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 a breach with a limit or condition identified in the safety case that has not been designated formally as an OR.

**Reality: See the previous bullet. ONR will take appropriate enforcement action commensurate with the circumstances of the breach. This is irrespective of whether and how the OR has been designated.**

* ORs are derived exclusively from the facility’s DBA.

**Reality: Most ORs will likely be derived from the facility’s DBA. However, the licensee should also seek to identify ORs from all parts of its safety case. This includes (where appropriate) the PSA, engineering analysis and severe accident analysis.**

* Criticality ORs need to be treated differently to other LC23 limits and conditions.

**Reality: Although ORs for criticality may be identified by methodologies and safety principles that are presented separately to other aspects of the safety case, they should be derived and implemented using precisely the same processes as are used for all other ORs.**

* Once an operating reactor has been finally shutdown and defueled, 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 defueling a reactor will remove a significant proportion of the site’s hazard potential, appropriately graded ORs will still be required for the remaining hazards. The licensee’s LC23 arrangements need to be suitable and sufficient for the prevailing risks and hazards at the site. This allows all necessary ORs to be 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. This follows 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 this guide will be relevant to all types of faults at all facilities. However, licensees should justify when it elects 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 considers international guidance and best practice at similar facilities elsewhere.**

# Appendix 3 – WENRA Safety Reference Levels of Relevance

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

| Reference Level | Description | Related SAP(s) | Coverage in this TAG |
| --- | --- | --- | --- |
| Safety Reference Levels for Existing Reactors 2020 [4] | | | |
| H1 | Purpose | FA.9 | Section 3 & 5.5 |
| H2 | Establishment and review of OLCs | FA.9 | Section 5.3, 5.7 & 5.9 |
| H4 | Scope of OLCs | FA.6 & FA.9 | Section 5.3 |
| H5 | Safety limits, safety systems settings and operational limits | FA.9 | Appendix 5 |
| H6 | Unavailability limits | FA.6 & FA.9 | Section 5.3 |
| H8 | Staffing levels | EHF.11 | Section 5.3 |
| H9 | Surveillance | EMC.24 & ESS.13c | Section 5.6 |
| H10 | Non-compliance | MS.4 | Section 3 & 5.8 |
| Decommissioning Safety Reference Levels [5] | | | |
| DE42 | Safety issue: Maintenance, Testing and Inspection | EMC.24 & ESS.13c | Section 5.6 |
| Waste and Spent Fuel Storage Safety Reference Levels [6] | | | |
| S26 | The licensee shall establish operational limits and conditions (OLCs) in order to maintain the storage facility and waste and spent fuel packages or unpackaged spent fuel elements in a safe state during facility operation. | FA.9 | Section 5.3 |
| S27 | The defined OLCs (see S-26) shall consider, in particular, and as appropriate:  • environmental conditions within the store (e. g. temperature, humidity, contaminants, …).  • the effects of heat generation from waste or spent fuel, covering both each individual waste and spent fuel packages or unpackaged spent fuel elements as well as the whole store.  • potential aspects of gas generation from waste or spent fuel, in particular the hazards of fire ignition, explosion, waste and spent fuel package or unpackaged spent fuel element deformations and radiation protection aspects.  • criticality prevention, covering both each individual waste and spent fuel packages or unpackaged spent fuel elements as well as the whole store (including operational occurrences and accidental conditions).  • suitability for handling and retrieval. | FA.6 & FA.9 | Section 5.3 |
| S42 | Modifications of design, equipment, storage conditions, waste or spent fuel characteristics, control or management, especially changes of SSCs, OLCs or operational procedures in a spent fuel or radioactive storage shall be subject to planning, assessment, review and authorization processes commensurate to the importance to safety of the modification. These processes shall ensure that the modifications will not impact adversely the safety of the facility or associated facilities or the further management of spent fuel or waste. | FA.9 | Section 5.3 & 5.9 |

