

# NUCLEAR SAFETY DIRECTORATE - BUSINESS MANAGEMENT SYSTEM

## TECHNICAL ASSESSMENT GUIDE THE LIMITS AND CONDITIONS FOR NUCLEAR PLANT SAFETY

T/AST/035

ISSUE 002

Approved By: C H Waker

CWaker

Issue Date: 18/11/04

Open Government Status: Fully Open

Review Date: 17/11/07

## 1. Purpose and scope

1.1 This guide provides advice to inspectors on the interpretation of the safety assessment principles (SAPs) P325 to P328. These cover operating safety limits and conditions for nuclear plant and state definitions for the principal points within the safe envelope of a nuclear plant.

This guide is concerned with the methodology of how these limits and conditions should be derived and implemented by the licensee. Its purpose is to advise and inform NSD inspectors in the exercise of their professional regulatory judgment. Comments on this guide, and suggestions for future revisions, should be recorded on the appropriate registry file.

## 2. SAPs addressed

2.1 This guide covers principles 325-328 and takes account of principles 26, 27, 61 and 62 of the Safety Assessment Principles <sup>[1]</sup>

## 3. Relationship to licence and other relevant legislation

The relevant licence conditions are: -

### 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, if in its opinion circumstances render it necessary at any time, agree to the temporary suspension of any approved operating rule.

The licence condition requires the operator to produce a safety case to justify the operation of the installation. One purpose of such a safety case is to identify all of the necessary limits and conditions that ensure the plant is kept within such parameters that ensure the safety of the plant during normal operation, fault and accident conditions.

## **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.

## **Licence Condition 27 SAFETY MECHANISMS, DEVICES AND CIRCUITS**

The licensee shall ensure that a plant is not operated, inspected, maintained or tested unless suitable and sufficient safety mechanisms, devices and circuits are properly connected and in good working order.

The linkage between the licence conditions 24 and 27 and the SAPs is implied by P27. This indicates that it is design basis (fault) analysis (see T/AST/006) that should provide the relevant information that is required by these license conditions.

## **4. Advice to assessors**

### **4.1 Philosophy**

1) The above licence conditions (LC) require that limits and conditions be set on plant parameters and operational circumstances, and measures applied to ensure that they are not breached. The means by which such limits and conditions are determined, the levels at which they are set, and the measures that ensure compliance, form the subject matter of this guide. Reference has been made in preparing this guide to IAEA guidance on the specific area of Nuclear Power Plants<sup>(3)</sup> and some similarities will be observed.

2) A potential difficulty arises, especially with respect to setting a limit, in that a fixed value is required for what is often a continuous parameter, with a corresponding scale of harmful consequences. This issue is addressed herein by recommending consequence thresholds in terms of the whole body annual dose limits in IRR99<sup>(4)</sup>, namely 20mSv for workers and 1mSv for members of the public, calculated on a conservative basis in both

cases. Also included are consequences corresponding to serious loss of control as indicated in SAPs P45 and P46. These consequence levels are considered to be high enough to avoid there being so large a set of limits and conditions for any particular plant that their management would be unduly difficult, and low enough to ensure an appropriate level of seriousness. In this guide accident consequences equal to or greater than these will be referred to as "**Significant Consequences**".

3) In the ideal world, where knowledge and understanding would be complete, then suitable analysis for a given plant should enable all fault sequences with a Significant Consequence to be linked to corresponding parameter limits and operational conditions. In such circumstances, as long as these are not breached, then accidents with Significant Consequences cannot occur. This provides a benchmarking principle against which judgements can be made as to whether all that is reasonably practicable has been done, since in the real world knowledge and understanding are rarely complete and it is not possible to assert with absolute confidence that accidents can never occur. To allow for this uncertainty there should be some appropriate margin of safety between the limits and conditions that are applied in practice to comply with LC23 (herein abbreviated to "**L23LAC**"), and those that the analyses indicate as possible but with no margin of safety, (herein referred to as "**Safety Limits**").

## 4.2 Application

1) Licensees are required to apply and demonstrate adequate control of safety with respect to LC 23, 24 and 27 at all times. They may do so by applying the methods indicated herein, or by other means, providing they are shown to be effective. Also the terms and definitions used herein relate to the regime set out in this guide for complying with LC 23, 24 and 27. Their use does not imply any obligation on licensees to either use them, or to keep to these definitions if they use the same terms.

2) The set of Safety Limits and corresponding L23LAC must be complete (i.e. no Significant Consequence can occur providing they are not exceeded), determined by an appropriate deterministic analysis (P27), and documented in the safety case.

3) Where safety systems <sup>(5)</sup> are needed to ensure that the limits and conditions are not exceeded, they may be provided by equipment (LC27 - Safety Mechanisms, Devices and Circuits), and/or procedures (LC24 - Operating Instructions).

4) The L23LAC must be such that compliance can be established and demonstrated, and any breach can be clearly identified.

5) L23LAC should be set at or below the starting point of the largest identifiable design basis transient <sup>(2)</sup>, assuming proper action of a safety measure that stays within the

relevant Safety Limit. The "**Safe Operating Envelope**" (SOE) is the term used herein for the boundary of plant limits and conditions that define the starting points of such transients. The "**Range of Normal Operation**" is the term used herein for the area that encompasses the operating region and all acceptable fluctuations. (See figure 1 for an illustration of the guide's definitions)

6) In some cases a 'safe' state can only be defined by combinations of parameters and circumstances - e.g. criticality is a function of enrichment, moderator, reflector, mass and configuration. Hence some Safety Limits and L23LACs will need to embody such combinations.

7) In setting Safety Limits and L23LACs account should be taken of the requirements of P327 with respect to expected extremes of plant conditions, expected combinations of parameter values, and possible short and long term or cumulative damage processes.

#### 4.3 Safety Systems

1) These are the systems put in place by the licensee to control any deviation from normal operation that threatens to exceed the LC23LAC. Their function is to ensure safety and not to assist in normal operation (See T/AST/003<sup>(5)</sup>).

2) Once the LC23LAC are defined, the safety systems (both equipment and procedures) that are necessary to ensure that they are complied with should be elevated in status above other safety systems, such that their availability when needed is assured so far as is reasonably practicable.

3) For these safety systems, what is sought, for each "**significant**" fault, is an identified basket of measures, which are shown by analysis to be "**sufficient**" to protect the fault, and which are covered by explicit arrangements to ensure that they are "**available**" when needed.

4) "Significant" means having potential consequences that are equal to or greater than Significant Consequences.

5) "Sufficient" means able, as a group, to reduce risks to as low as is reasonably practicable without other safety systems. Although the SOE only relates to potential accident consequences, frequency aspects are catered for by Sufficiency of safety systems, such that the higher the unprotected frequency the more safety systems that are required in the basket. In addition, this sufficiency of safety systems embraces the requirements of P328 that the safety case should identify minimum equipment levels and minimum staffing levels, which then become explicit in the arrangements made

under LC23.

6) "Available" for equipment means: (a) not known to be unavailable (i.e. either able to function properly or failed due to an unrevealed fault); or (b) having an appropriate form of substitute protection when known to be unavailable. This requires pre-planned arrangements to deal with known unavailability, regular testing and maintenance to keep the equipment in good condition and reveal failures, and usage only during its useful life.

7) "Available" for procedures means having a sufficiently high profile that implementation is assured. The expectation is that implementation would require an appropriate level of training.

8) Safety systems may be implemented by equipment and/or procedures, although in keeping with modern safety practice procedures should only be used in isolation when it is not reasonably practicable to provide equipment. Ideally there should be dedicated and demonstrably reliable engineered safety systems, set at or before the LC23LAC, whose function is to terminate the fault sequence, and also other safety systems whose function is to mitigate the consequences.

9) Wherever reasonably practicable safety systems should operate automatically and not depend on operator control.

10) Where reasonably practicable substitution should be by other equally reliable equipment, but may be by a regime of special monitoring or inspection.

11) Substitution duration should be controlled and justified in the safety case.