# Appendix 4 – Technical Specifications for Nuclear Power Plants

1. UK nuclear power plants generally employ a Technical Specifications (Tech Spec) approach to implementing ORs. This approach was adopted from the US with the construction of Sizewell B and was subsequently implemented across the AGR fleet. Given the US heritage of Tech Specs, inspectors may find information published by US NRC useful ([Technical Specifications | NRC.gov](https://www.nrc.gov/reactors/operating/licensing/techspecs.html)). Particularly ‘§ 50.36’, which discusses the establishment and use of Tech Specs. It should be noted however, that some significant differences exist between the approaches in the US and the UK. For example, US Tech Specs generally apply only to ORs relating to the highest classification of SSCs identified for the plant, whereas ONR expects greater coverage for ORs.
2. Tech Specs specify the plant configuration and availability requirements, protection settings and parameter values that define the safe operating envelope beyond which the plant shall not be intentionally operated. Each Tech Spec typically consists of a specific limit or condition, surveillance requirements and an action (or actions) to follow if the limit or condition is breached.
3. Tech Specs are generally formulated from the upper bound normal operating limits rather than analysed safety limits (see figure 1). In the case of parametric ORs, station operating instructions (or similar) should also be defined below the Tech Spec limit. The need for, and importance of, these supporting limits and conditions is so that operator action and / or engineered means may be used to return conditions back to normal without contravening any NOOR (this is discussed further in para 2, Appendix 5). 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.
4. A feature of the Tech Spec approach is that limits and conditions include specific time periods. This is 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. This approach, where justified within the safety case, provides a graded method of OR compliance. This method seeks to avoid situations in which an immediate return to normal operations induces greater risks than a slower, but more considered return. For example, the immediate trip of a power reactor following the loss of a back-up pump could incur greater risks than running for a limited period without that pump available. As long as provision is made to shut down the reactor if the unavailability extends beyond prescribed limits, pre-justified in the safety case, then setting ORs in this manner should be encouraged. Indeed, the Tech Spec approach, through which ORs provide operators with a suitable but well-defined degree of operational flexibility, is considered to align with internationally accepted good practice and meet the requirements of LC23.
5. The licensee should have procedures to derive the limits and conditions in the Tech Specs from its safety case. Suitably Qualified and Experienced Persons should identify and implement these within the licensees’ LC23 arrangements. To demonstrate compliance, there should be an auditable trail from the safety case to the limits and conditions embodied in the Tech Specs.
6. Inspectors should therefore consider the various aspects of Tech Spec production at the most suitable points in the development of the safety case. This may mean that the identification of appropriate parametric and operational limits is considered as part of GDA, despite the fact that the Tech Specs they inform are unlikely to have been developed. During site licensing inspectors should sample to gain confidence in the duty holder’s arrangements for LC23, and so this may include consideration of the processes that will be used to produce Tech Specs. Although any given duty holder’s schedule for development / production of Tech Specs will vary, inspectors should sample evidence of the implementation of its arrangements to gain confidence in the final output. Inspectors should seek to do this during the construction / commissioning phase, and in any event prior to radiological risks being introduced to the site.
7. In some circumstances, it may be the case that a given nuclear power plant design has been constructed in another country. As such it will have already been subject to regulatory scrutiny. In such circumstances it may be possible to take credit for the assessment activities of other national regulatory bodies. However, inspectors should be mindful of the potential differences which may affect the validity of any such assessments, in the UK regulatory context. Such differences may exist between the regulatory regimes of the countries concerned (e.g., the level of prescription), environmental and climatic conditions, or the specific detailed designs (i.e., design modifications for a given site may not be duplicated across all sites). This is not intended as an exhaustive list, rather as a prompt that inspectors should seek to identify any differences and consider the implications for their specific intervention strategies.

# Appendix 5 – Operating Rules and Defence in Depth

As discussed in section 5, the extent to which ORs at Levels 2 to 5 need be identified will vary according to the type of facility. Further guidance on ORs, level by level, is provided in the following paragraphs, which expand upon the schematic in Figure 1.

**Level 2** – Prevention and control of abnormal operation and detection of failure

1. The safety case should identify ORs at the limit of normal operations (Normal Operations ORs, hereafter referred to as NOORs). These NOORs are for the prevention and control of abnormal operation and detection of failure. 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 then define the totality of normal operations.
2. The NOORs should, SFAIRP, be set some margin away from the conditions where the facility is intended to be operated. This is because contravening a NOOR should be regarded as a serious matter. In cases where a NOOR can be gradually approached (in which the limit is set in terms of a continuous parameter such as pressure or temperature), the safety case should identify further supporting limits and conditions. These supporting limits and conditions should be set before the NOOR. This allows operator action and / or engineered means to return the conditions back to normal without contravening any NOOR.
3. Normally, these supporting limits and conditions would be defined in the operating instructions (LC24)[[6]](#footnote-7). These instructions are 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. This approach minimises 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. For example, by providing redundant / diverse equipment that can be substituted-in in the event of equipment unavailability.
4. 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. The concept of ‘action on entry’ may be of value in these situations. For example, chemistry action level 1 typically allows for approximately 30 days for corrective action when there’s a deviation from the normal operating range. That action should take place on entry into the condition, not on day 29. This philosophy is driven by the fact that many chemistry-based degradation routes lead to integral damage that accrues over time.