12) If substitution is not reasonably practicable then the hazardous operation should be stopped, though in some cases it may be possible to justify in the safety case continued operation without the safety measure for a limited time.

13) The expectation is that the safety systems should be as high as possible on the P61/62 hierarchy i.e. drive toward inherently safer plant design provisions, and should meet the requirements of P65: 'defence in depth'. An example of the application of defence in depth may be found in Appendix 1. Accordingly the expectation is that there is a hierarchy of indications and alarms, which will allow the operator to restore plant conditions prior to reaching the LC23LAC.

14) Trip and mitigation systems are required to operate outside the normal operating range. Hence it is essential that they and any associated monitoring equipment meet the requirements of P326 - their safe operating limits should be appropriate to any reasonably foreseeable combination of plant conditions likely to arise during the fault.

15) Faults with potential consequences less than Significant are still likely to require the provision of safety systems, but the arrangements for assurance of their availability are not expected to be provided to the same degree of rigour as those for faults with Significant Consequences.

#### 4.4 Operating Instructions

1) Operating Instructions are developed in accordance with LC24. LC 24(1) sets the general requirement for written operating instructions for all operations that may affect safety.

2) Operating Instructions should be designed to minimise the risk from potential hazards. They may operate to: -  
prevent a hazardous situation arising  
mitigate its effects  
bring the plant back to a safe operating region.

3) Maintenance instructions and administrative procedures for Criticality Clearance Certificates are also examples of preventative Operating Instructions.

4) LC 24(2) (which is the part relevant to this guide) requires operating instructions (OI) to support or enable the LC23LAC. As with LC23LAC licensees have chosen their own terms to describe these instructions. Within this guide the general term LC24(2)OI is used.

5) LC24(2)OI are: -

- Required to supplement an automatic system to prevent the breach of an LC23LAC, or where manual action is the only method that can achieve such protection
- Expected to complement engineered safety features of the plant.
- Can either be specifically identified instructions within the general detail working level instructions or form a high level statement of operating requirements that are implemented by underlying detailed instructions.
- Expected to state the operating rule they support or enable.
- Expected to define the management level required to action them
- Expected to state the conditions required to invoke them
- Should not be complex

- Should have sufficient steps to enact them without providing excessive detail that may cause delay or confusion
- Should be understood by those using them
- Should include indicators for the success of the action and for higher order actions where required
- Should contain actions that are both verifiable and capable of being tested
- Should list all required equipment and their locations

6) Operators should be trained and undergo regular refresher courses on the use and importance of LC24(2)OI within their area.

## 5. References

1. HM Nuclear Installations Inspectorate: Safety Assessment Principles for Nuclear Plant, ISBN 0 11 882043 5, 1999.
2. Technical Assessment Guide 'TRANSIENT ANALYSIS FOR DBAs IN NUCLEAR REACTORS', T/AST/034.
3. IAEA 'Operating Limits and Conditions and Operating Procedure for Nuclear Power Plants', IAEA Safety Standards Series, Safety Guide No. NS-G-2.2
4. Ionising Radiation Regulations 1999 (SI1999/3232)
5. Technical Assessment Guide 'Safety Systems', T/AST/003.

---

### **Appendix 1: Example of the application of Defence in Depth**

When applying defence in depth the following principles are considered the elements of good practice

- 1) Defence in Depth should be proportional to the degree of hazard.
- 2) During normal operation a plant is expected to operate, where possible, under automatic control. However plant control may include warnings to the operator that require operator response.

3) As defined in P328 the minimum staffing levels of suitably qualified and experienced people and the minimum level of operational equipment necessary to ensure safety in normal or fault conditions should be specified according to the degree of interaction required between operator and control system.

4) The degree of required interaction should not place undue stress on operators and those criteria addressed within P91-94 (human factors) should be met.

A generic example is displayed in the following figure, based on Figure A-1 in Reference 3, and explained as follows: -

1) In the event of a plant moving outside of the normal operating envelope it is expected that the first line of defence would be an alarm (Point 1) that allowed operator intervention to correct the situation.

2) It is expected that in the event operator intervention cannot halt the excursion then according to best practice a second line of defence in the form of a pre-LC23LAC automatic trip would activate (Point 2).

3) The Pre-LC23LAC trip is expected to act immediately to move the plant towards a safe state or to immediately initiate mitigation systems. Examples of such mitigation systems are included within appendices 2 and 3.

4) It is expected that the response to the Pre-LC23LAC trip would be an excursion that did not exceed the LC23LAC.

5) The reaction time that a safety system is required to operate at should be defined by the safety analysis of the speed of propagation of the fault and its effects.

6) Trip and mitigation systems are required to operate outside the normal operating envelope. It is essential that they and any associated monitoring equipment meet the requirements of P326. I.e. their safe operating limits should be appropriate to any reasonably foreseeable combination of plant conditions likely to arise during the fault and the design criteria should be chosen as if such conditions are the normal operating conditions for that equipment.

7) In the event of the system continuing to follow an excursion that exceeds the LC23LAC then at that point (Point3) there would ideally be a further automatic trip.

8) The trip at the LC23LAC is also expected to immediately act to move the plant towards a safe state or to immediately initiate mitigation systems.

9) In addition it is expected that if all other measures fail and the accident occurs, there will be dedicated safety systems, preferably engineered, to mitigate the consequences. P325 requires that the plant parameters relevant to safe operation should be identified and operational limits on those parameters derived such that in the event of any design basis fault sequence: a) the integrity of the physical barriers to radioactive release is maintained and the fault consequences limited as required by P25; and b) no safety-related component (or structure or system) required to prevent or mitigate the fault sequence will be caused to operate outside the conditions for which it has been qualified.

10) The design of the dedicated safety systems should take into account the effects of cumulative damage processes (P327), including the possibility of short or longer-term cumulative damage processes producing larger extremes than those foreseen from a single event.

---

## **Appendix 2: Examples of Limits and Conditions for Nuclear Power Plant**

### **Examples of LC23 Conditions**

1. Within Nuclear Power Station Tech Specs it might be a condition that all four gas turbines emergency generators shall be available when operating at power. As it is possible for a number of reasons including maintenance that at least one may be out of service this is further qualified by time periods for which this condition may be allowed to be unmet before shutdown is commenced. E.g. 1 gas turbine (GT) is allowed to be unavailable for 31 days, 2GT's may be unavailable for up to 24 hrs provided refuelling is suspended.

2. Within Nuclear Power Station's operation there might be a condition that all three emergency boiler feed pumps (EBFP's) shall be available when operating at power. As it is possible for a number of reasons including maintenance that at least one may be out of service this is further qualified by time periods for which this condition may be allowed to be unmet before shutdown is commenced. E.g. 1 EBFP is allowed to be unavailable for 31 days. If this should extend to 2 EBFP's then that time allowance falls to 8 hours.

### **Examples of LC23 Limits**

1. Maximum Outlet Temperature of the Reactor Coolant System

2. Maximum Neutron Flux

## **Examples of Prevention / Mitigation Systems**

In order of actuation: -

1. Guardlines
2. Shutdown system (Rods/Nitrogen Injection/Borated Water)
3. Engineered Safety Features Systems including: -

Post Trip Sequencing Equipment (PTSE)  
Reactor Shutdown Sequencing Equipment (RSSE)  
Engineered Safety Feature Actuation System (ESFA).

---

## **Appendix 3: Examples of Key Areas for Limits and Conditions for Nuclear Chemical Plant**

### **Examples of LC23 Conditions**

1. Within the Windscale Vitrification Plants HAL is only to be fed to the calciner if there is a ventilation depression between the C5 and the C2/3 vents.

### **Examples of LC23 Limits**

1. Within the Thorp plant the initial enrichment of the spent fuel feed must have been no greater than 4% U<sup>235</sup>.
2. Within any plant that contains hydrogen the normal operating limit within air shall be 25% of the Lower Flammable Limit.

## **Examples of Prevention / Mitigation Systems**

1. In the event of total failure in the cooling of a Highly Active Storage Tank the off-gas system has been sized to deal with the gas flow generated by boiling liquids.