**Level 3** - Control of faults within the design basis

1. The safety case should identify limits and conditions that define the design basis of the plant or facility. There should always be ORs in place to define the corresponding safety settings and safety measures, together with any provisions that the safety measures will need in order to operate (power supplies, fuel stocks, chemical stocks etc). The ORs defining the required design basis safety measures will normally be amongst the most important safety limits and conditions and so their derivation should be a key focus of the safety case. The safety settings should have an adequate margin to normal operations to avoid inadvertent initiation/activation of the safety measures.
2. The safety case should include deterministic analysis. This analysis should show that safety measures, and the associated safety settings 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 without entailing serious consequences. Importantly, the term normal operations embody all the operating modes permitted at the facility. Hence the ORs governing minimum safety measures should not just be limited to the principal operating mode for which the facility was designed but address all permitted operating modes.
3. Importantly, the deterministic analysis should 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 (in line with ESS.4). The safety case should 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. In addition, where reasonably practicable, the design basis should incorporate substantiated operational margins to any relevant safety limit. Achieving this will normally require a balance to be struck between the operational 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.

**Level 4** - Control and mitigation of accident conditions

1. To reach Level 4 implies that the Level 3 safety measures protecting against the fault must have failed. Breaching 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, particularly through application of PSA and SAA.
2. In many types of facility, fault progression through Level 4 will be slow enough to make the implementation of beyond design basis measures reasonably practicable[[7]](#footnote-8). 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.

**Level 5** - Mitigation of significant radiological releases

1. The suite of ORs should always include a suitable and sufficient set of safety limits. These should be defined conservatively so that no significant radiological consequences can arise without at least one safety limit being exceeded. This should be interpreted as exceeding IRR dose limits. IAEA guidance [12] recognises that in such event’s additional safety measures and accident management strategies may be needed to mitigate the consequences. This is consistent with SAP EKP.3 which identifies *“emergency control and on- and off-site emergency response”* as essential means of achieving protection in Level 5.
2. Licensee’s may identify safety limits through a variety of different methods including DBA, PSA and SAA; taking due account of uncertainties and ensuring they are articulated in terms that are meaningful to the facility operators. Inspectors should be aware that the key application of these ORs is to inform (and potentially to act as triggers within) the emergency arrangements and accident management strategies. It is therefore important to recognise that although a suitable and sufficient set of ORs should be identified by the licensee, any emergency response for the mitigation of off-site releases may be outside its control.

# Appendix 6 – Criticality Safety Operating Rules

1. Previous revisions of this TAG provided specific guidance with regards to criticality limits and conditions. Although the ORs for criticality safety should be derived and implemented using the same principles as other ORs, it is deemed beneficial to retain examples of the application of criticality safety considerations to ORs here as an appendix to the main text, to demonstrate how they may be derived and implemented. It also demonstrates how ORs may be derived for other faults that rely purely on preventative measures.
2. In view of the major hazard potential associated with criticality safety, ORs should generally sit high in a licensee’s hierarchy of controls. SAP ECR.2 sets out ONR’s expectation that a double contingency approach should be applied to guard against unintended criticality, further detail of which is provided in [22]. Whether the double contingency principle can be satisfied or not, the DBA principles of fault tolerance and other relevant SAPs will still apply.
3. Criticality safety may be achieved through safety measures that prevent an unsafe change from developing or being initiated (e.g., engineered systems that detect an increase in fissile content or limit quantities of materials, and/or manually checking a permitted limit prior to moving fissile material or a moderator). The advice provided in the main body of this guide is equally valid and applicable to these scenarios; however, when considering such cases, Figure 1 may be modified to show the fault progression as a series of step changes (see Figure 2 below).

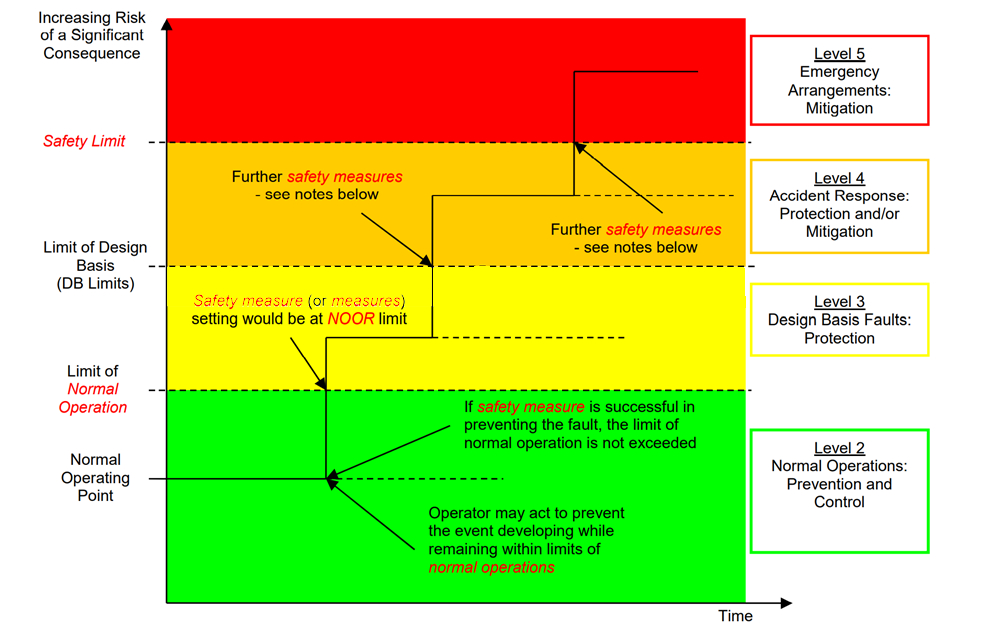
****

Figure 2 – Schematic Illustration of Defence in Depth Approach to Operating Rules for Operations Subject to Step Changes and Preventative Safety Measures

1. Considering Figure 2, application of the double contingency principle may result in limits on 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 as two changes leading to a beyond design basis event. In reality however, both safety measures should 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.
3. As an example, the analysis of Pu canisters in a glovebox might show that four canisters may be safe, but a fifth cannot be demonstrated to be safe from unintended criticality. Assuming there is no operational need to process more than one canister at a time, a NOOR should specify that no more than one is permitted to be present in the glovebox at any time (this is the first line of defence). The safety case should also identify safety measures to protect against multiple canisters being present in the glovebox. The safety limit should, however, be set at four canisters, since this is the last point that may be demonstrated to be safe.
4. In this example, the fault of inserting an extra canister would need to occur three times-over to reach the safety limit. 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 design basis limit is two cans). The design basis limit is set to maximise the margin to the safety limit whilst allowing the safety measures at the NOOR limit to act without the design basis limit being exceeded. ORs may therefore be set at Level 2 (the NOOR – one can, defining normal operations), Level 3 (to ensure the availability of safety measures which protect against multiple cans being present) and Level 4 (four cans – the safety limit, set relative to the realised hazard).
5. Of these, the NOOR (at one can) and the OR(s) requiring safety measures to protect against multiple cans should be categorised at the highest level in the licensee’s hierarchy, as these provide the most important means of protection. The safety limit would then sit in the lower category of a licensee’s hierarchy, as it is indirectly relevant to the operators (as it would only be monitored against in extreme circumstances).
6. In some cases, it may not prove reasonably practicable to maintain the margins described in the example above. If the analysis had shown that although two cans may be accommodated, a third can cannot be proven safe then, assuming the operation is necessary, and risks demonstrated to be ALARP, the design basis limit and safety limit would need to be the same. In such a situation a robust justification of sufficient Defence in Depth, would be required. The ORs would be defined in the same way as previously, but the safety limit and the design basis limit would both be at two cans.
7. Typically, licensees that undertake criticality sensitive operations use criticality clearance certificates (CCC) for a given marked criticality area to specify the criticality working limits in that area. CCCs are well established RGP for defining limits and conditions and typically specify the allowable masses / concentrations / numbers and types of material that are allowable in the area.

1. Such as, para 201, EHA.5, EPS.4, para 295j, para 313 (change to operating rules should be considered as a modification), EGR.3, EGR.12, para 525b, para 539, ERC.3, para 547 to 548, 551, ERC.4, EHT.2, para 564b, para 565, para 607 and para 809. [↑](#footnote-ref-2)
2. NS-G-2.2 was superseded by SSG-70 in 2022. However [13] was published in 2006, prior to the issue of SSG-70. [↑](#footnote-ref-3)
3. Note that, 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. [↑](#footnote-ref-4)
4. Including human factors substantiation. [↑](#footnote-ref-5)
5. Further discussion of the normal operating point, supporting limits & conditions, and the definition of operating instructions is provided in Appendix 5 (Level 2 - Prevention and control of abnormal operation and detection of failure). [↑](#footnote-ref-6)
6. These supporting limits and conditions may be identified from various sources, including EIMT instructions, substantiation documentation or operations and maintenance manuals. [↑](#footnote-ref-7)
7. Although inspectors should not necessarily expect to see accident management ORs at all types of facility as the speed of progression from Level 3 to Level 5 may make it impractical. [↑](#footnote-ref-8)